Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Open C3S
Open Competence Center for Cyber Security

Bachelorstudiengang Informatik/IT-Sicherheit

Einführung in die digitale Forensik [DigiFor]

Autoren:
Prof. Dr. Harald Baier
Thomas Göbel, M.Sc.

Universität der Bundeswehr München

Einführung in die digitale Forensik
[DigiFor]

Studienbrief 1: Einleitung

Studienbrief 2: Grundlagen der digitalen Forensik

Studienbrief 3: IT-forensische Software

Studienbrief 4: Datenträgerforensik

Studienbrief 5: Dateisystemforensik

Studienbrief 6: Analyse des FAT-Dateisystems

Studienbrief 7: Analyse des NTFS-Dateisystems

Studienbrief 8: Prozessmodelle

Autoren:

Prof. Dr. Harald Baier

Thomas Göbel, M.Sc.

---

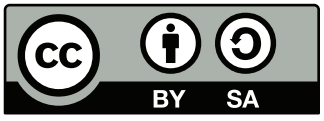
3. Auflage

Universität der Bundeswehr München

Forschungsinstitut Cyber Defence (CODE)
Carl-Wery-Straße 22
81739 München

3. Auflage (2021-09-13)

Autoren früherer Auflagen:
Sebastian Gärtner, M.Sc.
Björn Roos, M.Sc.
Frank Breitinger, M.Sc.
Denise Muth, M.Sc.
Georgios Stivaktakis



Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen **5**
I. Abkürzungen der Randsymbole und Farbkodierungen . . . 5
II. Zu den Autoren . . . 6
III. Modullehrziele . . . 7

Studienbrief 1 Einleitung **11**

Studienbrief 2 Grundlagen der digitalen Forensik **17**
2.1 Lernziele . . . 17
2.2 Advance Organizer . . . 17
2.3 Forensische Grundlagen . . . 17
2.4 Digitale Forensik und digitale Spuren . . . 21
2.4.1 Digitale Spuren . . . 21
2.4.2 Klassifikation digitaler Spuren . . . 23
2.4.3 Praktiken der digitalen Forensik . . . 25
2.5 Das digitale Austauschprinzip . . . 26
2.6 Vor- und Nachteile digitaler Spuren . . . 27
2.7 Post-Mortem- und Live-Forensik . . . 29
2.8 Darstellungen von Datenstrukturen . . . 30

Studienbrief 3 IT-forensische Software **35**
3.1 Lernziele . . . 35
3.2 Advance Organizer . . . 35
3.3 Grundsätzliche Eigenschaften IT-forensischer Werkzeuge . . . 35
3.4 Kryptographische Hashfunktionen . . . 37
3.5 Open-Source Software . . . 40
3.5.1 dd . . . 40
3.5.2 File Carver . . . 41
3.5.3 Strings . . . 43
3.5.4 Sleuthkit und Autopsy . . . 45
3.5.5 DFF . . . 46
3.5.6 IT-forensische Live-CDs . . . 46
3.6 Kommerzielle Software . . . 47
3.6.1 X-Ways . . . 47
3.6.2 EnCase . . . 48

Studienbrief 4 Datenträgerforensik **51**
4.1 Lernziele . . . 51
4.2 Advance Organizer . . . 51
4.3 Speichermedien . . . 51
4.4 Datensicherung . . . 53
4.4.1 Post-Mortem-Datensicherung . . . 54
4.4.2 Writeblocker . . . 55
4.5 Reservierte Bereiche auf Datenträgerebene . . . 58
4.5.1 Host Protected Area (HPA) . . . 58
4.5.2 Device Configuration Overlay (DCO) . . . 61
4.6 Partitionierung . . . 61
4.7 DOS Partitionsschema . . . 64
4.8 GPT-Partitionsschema . . . 72

Studienbrief 5 Dateisystemforensik **79**
5.1 Lernziele . . . 79
5.2 Advance Organizer . . . 79

5.3 Einführung . . . 79
5.4 Referenzmodell von Carrier . . . 80
5.5 Grundlagen der Dateisystem Analyse . . . 82

Studienbrief 6 Analyse des FAT-Dateisystems 93
6.1 Einführung . . . 93
6.2 Dateisystemdaten (reservierter Bereich) . . . 95
6.3 Metadaten in File Allocation Tables . . . 100
6.4 Metadaten in Verzeichnissen im FAT-Dateisystem . . . 104
6.5 Dateinamen . . . 115
6.6 Abschlussbetrachtungen . . . 117

Studienbrief 7 Analyse des NTFS-Dateisystems 121
7.1 Einführung . . . 121
7.2 Dateisystemdaten . . . 124
7.3 Metadaten in der MFT . . . 128
7.4 Metadaten in Attributen . . . 133
7.5 Dateinamen und Verzeichnisse in NTFS . . . 142
7.6 Inhaltsdaten in NTFS . . . 148
7.7 Vertraulichkeit in NTFS – das Encrypted File System . . . 152
7.8 Abschlussbetrachtungen . . . 157

Studienbrief 8 Prozessmodelle 161
8.1 Lernziele . . . 161
8.2 Advance Organizer . . . 161
8.3 Einleitung . . . 161
8.4 S-A-P Modell . . . 161
8.5 Computer Forensics Field Triage Process Model . . . 163
8.6 BSI Modell . . . 163
8.7 Casey's Investigation Process Model . . . 166
8.8 NIST Modell . . . 168
8.9 Diskussion der Begriffe . . . 170

Verzeichnisse 173
I. Abbildungen . . . 173
II. Beispiele . . . 174
III. Definitionen . . . 175
IV. Exkurse . . . 175
V. Kontrollaufgaben . . . 175
VI. Tabellen . . . 176
VII. Literatur . . . 177

Glossar 179

Stichwörter 181

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Merksatz	M
Übung	Ü

II. Zu den Autoren

Harald Baier promovierte 2002 an der TU Darmstadt über eine Arbeit zur effizienten Erzeugung elliptischer Kurven. Er war Mitarbeiter in einem Sicherheitsprojekt der Deutsche Bank AG und baute das Darmstädter Zentrum für IT-Sicherheit auf. Nach Professorentätigkeiten an der TH Bingen (2004-2009) und der Hochschule Darmstadt (2009-2020) ist er seit 01.09.2020 am Forschungsinstitut CODE der Fakultät für Informatik an der Universität der Bundeswehr München tätig. Dort hat er die Professur für digitale Forensik inne. Schwerpunkt seiner Arbeit sind daher unterschiedliche Aspekte der digitalen Forensik.

Thomas Göbel studierte Informationstechnik im Bachelorstudium an der DHBW Mannheim und später Informatik im Masterstudium an der Hochschule Darmstadt. Im Masterstudiengang spezialisierte er sich auf den Vertiefungsschwerpunkt IT-Sicherheit. Aktuell ist er als Doktorand im Bereich der Digitalen Forensik am Forschungsinstitut CODE an der Universität der Bundeswehr München tätig. Im Detail beschäftigt er sich mit der Synthese von forensisch relevanten Datensätzen und geeigneten IT-forensischen Analysemethoden. Seit Sommersemester 2018 ist er zudem als Dozent und Tutor im Open C³S Projekt tätig.

III. Modullehrziele

Die Studierenden sollen folgende Fähigkeiten erlangen:

- Grundlegendes Verständnis forensischer Wissenschaften.
- Sicherung, Analyse und Auswertung von unbekannten Datenträgern.
- Bewerten digitaler Beweise und deren juristische Relevanz.
- Forensische Analyse gängiger Dateisysteme (FAT, NTFS).
- Einsatz und Bewertung gängiger Werkzeuge im Bereich der digitalen Forensik.
- Kenntnisse über Vorgehensmodelle der digitalen Forensik und Gutachtenerstellung.
- Funktionsweise kryptographischer Hashfunktionen und deren Rolle in der digitalen Forensik.

Modulbeschreibung

Modulbezeichnung:	Einführung in die digitale Forensik (Introduction to digital forensics)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Einführung in die digitale Forensik Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	IT-forensisches Gutachten (Hausarbeit)
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen:	• Kenntnisse über digitale Zahlendarstellungen und Kodierungen (z.B. ASCII) • Grundkenntnisse im Umgang mit Betriebssystemen (insbesondere Linux) • Sicherheit im Umgang mit der Linux-Kommandozeile • Grundlegende Programmierkenntnisse
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss der Module • Einführung IT Sicherheit • Systemsicherheit 1
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 5
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Klassische forensische Wissenschaften und digitale Forensik • Grundlagen der digitalen Forensik • Digitale Spuren (Entstehung, Manipulier- und Kopierbarkeit, Personenbezogenheit) • Datenträgeranalyse (DOS / GPT Partitionsschema, HPA, DCO) • Einführung in die Dateisystemanalyse (Generelles Konzept, FAT, NTFS) • Analyse mit forensischen Tools (Sleuthkit, Autopsy, DFF, Filecarver) • Vorgehensmodelle und Gutachtenerstellung • Hashfunktionen in der digitalen Forensik • Praktische Bearbeitung von Aufgaben
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der digitalen Forensik und können diese anwenden. Sie haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Sie kennen weiter das grundlegende Konzept sowie die Eigenschaften der gängigen Dateisysteme FAT und NTFS und können mit diesem Wissen eine Dateisystemanalyse durchführen. Darüber hinaus kennen Sie die grundlegenden Schritte eines IT-Forensikers und können mit allgemeinen und speziellen forensischen Werkzeugen sicher umgehen. Des Weiteren sind die Studierenden mit der grundlegenden Funktionsweise kryptographischer Hashfunktionen, sowie deren Rolle in der digitalen Forensik vertraut. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit den Grundprinzipien der IT-Forensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer forensischen Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiteren besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Häufigkeit des Angebots:	Wintersemester

Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Brian Carrier: File System Forensic Analysis, 5th Printing. Addison-Wesley Longman, Amsterdam (17. März 2005), ISBN 978-0321268174 • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier Academic Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. • Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Studienbrief 1 Einleitung

Wachsende Informationsmenge

In den letzten Jahren hat die Verbreitung und der Gebrauch von elektronischen Geräten drastisch zugenommen. Traditionelle Informationsträger wie Bücher, Fotos, Briefe und Schallplatten wurden durch E-Books, digitale Fotografie, E-Mails und MP3s ersetzt. Dieser Wandel geht einher mit der wachsenden Speicherkapazität von heutigen Datenträgern, die von ein paar Megabyte auf mehrere Terabyte anwuchsen. Somit können Anwender ihre kompletten Informationen auf einer einfachen Festplatte speichern anstelle einer analogen Ablage in Hunderten Kartons auf dem Dachboden. Auch wenn der physikalisch eingenommene Platz sich um ein Vielfaches verringert, so bleibt die Informationsmenge zumindest dieselbe. Oftmals übersteigt sie diese aber um ein Vielfaches. Zur Sicherung, Selektion, Analyse und Auswertung dieser enormen digitalen Datenmenge bedarf es geschulten Personals – eines *IT-Forensikers*.

Forensik

Die deutschsprachige Seite der Online-Enzyklopädie Wikipedia beschreibt den allgemeinen Begriff *Forensik* als 'Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen z.B. kriminelle Handlungen systematisch untersucht werden. Der Begriff stammt vom lateinischen *forum* „Forum, Marktplatz", da Gerichtsverfahren, Untersuchungen, Urteilsverkündungen sowie der Strafvollzug im antiken Rom öffentlich und meist auf dem Marktplatz durchgeführt wurden.'[1].

Forensic science

Diese Beschreibung von Forensik ist mittlerweile ganz passend, da kriminelle Handlungen nur beispielhaft erwähnt werden (das war in früheren Wikipedia-Darstellungen anders). Die englischsprachige Seite von Wikipedia verwendet folgende Beschreibung: 'Forensic science is the application of science to criminal and civil laws. Forensic scientists collect, preserve, and analyse scientific evidence during the course of an investigation.'[2] Diese Begriffsklärung ist allgemeiner, sie führt den Begriff der forensischen Wissenschaft auf den etablierten Begriff der wissenschaftlichen Methodik zur Untersuchung von Begebenheiten der Vergangenheit zurück. Und Forensik findet im Kontext des Rechts statt. Das trifft unser Verständnis der Forensik schon ganz gut.

Definition des BSI

Etwas spezieller für IT-Forensik beschreibt das BSI den Begriff *IT-Forensik* so, dass es darum geht, strafbare bzw. anderweitig rechtswidrige oder sozialschädliche Handlungen nachzuweisen und aufzuklären, indem digitale Spuren gerichtsverwertbar gesichert und ausgewertet werden[3]. Die Ziele einer solchen Ermittlung sind nach einem Systemeinbruch oder einem anderen Sicherheitsvorfall in der Regel,

- die Identifikation der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,
- die Ermittlung des entstandenen Schadens,
- die Identifizierung der Täter/Angreifer und
- die Sicherung der Beweise für weitere juristische Aktionen.

Eine Frage des Rechts

Letztlich geht es bei einer forensischen Untersuchung stets darum, eine Frage des Rechts im Zusammenhang mit einer zurückliegenden Begebenheit zu beantworten. Es soll also eine Zeitreise in die Vergangenheit unternommen werden, um

[1] de.wikipedia.org, abgerufen am 11.04.2016
[2] en.wikipedia.org, abgerufen am 11.04.2016
[3] https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m06/m06126.html

eine juristische Frage zu klären. Zur Beantwortung werden dann erprobte wissenschaftliche Methoden unterschiedlicher Fachdisziplinen herangezogen, so dass der Begriff Forensik viele Teilgebiete umfasst. Einige Beispiele sind:

- *Forensische Medizin / Rechtsmedizin*: im Zusammenhang mit einer vermuteten nicht-natürlichen Todesursache eines Menschen ist eine typische Fragestellung, wann und warum der Tod der Person eingetreten ist. Dazu führt der Rechtsmediziner im Auftrag eines Rechtsorgans (z.B. Staatsanwaltschaft, Gericht) eine Autopsie (Leichenschau) durch. Durch den Zeitpunkt des Todes können dann weitere Fragen gestellt werden, z.B. ob eine verdächtige Person zu diesem Zeitpunkt ein Alibi vorweisen kann oder nicht.
- *Forensische Toxikologie*: als interdisziplinäres Gebiet zwischen Pharmakologie, Medizin, Chemie und Biologie führt der Rechtsmediziner oft auch toxikologische Untersuchungen durch. Eine mögliche Fragestellung ist, ob ein unnatürlicher Tod durch eine Vergiftung herbeigeführt wurde und falls ja, durch welche Stoffe. Eine andere typische Frage beschäftigt sich mit der Schuldfähigkeit eines Angeklagten, z.B. ob dieser auf Grund von Drogenmissbrauchs zu einem bestimmten Zeitpunkt überhaupt bewusst handlungsfähig war.
- *Ballistik*: im Zusammenhang mit forensischen Fragestellungen bezeichnet die Ballistik die Untersuchung von Geschossen. Eine typische Aufgabe der Ballistik ist die Beantwortung der Frage, ob ein an einem Tatort gefundenes Geschoss zu einer bereits bekannten Waffe passt. Dadurch kann der Ermittler dann die Zuordnung zu einer bestimmten Person (etwa dem Eigentümer der Waffe) oder zu anderen Verbrechen vornehmen, die mit der gleichen Waffe begangen wurden. Die Ballistik ist eine klassische Aufgabe der Kriminalistik und wird oft von Kriminaltechnikern innerhalb einer Strafverfolgungsbehörde durchgeführt.
- *Daktyloskopie*: Lehre vom Identitätsnachweis mittels Fingerabdruckverfahren. Die Daktyloskopie nutzt die allgemein akzeptierte Meinung aus, dass der menschliche Fingerabdruck individuell ist, d.h. wir können (praktisch) eindeutig von einem Fingerabdruck auf die zugehörige Person schließen. Dahinter steckt die Annahme, dass die Wahrscheinlichkeit, zwei verschiedene Personen mit dem gleichen Fingerabdruck zu finden, praktisch vernachlässigbar ist.
- *IT-Forensik / Computerforensik*: diese Disziplin hat sich innerhalb der Informatik entwickelt. Sie beantwortet Fragen des Rechts, wenn IT-Systeme Ziel oder Tatmittel in einer forensischen Untersuchung sind. Ein IT-System kann dabei ein Computer eines Endanwenders sein (z.B. um die Frage zu beantworten, ob auf dem Computer kinderpornographische Schriften gespeichert oder gar verbreitet wurden), ein Server (z.B. weil dieser kompromittiert wurde, um Malware auszuliefern) oder ein Smartphone (z.B. um Kontakte eines Beschuldigten zu extrahieren oder ein Bewegungsprofil von diesem zu erstellen).

IT-Forensik vs. Computerforensik

Während vor einigen Jahren noch der Begriff 'Computerforensik' als Standardbegriff verwendet wurde, so ist dieser auf Grund der wachsenden Bedeutung von mobilen Geräten wie Smartphones oder Tablets mittlerweile zu speziell. Außerdem erfasst Computerforensik nicht die Teilgebiete Netzwerkforensik oder Cloudforensik. Daher bevorzugen wir den allgemeineren Terminus *IT-Forensik* oder *digitale Forensik*. Diese beiden Begriffe verwenden wir synonym.

Spur = hinterlassenes Zeichen

Ausgangspunkt einer forensischen Untersuchung ist eine *Spur*. Dieser Begriff ist auch gebräuchlich in anderem Zusammenhang, z.B. bei Tieren. Nimmt ein Hund eine Spur auf, so meint man damit, dass er eine Fährte gefunden hat, um etwa ein anderes Tier zu verfolgen. Ähnlich ist die Bedeutung in der Forensik. Für unsere

Zwecke bedeutet Spur, dass wir ein *hinterlassenes Zeichen* gefunden haben, das Ausgangspunkt für eine Untersuchung ist (z.B. ein roter Fleck an einem Tatort (mutmaßlich ein Blutfleck), ein Abdruck in einem Blumenbeet (mutmaßlich ein Schuhabdruck) oder eine Bilddatei auf einem Computer). Spuren im kriminalistischen Sinne sind also Gegenstände oder Hinweise im Rahmen einer Untersuchung, die eine Theorie über einen Vorgang bestätigen oder widerlegen können. Spuren unterteilt man in *materielle Spuren* sowie *immaterielle Spuren*:

Materielle Spuren

- *Materielle Spuren* sind physische Spuren und daher gegenständlich. Typische Beispiele für materielle Spuren sind Fingerabdrücke, Schuhabdrücke, Haare, DNA-Spuren oder Kleiderfasern.

Immaterielle Spuren

- *Immaterielle Spuren* sind nicht gegenständlich. Sie ergeben sich daher aus anderen Quellen. Ein typisches Beispiel einer immateriellen Spur ist das menschliche Verhalten, zum Beispiel weil eine verdächtige Person sich im Rahmen einer Vernehmung auffällig verhält oder sich in Widersprüche verstrickt.

Digitale Spuren

Digitale Spuren sind Hinweise im Zusammenhang mit einem IT-System. Eine digitale Spur kann zum Beispiel eine Datei sein, etwa die History-Datei eines Browsers, aus der sich Informationen über das Surfverhalten eines Nutzers des Computers ergeben. Interessant ist die Frage, ob man digitale Spuren auch zu den materiellen Spuren zählt, denn digitale Spuren erfordern eine Interpretation der materiell gespeicherten Bits und Bytes.

Indiz = gewürdigte Spur

Während bei einer Spur noch unklar ist, inwiefern eine Frage des Rechts damit beantwortet werden kann oder nicht, so versteht man unter einem *Indiz* einen Hinweis, der bereits gewürdigt und damit bewertet wurde in dem Sinne, dass er eine Hypothese bestätigt. Beispielsweise liegt ein Indiz vor, wenn ein am Tatort gesicherter Schuhabdruck mutmaßlich zu einem Schuh des Verdächtigen gehört. Durch eine Bewertung lässt ein Indiz zusammen mit anderen Indizien auf das Vorliegen eines Sachverhalts schließen. Damit ist die Zeitreise in die Vergangenheit *mutmaßlich* bzw. *vermutlich* geglückt. Das Adverb *mutmaßlich* bzw. *vermutlich* bringt zum Ausdruck, dass Indizien eine Hypothese stützen, nicht aber beweisen können.

Beweis

Der stärkste Begriff in diesem Zusammenhang ist der eines *Beweises*, denn ein Beweis bezeichnet die Feststellung eines Sachverhalts als Tatsache in einem Gerichtsverfahren aufgrund richterlicher Überzeugung. Damit wird zumindest juristisch die Wahrheit ermittelt. Inwiefern es sich dabei auch um die tatsächliche Wahrheit handelt, ist dabei unerheblich.

Untersuchungsziele, Integrität von Spuren

Die Ziele einer forensischen Untersuchung sind das Identifizieren, Sicherstellen, Vorverarbeiten, Selektieren, Analysieren und Korrelieren von Spuren, die im weiteren Verlauf der Ermittlungen zu Indizien und Beweisen werden können. Dabei soll der Forensiker so wenig wie möglich in den Untersuchungsgegenstand eingreifen. Grundsätzlich gilt das Paradigma der *Integrität von Spuren*, also der Unveränderheit des Untersuchungsgegenstandes. Im Bereich der IT-Forensik bedeutet das beispielsweise bei der Untersuchung einer Festplatte, dass diese unverändert bleiben muss. Dazu haben sich geeignete Methoden etabliert, die wir ausführlich in diesem Modul beschreiben werden. In einigen Bereichen der IT-Forensik ist es aber nicht möglich, den Untersuchungsgegenstand während der IT-forensischen Untersuchung nicht zu verändern, z.B. im Bereich der Smartphone-, Hauptspeicher- oder Netzwerkforensik. Dann gilt es, minimalinvasiv in das System einzugreifen und jeden Untersuchungsschritt zu dokumentieren, um die durch den IT-Forensiker durchgeführten Veränderungen später nachvollziehen zu können.

Dokumentation

Überhaupt ist Dokumentation eine der wichtigsten Tätigkeiten eines Forensikers, um gegenüber Dritten jeden Schritt von der Sicherstellung von Spuren über die Datenakquise bis zum Analyseergebnis nachzuweisen.

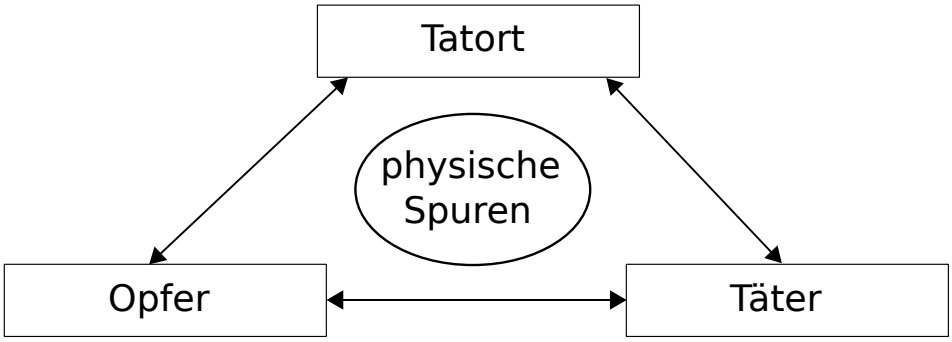
Chain of Custody

Eine wichtige Aufgabe der Dokumentation ist die Darstellung, wer wann wie auf Spuren zugreifen konnte. Unter dem Begriff *Chain of Custody* versteht man diese Dokumentation über Spuren bzw. Indizien. Im Deutschen bedeutet dieser Begriff *Aufbewahrungskette*.

Locardsches Austauschprinzip

Schon immer treibt die Menschen die Frage um, ob es das 'perfekte Verbrechen' gibt. Für die reale physische (also nicht-digitale) Welt gibt der französische Kriminologe und Forensiker Edmond Locard die Antwort. Er formulierte 1920 das *Locardsche Austauschprinzip*, wonach es immer zu einem Austausch von Spuren zwischen Täter, Opfer und Tatort kommt, d.h. sowohl Täter als auch Opfer bringen etwas zum Tatort hin, nehmen etwas mit und tauschen untereinander Spuren aus (siehe Abbildung 1.1).

Abb. 1.1: Das Locardsche Austauschprinzip



Zitat zum Austauschprinzip

Locard beschreibt sein Austauschprinzip wie folgt: *Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value.*

Digitales Austauschprinzip?

Dieses axiomatische Prinzip von Locard gilt aber nur für die physische Welt, es besagt damit, dass es das perfekte Verbrechen bei klassischen, nicht-digitalen Taten nicht gibt, sondern dass die Aufklärung am Nichtentdecken von Spuren scheitert. Die Übertragung auf digitale Taten ist nicht einfach, vermutlich gilt das Locardsche Austauschprinzip aber auch in der IT-Forensik.

Arbeitgeber

Die wachsende Bedeutung der IT-Forensik spiegelt sich auch in einem immer breiteren Angebot an Arbeitgebern wider. Typische Arbeitsplätze eines IT-Forensikers sind neben Strafverfolgungsbehörden wie dem Bundeskriminalamt (BKA), den Landeskriminalämtern (LKA) und Polizeipräsidien auch immer mehr spezialisierte IT-Forensikunternehmen. Weiterhin unterhalten die großen Wirtschaftsprüfungsgesellschaften wie Ernst&Young, Deloitte, PricewaterhouseCoopers oder KPMG eigene IT-Forensik-Abteilungen, die typischerweise bei Wirtschaftskriminalität zum Einsatz kommen. Insbesondere Alexander Geschonneck von KPMG

gilt als einer der Pioniere der IT-Forensik im deutschsprachigen Raum. Schließlich arbeiten IT-Forensiker auch als unabhängige Sachverständige.

Kontrollaufgabe 1.1: Definition Forensik

Erläutern Sie den Begriff *Forensik* und nennen Sie drei forensische Teildisziplinen.

K

Kontrollaufgabe 1.2: Spuren, Indizien, Beweise

Erläutern Sie den Unterschied zwischen Spuren, Indizien und Beweisen.

K

Kontrollaufgabe 1.3: Locardsche Austauschprinzip

Was besagt das Locardsche Austauschprinzip?

K

Studienbrief 2 Grundlagen der digitalen Forensik

2.1 Lernziele

Nach der Durcharbeitung dieses Studienbriefs besitzen Sie allgemeine theoretische Kenntnisse der Forensik sowie insbesondere der digitalen Forensik. Sie verstehen den Unterschied zwischen physischen sowie digitalen Spuren und die Problemstellungen der Interpretation digitaler Spuren. Sie können Vor- und Nachteile digitaler Spuren bewerten und klassifizieren.

2.2 Advance Organizer

In diesem Kapitel lernen Sie Grundlagen der digitalen Forensik kennen. Wir beginnen in Abschnitt 2.3 mit allgemeinen forensischen Grundlagen zum Ermittlungsprozess. Anschließend legen wir in Abschnitt 2.4 den Fokus auf die digitale Forensik sowie digitale Spuren. In Abschnitt 2.5 übertragen wir das Locardsche Austauschprinzip auf digitale Spuren. Die Vor- bzw. Nachteile digitaler Spuren im Vergleich zu analogen Spuren betrachten wir in Abschnitt 2.6. Danach lernen Sie mit der Post-Mortem- sowie Live-Forensik in Abschnitt 2.7 die beiden zentralen Vorgehensweisen der digitalen Forensik kennen. Wir schließen dieses Grundlagenkapitel mit Darstellungen von Datenstrukturen in Abschnitt 2.8 ab.

2.3 Forensische Grundlagen

Ausgangspunkt ist Frage des Rechts

In Kapitel 1 haben Sie kennengelernt, dass Forensik die Beantwortung von Fragen des Rechts durch wissenschaftliche Methoden einer wissenschaftlichen Teildisziplin bedeutet. Ohne einen Rechtsrahmen gibt es keine Frage des Rechts und damit auch keine Forensik. Wichtige forensische Teildisziplinen haben wir in Kapitel 1 erläutert, zum Beispiel forensische Medizin, Ballistik, Daktyloskopie oder digitale Forensik.

Übersetzung rechtliche Frage in forensische Frage

Die Antwort auf eine Frage des Rechts dient typischerweise dazu, ein rechtswidriges Verhalten zu belegen oder zu widerlegen. In der Forensik geht es dann darum, die Frage des Rechts in passende wissenschaftliche Fragen zu übertragen und diese wissenschaftlichen Fragen mittels wissenschaftlich akzeptierter Methoden zu beantworten. Diese Antworten sind dann im wissenschaftlichen Sinn richtig, inwiefern sie zur Beantwortung der zugrundeliegenden Frage des Rechts beitragen, ist aber Aufgabe der Ermittler (z.B. Strafverfolger, interne Ermittler, Gerichte). Beispiel 2.1 stellt dies für Blutspuren in einem nicht-natürlichen Todesfall dar.

B

Beispiel 2.1: Übersetzung rechtliche Frage in forensische Frage

Als Beispiel sei die Frage des Rechts erwähnt, ob ein Beschuldigter tatsächlich den ihm vorgeworfenen Mord begangen hat – also die Schuldfrage am Tod zu klären. Im Rahmen des Ermittlungsverfahrens werden mutmaßlich Blutspuren am Beschuldigten sichergestellt. Die rechtliche Schuldfrage wird übersetzt in die Frage an die forensische Medizin, ob die mutmaßlichen Blutspuren am Beschuldigten tatsächlich Blutspuren sind und falls ja, ob sie vom Opfer stammen. Nehmen wir an, die Antwort der forensischen Medizin lautet jeweils 'ja', d.h. der Beschuldigte trägt Blutspuren des Opfers. Ob der Beschuldigte aber tatsächlich der Täter ist, ergibt sich nicht alleine aus dieser Antwort.

Entstehung von Spuren

Grundlegende Begriffe im Kontext der Forensik wie Spuren, Indizien sowie Beweise kennen Sie aus Kapitel 1. Unter einer Spur verstehen wir ein *hinterlassenes*

Zeichen. Eine Spur kann eine materielle oder eine immaterielle Spur sein. In der klassischen Forensik sind typische Beispiele für eine materielle Spur ein Fuß- oder Schuhabdruck, Haare, Hautpartikel, Blut, Kleiderfasern bzw. ein Kleidungsstück, ein Messer oder eine Pistole. Da unsere Realität aus praktisch beliebig vielen Spuren besteht, müssen im Rahmen der Ermittlung die für die Beantwortung der zugrundeliegenden Frage des Rechts relevanten Spuren identifiziert werden.

Behandlung von Spuren

Um die richtige Antwort auf die Frage des Rechts zu geben, gibt es Anforderungen an die Behandlung von Spuren:

Spurensicherung

- Zunächst muss der Ermittler am Tatort nach solchen Spuren suchen, die im Zusammenhang mit der aufzuklärenden Tat stehen. Interessant für die Ermittlung sind solche Spuren, die unbeabsichtigt durch den Täter hinterlassen werden, z.B. weil er sie nach dem Locardschen Austauschprinzip nicht vermeiden kann. Die relevanten Spuren müssen *unverändert* gesichert werden (bitte denken Sie an das forensische Prinzip der Integrität von Spuren aus Kapitel 1). Das ist eine schwierige Aufgabe, die eine spezielle Ausbildung und Erfahrung voraussetzt. Der Vorgang der Sicherung von Spuren wird daher von den Spezialisten der *Spurensicherung* durchgeführt.

Spurenanalyse, KTU

- Aus Kapitel 1 wissen Sie, dass ein Indiz eine gewürdigte Spur ist, also im Rahmen der Ermittlung als für die Tat relevant eingestuft wurde. Diese Einstufung geschieht im Rahmen der *Spurenanalyse*. Auch die Spurenanalyse erfordert Spezialwissen und Erfahrung, sie geschieht typischerweise in speziellen Laboren. In Strafverfolgungsbehörden hat sich das Kürzel KTU für *kriminaltechnische Untersuchung* zur Bezeichnung der Spurenanalyse durchgesetzt.

Beweismittel

- Kann eine Spur eine Hypothese über den Tathergang stützen oder widerlegen, bezeichnen wir im Rahmen dieses Moduls diese Spur als *Indiz*. In der Literatur finden Sie oft auch den Begriff *Beweismittel* für unseren Begriff Indiz. Bitte beachten Sie, dass ein Beweismittel in jedem Fall von einem Beweis in unserem Sinne als Feststellung der legalen Wahrheit zu unterscheiden ist.

Rekonstruktion einer Tat

Spuren spielen die zentrale Rolle zur Rekonstruktion eines Tathergangs. Es ist die Aufgabe eines Ermittlers, eine Menge von Hypothesen über mögliche Tathergänge zu formulieren und diese jeweils mit den im Rahmen der Spurensicherung gesicherten und im Rahmen der KTU bewerteten Spuren abzugleichen, d.h. ob die jeweilige Hypothese durch die Spuren bestätigt oder widerlegt wird.

Ereignis

Nach dem Locardschen Austauschprinzip kommt es zum Austausch von Spuren zwischen Täter, Opfer und Tatort (siehe Abbildung 1.1). Allgemeiner bezeichnet man in der Kriminalistik die Feststellung der Tatsache, dass zwei Objekte miteinander in Kontakt standen, als *Ereignis*. Zum Beispiel bedeutet ein Fingerabdruck einer Person auf einem Türgriff, dass beide Objekte (Person und Türklinke) in Kontakt standen und die Person daher in dem entsprechenden Raum war.

Assoziation

Der Weg im Rahmen der Ermittlung, das Ereignis festzustellen, heißt *Assoziation*. Eine Assoziation besteht zum Beispiel darin, einen Fingerabdruck auf der Türklinke zu entdecken, zu sichern und dem Verdächtigen zuzuordnen. Wichtig für eine Assoziation ist die Erkennungs- bzw. die Irrtumswahrscheinlichkeit, also mit welcher Wahrscheinlichkeit eine Zuordnung zutrifft bzw. falsch ist. Oft gibt es kaum wissenschaftliche belastbare Aussagen zu diesen Wahrscheinlichkeiten.

Feststellung eines Ereignisses

Um ein Ereignis als Ergebnis einer Assoziation festzustellen, sind einige Schritte notwendig. Diese sind in Abbildung 2.1 dargestellt, wir erläutern sie kurz. Im oberen Teil von Abbildung 2.1 sehen Sie die Menge aller Objekte an einem Tatort.

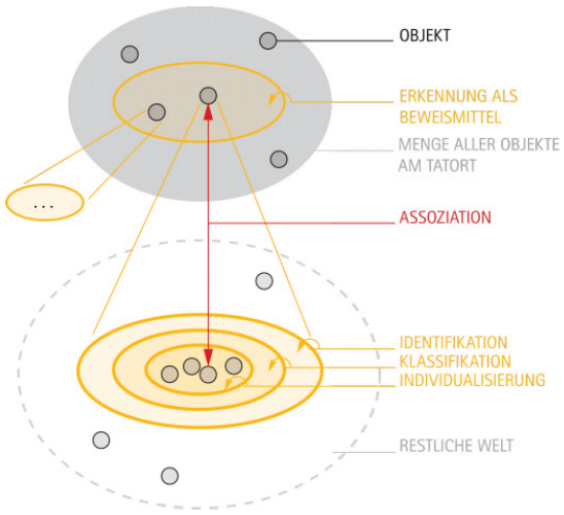


Abb. 2.1: Weg zur Assoziation

Zunächst muss der Ermittler aus dieser Menge alle Spuren erkennen, die relevant für den Fall sind, also als Beweismittel in Betracht kommen. Die Menge der möglichen Beweismittel ist im oberen Teil der Abbildung gelb umrandet.

Drei Schritte zur Assoziation

Im unteren Teil von Abbildung 2.1 sehen Sie dann für ein Beweismittel die drei Schritte zur Assoziation:

Identifikation

1. Der erste Schritt besteht in der *Identifikation* der Spur. Bei der Identifikation wird festgestellt, worum es sich vermutlich bei der Spur handelt und festgestellt, ob diese zur Klärung der Frage des Rechts relevant sein könnte. Zum Beispiel erkennt ein Ermittler rote Flüssigkeit auf dem Fußboden eines Tatorts und vermutet, dass es sich um Blutspuren handelt. Daher wird die rote Flüssigkeit durch die Spurensicherung gesichert.

Klassifikation

2. Im zweiten Schritt wird die Spur *klassifiziert*. Dabei wird konkret festgestellt, zu welcher Klasse von Objekten die Spur gehört. Im eben genannten Beispiel stellt die KTU fest, dass es tatsächlich um Blut handelt.

Individualisierung

3. Im dritten und letzten Schritt erfolgt die *Individualisierung* der Spur. Dabei wird die Spur einer konkreten Referenz zugeordnet, zum Beispiel die gesicherte Blutspur zu einer bestimmten Person.

7 W-Fragen

Ermittler nutzen zentrale, allgemeine Fragestellungen der Kriminalistik zur Rekonstruktion eines Tathergangs. Das sind die berühmten sieben W-Fragen („7 W's") der Kriminalistik, die wir nur verkürzt angeben:

- Wer?
- Was?
- Wo?
- Wann?
- Womit?
- Wie?
- Weshalb?

Legalität der Untersuchung

Bei forensischen Untersuchungen müssen einige rechtliche Aspekte von den Ermittlern eingehalten werden. Oft ist im Rahmen eines Strafverfahrens eine richterliche Anordnung notwendig zur Sicherung von Spuren, zum Beispiel im Rahmen einer

Hausdurchsuchung Ähnlich verhält es sich auch bei unternehmensinternen Untersuchungen, beispielsweise zur Aufklärung von wirtschaftskriminellen Delikten wie Datendiebstahl oder Korruption. Bei solchen Untersuchungen sollte bereits vorher der rechtliche Rahmen, wie etwa Datenschutzgesetze, geklärt werden, damit aufgefundene Beweise nicht ihre Verwertbarkeit verlieren[1]. Als Vorbereitung für forensische Untersuchungen ist es daher unerlässlich, die Vorgehensweise und die zu verwendenden Methoden auf ihre Legalität hin zu prüfen.

Anforderungen an den Ermittlungsprozess

Damit die Resultate einer forensischen Untersuchung als Beweise vor Gericht oder anderen Auftraggebern verwendet werden können, ist also eine gründliche und sorgfältige Vorgehensweise nötig. An einen Ermittlungsprozess werden die folgenden Anforderungen gestellt [11, 10]:

- **Akzeptanz**: Bei der Untersuchung sollen Verfahren und Methoden eingesetzt werden, die in der Fachwelt beschrieben und allgemein akzeptiert sind. Bei Einsatz von neuen Verfahren oder Methoden muss ein Nachweis über die korrekte Funktionsweise erbracht werden.
- **Glaubwürdigkeit**: Die Robustheit und Funktionalität der eingesetzten Methoden und Verfahren muss sichergestellt oder bewiesen werden.
- **Wiederholbarkeit**: Durch Anwendung der gleichen Verfahren, Methoden und Hilfsmittel durch Dritte müssen, ausgehend vom selben Ausgangsmaterial, die gleichen Ergebnisse erzielt werden.
- **Integrität**: Während einer Untersuchung dürfen Spuren weder bewusst noch unbewusst geändert werden. Die Integrität und die Sicherung der Integrität der digitalen Beweise muss dokumentiert werden und zu jeder Zeit belegbar sein.
- **Ursache und Auswirkungen**: Mit den verwendeten Verfahren und Methoden muss es möglich sein, logisch nachvollziehbare Beziehungen zwischen Ereignissen, Beweismitteln und Personen herzustellen.
- **Dokumentation**: Während der Ermittlung müssen alle Arbeitsschritte angemessen und detailliert dokumentiert werden.
- **Authentizität**: Es muss gewährleistet werden, dass zum einen das Vorgehen der Ermittler und zum anderen die erhobenen und gewonnenen Daten authentisch sind. Dazu müssen alle Arbeitsschritte der forensischen Untersuchung sowie die daraus gewonnen Erkenntnisse dokumentiert werden.
- **Lückenlosigkeit**: Der Verbleib der digitalen Spuren und der Ergebnisse muss ab dem Zeitpunkt der Erfassung lückenlos nachgewiesen werden um jederzeit potentielle Manipulationen ausschließen zu können (engl. „chain of custody“).

Prozessmodelle

Um diese Anforderungen im Rahmen einer forensischen Untersuchung einzuhalten, gibt es etablierte Beschreibungen zur Vorgehensweise bei einem Ermittlungsprozess. Diese Beschreibungen nennt man *Prozessmodelle* oder *Vorgehensmodelle*. Da wir uns für digitale Forensik interessieren und eine standardisierte Vorgehens-

[1] Ein Beispiel zur Unwirksamkeit von Spuren auf Grund der Anwendung unzulässiger Methoden finden Sie unter http://www.computer-forensik.org/blog/2012/10/05/einsatz-von-ueberwachungssoftware/#more-1303.

weise wichtig ist, widmen wir uns intensiv unterschiedlichen Prozessmodellen der digitalen Forensik in einem späteren Kapitel.

Kontrollaufgabe 2.1: Weg zur Assoziation

Nennen Sie die drei Schritte zur Assoziation und erläutern Sie diese an Hand eines Beispiels.

K

Kontrollaufgabe 2.2: Anforderungen an den Ermittlungsprozess

Nennen und erläutern Sie drei Anforderungen an den Ermittlungsprozess.

K

2.4 Digitale Forensik und digitale Spuren

Digitale Forensik

Die digitale Forensik (auch: IT-Forensik) überträgt Prinzipien und Methoden der klassischen forensischen Wissenschaften in die digitale Welt. Das zentrale Ziel ist daher die Sicherung, Aufbereitung und Analyse von digitalen Spuren in einer Weise, die in einer möglichen späteren Gerichtsverhandlung akzeptiert wird – auch wenn es wie bei internen Ermittlungen nicht immer dazu kommen muss. Die digitale Forensik ist eine noch relativ junge Wissenschaft, die erst mit der Digitalisierung von Informationen und Kommunikation entstand.

Digitale Spur

Der wesentliche Unterschied zwischen der digitalen Forensik und den klassischen forensischen Wissenschaften besteht in der Art der Spuren. Während in den klassischen Wissenschaften digitale Spuren unbekannt sind, stehen sie in einer IT-forensischen Untersuchung im Mittelpunkt. Daher steht der Begriff der digitalen Spur im Mittelpunkt dieses Abschnitts.

Aufbau dieses Abschnitts

Abschnitt 2.4 ist wie folgt aufgebaut: in Abschnitt 2.4.1 geben wir zunächst eine kurze Einführung für den Begriff „digitale Spur“ und erläutern den Zusammenhang zu physischen Spuren. Wir betrachten auch, wo digitale Spuren entstehen. Anschließend betrachten wir in Abschnitt 2.4.2 Eigenschaften und Klassifikationen digitaler Spuren, insbesondere die Unterscheidung in *vermeidbare* sowie *unvermeidbare* Spuren. Zum Abschluss fassen wir in Abschnitt 2.4.3 die speziellen Praktiken der digitalen Forensik zusammen, die sich aus den allgemeinen Anforderungen an den Ermittlungsprozess ergeben.

2.4.1 Digitale Spuren

Definition nach Casey

Nach der Definition von Eoghan Casey basieren digitale Spuren auf Daten, die in Computersystemen gespeichert sind oder zwischen Computersystemen übertragen werden [8]. Digitale Spuren basieren immer auf physischen Spuren, beispielsweise der Magnetisierung einer Festplatte, dem Ladezustand von Transistoren im flüchtigen Speicher oder elektromagnetischen Wellen auf Kabeln. Dies bedeutet, dass zuerst physische Spuren gefunden werden müssen, bevor man weiter nach digitalen Spuren suchen kann. Durch die enge Bindung von physischen und digitalen Spuren können auch die Prinzipien der klassischen Forensik auf die digitale Forensik übertragen werden.

Wo entstehen digitale Spuren?

Bei der Datenverarbeitung in IT-Systemen fallen überall digitale Spuren an. Es ist quasi nicht möglich, mit einem IT-System zu interagieren, ohne digitale Spuren zu hinterlassen. Beispielsweise werden schon beim Einschalten des Geräts digitale Spuren hinterlassen, wie etwa Zeitstempel im Dateisystem, Logdateien des Betriebssystems oder durch Laden von Daten in den Arbeitsspeicher. Digitale Spuren

entstehen an verschiedenen Stellen, die wir zunächst in *lokale digitale Spuren* sowie *nicht-lokale digitale Spuren* untergliedern (eine weitere Unterteilung nehmen wir in Abschnitt 2.4.2 vor):

Lokale digitale Spuren

1. **Lokale digitale Spuren** entstehen auf dem Gerät selbst, sie können durch die Analyse des Geräts gesichert und analysiert werden. Als Gerät kommen dabei IT-Systeme oder Datenträger in Frage, also etwa ein Computer, ein Smartphone, eine Digitalkamera oder Datenträger wie USB-Sticks, SD-Karten, DVDs oder CDs. Beispiele für lokale digitale Spuren sind:
   - Inhaltsdaten einer Datei (z.B. doc-Datei, sqlite-Datei)
   - Dateisystem (z.B. Zeitstempel, Journal)
   - Dateinamen
   - 'Komfortdaten' von Applikationen (z.B. Browser-History, Browser-Cache, 'recently used')
   - Windows-Registry
   - Log-Dateien (von lokalen Diensten)
   - Temporäre Dateien
   - Lokale Daten von Diensten (z.B. soziale Netzwerke, Instant Messenger)
   - Backups

Nicht-Lokale digitale Spuren

2. **Nicht-lokale digitale Spuren** entstehen nicht auf dem Gerät selbst, sie fallen an einem anderen Ort an, also etwa bei einem Dienst (Webserver, Mailserver, soziales Netzwerk), in der Cloud, dem Internet Service Provider (ISP) oder dem Mobilfunkanbieter. Beispiele für nicht-lokale digitale Spuren sind:
   - Verkehrsdaten bei Internet Service Provider
   - Inhaltsdaten bei Online-Speicherdiensten
   - Daten bei Diensten (z.B. soziale Netzwerke, Suchmaschinen, Bahn, Buchungsanbieter wie HRS oder fluege.de)
   - Firewalls
   - SIEM (Security Information and Event Management)
   - Digitale Überwachungskamera (CCTV)
   - Geldausgabeautomat
   - Daten des Mobilfunkanbieters (Abrechnungsdaten, Standortdaten)

Interpretationsebenen

Digitale Spuren können nicht ohne Weiteres aus den zugehörigen physischen Spuren vom Menschen gelesen und verstanden werden, stattdessen müssen die zugehörigen physischen Spuren mit Hilfe von forensischen Werkzeugen oder anderen Anwendungen interpretiert werden. Erst nach der Interpretation durch diese Werkzeuge kann ein Ermittler die digitalen Daten verstehen und einschätzen. In IT-Systemen ist es üblich, dass mehrere Interpretationsebenen durchlaufen werden müssen. Dies soll anhand von Beispiel 2.2 und Abbildung 2.2 für eine Bilddatei kurz erläutert werden.

B

Beispiel 2.2: Interpretationsebenen einer digitalen Spur

Wir erläutern die Interpretationsebenen einer digitalen Spur aus Abbildung 2.2 für eine Bilddatei. Auf der untersten Ebene befindet sich die physi-

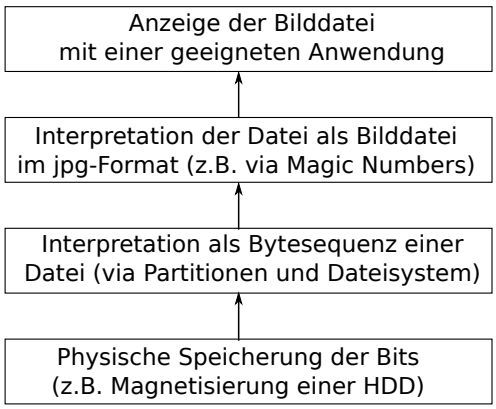


Abb. 2.2: Beispiel für Interpretationsebenen: Bilddatei

sche Spur als gespeicherte Bits auf dem Datenträger (z.B. die Magnetisierung einer HDD, der Ladezustand eines Transistors). Die für die betrachtete Datei relevanten Bits müssen durch unterschiedliche Interpretationswerkzeuge in die richtige Reihenfolge der Bytes der Bilddatei transformiert werden. Typischerweise muss dazu das Partitionsschema des Datenträgers bestimmt werden, in der betroffenen Partition das Dateisystem. Mit Hilfe von Informationen aus dem Dateisystem kann dann die richtige Bytesequenz der Bilddatei bestimmt werden. Im nächsten Schritt wird die Datei als Bilddatei im jpg-Format identifiziert, zum Beispiel durch die ersten charakteristischen Bytes der Datei, die sogenannten Magic Numbers. Zuletzt nutzt der Ermittler eine geeignete Anwendung, um den Inhalt der Bilddatei menschenlesbar auf dem Bildschirm anzuzeigen und damit die zugehörige digitale Spur.

Fehlinterpretation

Der Ermittler selbst sieht nicht die physischen Spuren, sondern lediglich deren Interpretationen. Bei jeder Interpretation zwischen zwei Ebenen können Fehlinterpretationen entstehen, welche für den Ermittler nicht direkt erkenntlich sind. Der Ermittler muss sich hier in der Regel auf die korrekte Funktionsweise der Werkzeuge verlassen (z.B. weil diese allgemein als zuverlässig gelten) oder diese in aufwändigen Verfahren für jede Ebene selbst nachprüfen.

2.4.2 Klassifikation digitaler Spuren

Klassifikationsschemata

In Abschnitt 2.4.1 haben Sie bereits die Unterscheidung digitaler Spuren in die beiden Kategorien *lokale digitale Spuren* bzw. *nicht-lokale digitale Spuren* kennengelernt. In diesem Abschnitt verfeinern wir diese Kategorisierung, indem wir Spuren zunächst nach zwei Klassifikationsmerkmalen unterscheiden, und zwar nach der *Entfernung zum Tatort* sowie nach der *Flüchtigkeit der Spur* [9]. Nachfolgend führen wir gemäß Brian Carrier [7] die Unterscheidung digitaler Spuren in die beiden Kategorien *vermeidbar* bzw. *unvermeidbar* ein. Die drei Klassifikationsschemata sind unabhängig voneinander zu betrachtende Eigenschaften, zum Beispiel gibt es unvermeidbare, lokale, nicht-flüchtige Spuren (etwa die Partitionierung eines Datenträgers). Mögliche weitere Klassifikationen (z.B. eine Einteilung nach zugehörigen Delikten) nehmen wir hier nicht vor.

Entfernung zum Tatort und Flüchtigkeit digitaler Spuren

Entfernung zum Tatort

Anders als in den klassischen forensischen Wissenschaften kann ein Cybertäter digitale Spuren an Orten hinterlassen, an denen er physisch nie anwesend war. In der Cybersicherheit werden viele Delikte über digitale Netzwerke wie dem Internet begangen. Vom heimischen Computer aus können Täter so auch digitale Spuren

in anderen Regionen oder gar Ländern hinterlassen. Wie Dewald und Freiling [9] behaupten, nimmt die Menge der hinterlassenen relevanten Spuren vermutlich mit der Entfernung zum Tatort ab. Unter dem Tatort wird hier der Ort verstanden, von dem aus der Täter handelt. Bei der Einteilung der Entfernung vom Tatort untergliedern die Autoren grob in drei Bereiche:

1. dem Computer des Täters
2. dem lokalen Netzwerk, von dem aus der Täter agiert
3. dem externen Netzwerk (Internet) samt aller Geräte.

Dabei ist intuitiv anzunehmen, dass auf dem Computer des Täters die meisten relevanten digitalen Spuren zu finden sein werden.

Flüchtigkeit einer digitalen Spur

Die Flüchtigkeit bestimmt, wie lange Daten für eine IT-forensische Untersuchung erhalten bleiben. Je nach Speichermedium müssen IT-forensische Ermittler schnell und effektiv handeln, um Verluste digitaler Spuren zu verhindern. Dazu ist Fachwissen, Erfahrung und Vorsicht nötig – auch um unbeabsichtigte Datenmanipulationen zu vermeiden. Es wird im Wesentlichen zwischen drei Kategorien der Flüchtigkeit von Daten unterschieden [9]:

Persistente Spuren

1. **Persistente Spuren** können über eine lange Zeit hinweg auf einem Speichermedium auch ohne Stromzufuhr erhalten bleiben. Typische Vertreter dieser Kategorie sind Spuren, die auf Festplatten, CDs, DVDs, USB-Sticks oder Speicherkarten liegen. Diese Spuren sind auch nach einem langen Zeitraum noch auffindbar, weswegen eine Analyse auch zu einem späteren Zeitpunkt noch möglich ist.

Semi-persistente Spuren

2. Dagegen bleiben **semi-persistente Spuren** nur bei aktiver Stromzufuhr über einen langen Zeitraum erhalten. Wird die Stromzufuhr unterbrochen, so gehen die Spuren nach kurzer Zeit schon vollständig verloren. Um den Verlust der Spuren zu vermeiden, sollten diese Daten für eine spätere Analyse auf einen persistenten Datenträger dupliziert werden. Alternativ können diese Spuren auch bei der Sicherung des Systems im laufenden Betrieb analysiert werden. Typische Beispiele für semi-persistente Spuren sind der Arbeitsspeicher oder aktive Prozesse des Systems.

Flüchtige Spuren

3. Die dritte Kategorie sind die **flüchtigen Spuren**. Diese sind selbst bei aktiver Stromzufuhr nur für eine kurze Zeit verfügbar. Dazu zählen Inhalte von Prozessorregistern oder Netzwerkdaten auf einem Datenkabel. Diese Daten müssen im laufenden Betrieb analysiert werden oder zu einer späteren Analyse protokolliert und aufgezeichnet sowie auf einem persistenten Datenträger gesichert werden.

Order of Volatility

Die Einstufung einer digitalen Spur nach ihrer Flüchtigkeitseigenschaft ist wichtig für die Reihenfolge der Sicherung digitaler Spuren. Prinzipiell gilt, dass mögliche fallbezogene digitale Spuren mit höherer Flüchtigkeit zuerst gesichert werden sollen. Diese Reihenfolge bezeichnet man als *Order of Volatility*.

Vermeidbare und unvermeidbare Spuren

Technisch vermeidbare Spuren

In der digitalen Forensik unterscheidet man bei digitalen Spuren zwischen *technisch vermeidbaren* und *technisch unvermeidbaren digitalen Spuren*. Technisch vermeidbare Spuren werden definiert als Spuren, die um ihrer selbst Willen erzeugt wurden [6]. Dazu zählen beispielsweise Log-Dateien, Zeitstempel im Dateisystem oder Protokolldaten aus einer Firewall. Ebenso zählt auch jede Datei oder abgespeicherte E-Mail dazu [6]. Technisch vermeidbare Spuren sind leichter zu manipulieren,

so können Logdateien direkt in einem Texteditor geändert werden. Carrier [7] nennt technisch vermeidbare Spuren im Kontext von Dateisystemen auch nicht-essentielle („non-essential“) Daten. Dies sind Daten, die keine Auswirkungen auf die Funktionsweise des Dateisystems haben. Wenn jemand digitale Spuren verwischen will und Zeitstempel oder Dateien manipuliert, dann kann er das System ohne zusätzlichen Aufwand weiter nutzen. Manipulationen sind somit ohne große Kosten möglich, wodurch die Glaubwürdigkeit der Echtheit von technisch vermeidbaren Spuren in Frage gestellt werden muss.

Technisch unvermeidbare Spuren

Technisch unvermeidbare digitale Spuren sind Spuren, die unweigerlich anfallen und daher nicht durch einfache Veränderungen eines Systems vermieden werden können [6]. Dazu zählen etwa die Angabe der Clustergröße im Bootsektor eines Dateisystems oder die Angabe des physischen Speicherorts einer Datei. Beispielsweise kann ein Dateisystem nicht mehr korrekt funktionieren, wenn die Clustergröße im Bootsektor manipuliert wurde, da dadurch alle Referenzen auf Clusteradressen ungültig werden. Aber auch mit Mitteln des Betriebssystems gelöschte Dateien[2] werden zu den technisch unvermeidbaren Spuren gezählt [6]. Diese Einordnung geschieht aufgrund des hohen Aufwandes und Fachwissens, das nötig ist, um gelöschte Dateien endgültig von der Festplatte zu entfernen. Carrier [7] spricht von essentiellen („essential“) Daten eines Dateisystems, die benötigt werden, um die korrekte Funktionsweise zu gewährleisten. Wenn essentielle Daten manipuliert werden, dann funktioniert das System nicht mehr korrekt. Für jemanden, der Spuren manipulieren will, bedeutet das, dass er nach der Manipulation das System nicht mehr gewöhnlich verwenden kann, sondern die Manipulation erst wieder rückgängig machen muss, bevor das System ordnungsgemäß nutzbar ist. Dies bedeutet einen erhöhten Aufwand für Manipulationen. Des Weiteren ist für die Manipulation essentieller Daten auf Dateisystemebene ein höheres Fachwissen und die Nutzung fortgeschrittener Tools nötig, im Gegensatz zu einem einfachen Texteditor, mit dem eine Logdatei geändert werden kann.

Bezug zur Aussagekraft einer digitalen Spur

Da eine Manipulation bei technisch unvermeidbaren digitalen Spuren mit einem höheren Aufwand verbunden ist, ist die Aussagekraft dieser Spuren auch höher als bei den technisch vermeidbaren Spuren. Dies macht die unvermeidbaren Spuren für IT-Forensiker besonders vertrauenswürdig.

2.4.3 Praktiken der digitalen Forensik

Praktiken der digitalen Forensik

Basierend auf den Anforderungen an eine Untersuchung haben sich einige Praktiken im Bereich der IT-Forensik etabliert. Das Ziel ist es dabei zu verhindern, dass Beweise wegen Fehlern bei der Beweisführung vor Gericht verworfen werden müssen. Im Folgenden sind einige dieser Praktiken nach [26] aufgelistet:

- **Keine Veränderung an dem Beweismittel**: Um Manipulationen auszuschließen, ist es wichtig, dass während einer IT-forensischen Untersuchung keine Änderungen am originalen Untersuchungsobjekt erfolgen. Dazu werden Hardware-Schreibblocker benutzt, um exakte Kopien der Beweismittel anzufertigen. Die Untersuchung selbst erfolgt anschließend an einer dieser Kopien.
  In einigen Fällen, wie etwa bei einer Untersuchung an einem laufenden System oder bei einem Smartphone, kann es erforderlich sein, dass Veränderungen am Gerät herbeigeführt werden müssen, um digitale Spuren sichern zu können. In diesen Fällen müssen die Änderungen so minimal wie möglich gehalten werden, um einerseits zu vermeiden, dass digitale Spuren verloren

[2] Beim Löschen von Dateien mit Mitteln des Betriebssystems werden Dateien in der Regel nicht von der Festplatte gelöscht, sondern stattdessen werden lediglich Metainformationen im Dateisystem entfernt, wodurch die Dateien vom Dateisystem nicht mehr wiedergefunden werden können. Die Daten selbst verbleiben jedoch auf der Festplatte bis sie überschrieben werden.

gehen, und andererseits Manipulationen der Spuren ausgeschlossen werden können.

- **Dokumentation der Beweisführung**: Die gesamte Untersuchung inklusive aller verwendeter Methoden zur Beweissicherung muss ausführlich dokumentiert werden. Anhand dieser Dokumentation kann die Untersuchung zu einem späteren Zeitpunkt von Dritten nachvollzogen und auch nachgeprüft werden. Diese Reproduzierbarkeit ist ein wichtiger Faktor der Beweiswürdigung vor Gericht.
- **Dokumentation aller Veränderungen**: Auch wenn grundsätzlich keine Änderungen an einem Beweismittel vorgenommen werden sollen, lässt es sich in manchen Fällen nicht vermeiden. Beispielsweise bei der Untersuchung an einem laufenden System oder um Zugriffsrechte auf Smartphone-Speicher zu erhalten. In diesen Fällen müssen aber alle Veränderungen genauestens dokumentiert werden.
- **Verwendung einer allgemeinen Checkliste**: Zu forensischen Untersuchungen sollte eine allgemeine Checkliste verwendet werden, um zu garantieren, dass bei verschiedenen Untersuchungen stets die gleichen Wiederherstellungs- und Untersuchungsmethoden verwendet werden. Außerdem ist darauf zu achten, dass keine wichtigen Untersuchungsbestandteile vergessen werden.
- **Detaillierte Dokumentation**: Zu einer guten gerichtlichen Verwertbarkeit und Reproduktion der Untersuchung sollte eine sehr detaillierte Dokumentation vorgenommen werden. Grundsätzlich gilt, dass man lieber zu viel als zu wenig dokumentieren soll. Des Weiteren ist eine handschriftliche Dokumentation empfehlenswert.

K

Kontrollaufgabe 2.3: Digitale Spur

Definieren Sie den Begriff *digitale Spur*. Erläutern Sie dabei ebenfalls den Zusammenhang zwischen physischen und digitalen Spuren.

K

Kontrollaufgabe 2.4: Vermeidbarkeit digitaler Spuren

Erläutern Sie den Unterschied zwischen technisch vermeidbaren und unvermeidbaren digitalen Spuren.

K

Kontrollaufgabe 2.5: Klassifikation digitaler Spuren

Nach welchen Schemata lassen sich digitale Spuren klassifizieren?

2.5 Das digitale Austauschprinzip

Wiederholung

In Kapitel 1 haben Sie das Locardsche Austauschprinzip für physische Spuren kennengelernt. Danach kommt es stets zu einem Austausch zwischen Täter, Tatort und Opfer, weil die reale Welt nach Locard so komplex ist, dass Spuren immer vorhanden sind. In diesem Abschnitt diskutieren wir die Übertragung des Locardschen Austauschprinzips in die digitale Welt und formulieren abschließend das digitale Austauschprinzip.

Sehr großer Zustandsraum

Eine zentrale Eigenschaft bei Untersuchungen in der digitalen Forensik ist, dass die zu untersuchenden Geräte (beispielsweise Computer) eine sehr hohe Anzahl

möglicher Zustände besitzen. Die genaue Anzahl ist abhängig von der Größe des Speichers, je größer der Speicher desto komplexer wird ein System. Betrachten wir beispielsweise einen Hauptspeicher der Speicherkapazität 2 GiB (2^{31} Byte), so werden

$$8 \cdot 2^{31} = 2^{34} \text{ Bits} \tag{2.1}$$

dargestellt. Daraus ergeben sich insgesamt

$$2^{2^{34}} = 2^{17\ 179\ 869\ 184} \approx 10^{5 \text{ Mrd.}} \tag{2.2}$$

mögliche Zustände für den Hauptspeicher. Eine Zahl, die von herkömmlichen mathematischen Programmen gar nicht mehr ausgerechnet werden kann und stattdessen mit „unendlich“ gleichgesetzt wird. Im Vergleich dazu wird die Anzahl aller Atome im bisher bekannten Universum auf Größenordnungen von 10^{78} bis 10^{82} geschätzt [6].

Digitales Austauschprinzip

Die digitale Forensik muss sich also mit großen Zustandsräumen und sehr komplexen Systemen auseinander setzen. Allerdings kommt es einem IT-Forensiker entgegen, dass ein Großteil der möglichen Zustände nicht sinnvoll interpretierbar ist, sondern einfach sogenannten Zustandsmüll darstellt. Damit können wir das digitale Austauschprinzip in Definition 2.1 beschreiben.

Definition 2.1: Digitales Austauschprinzip

In jedem hinreichend komplexen digitalen System hinterlässt Datenverarbeitung notwendigerweise digitale Spuren.

D

Folgerung

Analog zum Locardschen Austauschprinzip für physische Spuren folgt aus dem digitalen Austauschprinzip, dass es das perfekte Cyberverbrechen nicht gibt.

2.6 Vor- und Nachteile digitaler Spuren

In diesem Abschnitt betrachten wir Vor- und Nachteile digitaler Spuren.

Vorteile

Vorteile digitaler Spuren sind wie folgt: in vielen Fällen können digitale Spuren exakt dupliziert werden, sie sind schwer zu vernichten und sie geben oft Aufschluss über einen früheren Zustand des Systems. Wir gehen auf diese Vorteile im Folgenden ein.

Exaktes Duplizieren

Bei persistenten digitalen Spuren ist exaktes Duplizieren eines Originaldatenträgers meist einfach möglich. Während die Duplikation für Festplatten, USB Sticks oder SD-Karten sehr einfach ist, ist die Duplikation von internen Speichermedien eines Smartphones nicht immer möglich. Das exakte Duplizieren bringt eine Reihe von Vorteilen im Umgang mit digitalen Spuren mit sich:

- Der originale Datenträger wird physisch geschont und kann nach der Duplizierung dauerhaft weggeschlossen bleiben. Damit sind insbesondere ungewollte Veränderungen am Beweismittel unwahrscheinlich.
- Die Übereinstimmung des Originals mit einem Duplikat kann einfach nachgewiesen werden. Typisches Hilfsmittel dazu ist eine geeignete kryptographische Hashfunktion, z.B. SHA-256.

- Eine spätere Veränderung an der Kopie wird erkannt. Sofern es keine gewollte, dokumentierte Veränderung ist, kann der IT-Forensiker erneut mit einem exakten Duplikat seine Untersuchungen beginnen.

Schwer zu vernichten

Während digitale Spuren leicht und fast permanent entstehen, ist es weitaus schwieriger, alle Spuren, die im Zuge einer bestimmten digitalen Handlung entstanden sind, wieder zu vernichten. Bereits beim Löschen von Dateien beginnen die Probleme. In der Regel werden dabei vom Dateisystem lediglich Metainformationen entfernt, so dass die Dateien vom Dateisystem nicht mehr gefunden werden können. Zusätzlich wird der Speicher wieder freigegeben und kann durch neue Daten beschrieben werden. Die Daten selbst verbleiben aber noch so lange auf der Festplatte, bis sie durch andere Daten überschrieben werden. In dieser Zeit können eigentlich gelöschte Daten potenziell (je nach Dateisystem oder Fragmentierung der Daten) wieder hergestellt werden. Des Weiteren fallen digitale Spuren an vielen Orten an, auch solchen, die der Nutzer nicht unter seiner Kontrolle hat (etwa beim Internet Service Provider). Bitte beachten Sie, dass dies eine Folgerung des digitalen Austauschprinzips aus Definition 2.1 ist.

Determinismus

Determinismus in der Informatik bedeutet, dass ein Zustand genau einen gültigen Nachfolgezustand besitzt. Viele Anwendungen, mit denen wir arbeiten, sind deterministisch. Dann kann man vom aktuellen Zustand des Systems auf vergangene Zustände schließen.

Nachteile

Nachteile digitaler Spuren sind wie folgt: Ermittler finden riesige Datenmengen vor (Datenüberlastung) und die Individualisierung einer Assoziation ist schwierig (d.h. die Verbindung einer digitalen Spur zu einer Person). Wir gehen auf diese beiden Nachteile im Folgenden ein.

Datenüberlastung

Heutige Festplatten überschreiten oft die Speicherkapazität von 1 TiB, USB Sticks sind viele GiB groß. Meist fallen mehrere Festplatten sowie USB Sticks in einer IT-forensischen Untersuchung an, so dass typischerweise mehrere TiB an digitalen Daten zu verarbeiten sind. Die Klassifikation von forensisch irrelevanten Daten (z.B. Systemdateien, nicht strafbare Bilder, ...) bzw. fallbezogen relevanten Daten kann schon an der schieren Menge von Daten scheitern. Die IT-forensische Untersuchung gleicht der sprichwörtlichen Suche nach der Nadel im Heuhaufen. Ermittler sprechen oft vom *Problem der Datenüberlastung*. Eine mögliche Lösung dieses Problems lernen Sie im Kapitel Hashfunktionen kennen.

Individualisierung einer Assoziation

Der Nachweis einer Verbindung zwischen einem Beschuldigten und einem Tathergang ist im Bereich der digitalen Forensik häufig problematisch. Es muss nachgewiesen werden, dass eine bestimmte Person eine bestimmte Handlung begangen hat, wobei ausgeschlossen werden muss, dass eine andere Person die Handlung ausgeführt hat. Wenn zum Beispiel ein Computer von mehreren Benutzern zu unregelmäßigen Zeiten gemeinsam genutzt wird, ist es schwierig, die Person ausfindig zu machen, die mit diesem Computer eine bestimmte Tat durchgeführt hat. Dies liegt daran, dass digitale Spuren nur selten Merkmale enthalten, mit denen eine reale Person eindeutig identifiziert werden kann. Beispielsweise muss eine E-Mail-Adresse nicht den Namen einer Person enthalten, was die Zuordnung erschwert. Wie hoch die Irrtumswahrscheinlichkeit bei einer Zuordnung zwischen einer Person und einer Handlung ist, hängt stark von der gegebenen Situation ab. Wenn beispielsweise mehrere Personen den gleichen Rechner benutzen können, sind effektive Authentifikationsmechanismen sehr nützlich für die Genauigkeit einer Assoziation. Durch Authentifikationsmechanismen kann eindeutig festgestellt werden, welcher Nutzer zu welcher Zeit auf dem System eingeloggt war und eine Tat

kann mit hoher Wahrscheinlichkeit einem bestimmten Nutzer zugeordnet werden. Allerdings bieten diese Verfahren auch eine Unsicherheit: Zugangsinformationen wie Passwort oder PIN können leicht weitergegeben oder gestohlen werden [6]. In der digitalen Welt ist es einfacher die Identität einer anderen Person zu stehlen, beispielsweise durch Phishing. Diese Faktoren müssen bei Assoziationen während einer Ermittlung beachtet werden.

2.7 Post-Mortem- und Live-Forensik

Bei IT-forensischen Untersuchungen unterscheidet man grundsätzlich zwischen zwei Formen von Vorgehensweisen: *Post-Mortem-* und *Live-Forensik*. Der Hauptunterschied ist folgender: Die Post-Mortem-Analyse findet typischerweise in einem IT-forensischen Labor auf einer Kopie eines sichergestellten Datenträgers statt, während die Live-Analyse an einem laufenden Computersystem (vor Ort bei der Sicherstellung) stattfindet.

Live-Forensik

Die Live-Forensik wird während des Sammelns und Sicherns von Daten vorgenommen. Dabei wird die Hard- und oft auch die Software des betroffenen IT-Systems verwendet. Dies kann beispielsweise während der Beschlagnahme eines Computers in der Wohnung des Beschuldigten geschehen. Die Voraussetzung für eine Live-Analyse ist, dass die Ermittler ein eingeschaltetes und laufendes System vorfindet. In diesem Fall ist es das Ziel des IT-Forensikers, flüchtige oder semi-persistente Spuren, die bei einer späteren Untersuchung im Labor bereits verschwunden sein werden, zu finden und zu sichern. So wird beispielsweise der Arbeitsspeicher (RAM) des Computers ausgelesen, aktive Netzwerkverbindungen protokolliert sowie geöffnete Dateien, Programme und Prozesse festgestellt. Außerdem haben die IT-Forensiker hier die Möglichkeit, potentielle Datenverschlüsselungen zu umgehen. Viele Festplattenverschlüsselungsprogramme wie etwa TrueCrypt[3] erfordern lediglich bei Systemstart die Eingabe eines Passwortes. Ist das Verschlüsselungspasswort eingegeben, so wird es im Arbeitsspeicher gesichert. Bei Zugriffen auf verschlüsselte Datenstrukturen entschlüsselt die Anwendung diese transparent für den Anwender. Wenn ein IT-Forensiker an einem laufenden System verschlüsselte Bereiche erkennt, so kann er diese häufig entschlüsselt auf ein externes Medium sichern, während es bei einer späteren Analyse im Labor vermutlich unmöglich wäre, die Verschlüsselung zu brechen. Eine Herausforderung stellt sich bei dieser Analyse aber den Ermittlern: Die Veränderungen am System müssen so minimal wie möglich ausfallen. Jede Handlung am System kann zu Änderungen im Arbeitsspeicher oder sogar an der Festplatte (z.B. bei Zeitstempeln) führen. Die Handlungen der IT-Forensiker müssen ferner genau dokumentiert werden. Erst wenn alle flüchtigen oder semi-persistenten Spuren gesichert wurden, können die Ermittler das System herunterfahren und zur weiteren Post-Mortem-Analyse ins Labor bringen.

Post-Mortem-Analyse

Bei der Post-Mortem-Analyse (lateinisch „nach dem Tod“) wird ein ausgeschaltetes System bzw. ein persistenter Datenträger analysiert. Der Umfang einer Post-Mortem-Analyse richtet sich nach dem Auftrag der Untersuchung. Der Datenträger muss gründlich untersucht werden, dies beinhaltet eine Datenträgeranalyse und eine oder mehrere Dateisystemanalysen. Je nach Untersuchungsauftrag müssen auch nicht-allozierte Bereiche gesondert betrachtet werden. Bei der Post-Mortem-Analyse muss ebenfalls verhindert werden, dass Änderungen am Datenträger vorgenommen werden. Dazu werden häufig unter Verwendung von Hardware-Schreibblockern exakte Kopien der Datenträger erstellt und die Untersuchungen an den Kopien vorgenommen. Der originale Datenträger wird dabei sicher vor unautorisierten Zugriffen aufbewahrt. Die Untersuchungen selbst müssen für eine mögliche spätere gerichtliche Verwendung genauestens dokumentiert werden. Teil

[3] http://www.truecrypt.org/

der Post-Mortem-Analyse ist auch die Untersuchung der sichergestellten flüchtigen und semi-persistenten Daten aus der Live-Analyse, wie etwa eine Kopie des Arbeitsspeichers oder sichergestellte Kopien von verschlüsselten Bereichen.

Die Post-Mortem- und die Live-Forensik stehen somit nicht in Konkurrenz zueinander, sondern sie ergänzen sich. Häufig bleiben Ermittlern die Möglichkeiten der Live-Forensik verwehrt, da sie nicht auf ein laufendes System treffen. Wenn eine Live-Analyse jedoch möglich ist, können zusätzliche Spuren gefunden und sichergestellt werden und dadurch die spätere Post-Mortem-Analyse erheblich erleichtert werden.

K

Kontrollaufgabe 2.6: Post-Mortem- und Live-Forensik

Erläutern Sie den Unterschied zwischen Post-Mortem und Live-Forensik. Nennen Sie hierzu jeweils ein anschauliches Beispiel.

2.8 Darstellungen von Datenstrukturen

Byte-String

In diesem Abschnitt betrachten wir Darstellungen unterschiedlicher Datenstrukturen, die häufig im Rahmen einer IT-forensischen Ermittlung untersucht werden. Eine Datenstruktur wird stets in einem Byte-String $B_0B_1 \ldots B_{n-1}$ der Länge n gespeichert. Dabei ist 0 die niederwertigste relative Speicheradresse der Datenstruktur und $n-1$ die höchste. Der Byte-String kann unterschiedliche Datentypen darstellen.

Ganze Zahl

Der erste Datentyp, den wir betrachten, ist eine *ganze Zahl*. Für die Darstellung einer ganzen Zahl stehen mehrere Zahlensysteme zur Verfügung. Das *Dezimalsystem* ist die übliche Darstellung einer ganzen Zahl für Menschen. Das Dezimalsystem verwendet die üblichen zehn Ziffern 0 bis 9. In der Informatik und im Speziellen in der digitalen Forensik werden Sie das Hexadezimal- und das Binärsystem besonders häufig antreffen:

Binärsystem

1. Für die Darstellung einer ganzen Zahl im *Binärsystem* stehen lediglich zwei Ziffern zur Verfügung: 0 und 1. Eine gegebene ganze Zahl wird also bezüglich der Basis 2 dargestellt. Das Binärsystem ist eine natürliche Wahl in der Informatik, weil ein Bit als Ziffer einer ganzen Zahl interpretiert wird.

Hexadezimalystem

2. Für die Darstellung einer ganzen Zahl im *Hexadezimalsystem* stehen sechzehn Ziffern zur Verfügung – die üblichen Dezimalziffern 0 bis 9 sowie die sechs weiteren Ziffern A (entspricht der ganzen Zahl 10) bis F (entspricht der ganzen Zahl 15). Eine gegebene ganze Zahl wird also bezüglich der Basis 16 dargestellt. Um anzuzeigen, dass eine Zahl im Hexadezimalsystem dargestellt wird, stellt man den Ziffern ein $0x$ voran oder hängt ein h an.

Umrechnung von Zahlensystemen

Die Umrechnung einer ganzen Zahl vom Binär- in das Hexadezimalsystem ist einfach. Sie gruppieren die Bits in Gruppen von jeweils 4 Bit und fassen diese Gruppen jeweils als eine Hexadezimalziffer auf. Ebenso einfach ist die Umrechnung vom Hexadezimal- in das Binärsystem. Jede Hexadezimalziffer wird einfach durch die entsprechenden 4 Bits ersetzt. Etwas mehr Aufwand erfordert die Umrechnung vom Dezimalsystem in das Binär- oder Hexadezimalsystem.

B

Beispiel 2.3: Umrechnung Hexadezimal-, Binär-, Dezimalsystem

Die Umrechnung der ganzen Zahl $0x1AE4$ von der gegebenen Hexadezimaldarstellung in die Binärdarstellung ist einfach:

```
Hexadezimal:      1     A     E     4
Binär:          0001  1010  1110  0100
```

Sie müssen einfach jede Hexadezimalziffer in die entsprechenden 4 Bits umrechnen, also z.B. $0x4$ in den Bitstring 0100 oder $0xE$ in den Bitstring 1110. Die Umkehrung ist ebenso einfach.

Die Umrechnung von $0x1AE4$ in das Dezimalsystem ist etwas schwieriger. Es gilt

$$\begin{aligned} 0x1AE4 &= 1\cdot 16^3 + 10\cdot 16^2 + 14\cdot 16^1 + 4\cdot 16^0 \\ &= 2^{12} + 10\cdot 2^8 + 14\cdot 2^4 + 4 \\ &= 4096 + 10\cdot 256 + 14\cdot 16 + 4 = 4096 + 2560 + 224 + 4 \\ &= 6884. \end{aligned}$$

Ein weiteres gängiges Beispiel eines Datentyps ist eine *Zeichenkette* oder ein *String*. Damit man aus dem Byte-String die einzelnen Zeichen richtig interpretieren kann, muss man die zugrundeliegende Kodierung kennen. Gebräuchliche Kodierungen für Zeichen sind: Zeichenkette

- ASCII (American Standard Code for Information Interchange): Jedes Byte wird als ein Zeichen interpretiert. Allerdings nutzt ASCII nur sieben Bits aus einem Byte, d.h. es gibt 128 ASCII-Zeichen. Zum Beispiel steht der (hexadezimale) Wert $0x4E$ für den Buchstaben `N`, d.h. dessen Bytedarstellung ist `4E`. Die ersten 32 ASCII-Werte von $0x00$ bis $0x1F$ sind Steuerzeichen (z.B. $0x0A$ für Zeilenumbruch) und damit nicht druckbar. ASCII
- Unicode: Die Unicode Kodierung hat zum Ziel, Umlaute und weitere spezielle Zeichen unterschiedlicher Sprachen zu kodieren. Unicode gibt es in verschiedenen Varianten. Bekannt aus dem Umfeld des Internet ist die Unicode-Kodierung *UTF-8*, die ein volles Byte zur Kodierung nutzt. UTF-8 ist abwärtskompatibel mit ASCII (d.h. UTF-8 stimmt in den sieben niederwertigen Bits in einem Byte mit den entsprechenden ASCII-Werten überein). Im Umfeld der digitalen Forensik ist auch die Unicode-Kodierung *UTF-16* relevant, zum Beispiel weil das unter Windows gebräuchliche Dateisystem NTFS die UTF-16-Kodierung nutzt. UTF-8, UTF-16

Ein wichtiger Punkt bei der Interpretation der Datenstruktur in einem Byte-String ist die *Speicherorganisation* bzw. das *Byte-Ordering*. Auf unterschiedlichen Rechnerarchitekturen haben sich zwei verschiedene Speicherorganisationen durchgesetzt, die wir kurz beschreiben: Byte-Ordering

- Systeme mit Speicherorganisation *Little-Endian* speichern das niederwertigste (*least significant*) Byte der Datenstruktur in der **niedrigsten Speicheradresse** (d.h. der relativen Speicheradresse 0). Die Little-Endian Byte-Reihenfolge nutzen heute gängige x86- und x64-Systeme. Little-Endian
- Systeme mit Speicherorganisation *Big-Endian* speichern das niederwertigste (*least significant*) Byte der Datenstruktur in der **höchsten Speicheradresse** Big-Endian

(d.h. der relativen Speicheradresse $n-1$). Die Big-Endian Byte-Reihenfolge nutzen zum Beispiel Mainframe Umgebungen.

B

Beispiel 2.4: Byte-Ordering (Big-Endian vs. Little-Endian)

Wir betrachten den dreistelligen Hexadezimalwert $0x123456$ und geben dessen Darstellung im Big- und Little-Endian an. Wir nehmen an, die Zahl wird ab Adresse 23 gespeichert. Dann gilt:

Absolute Speicheradresse	23	24	25
Relative Speicheradresse	0	1	2
Little-Endian	56	34	12
Big-Endian	12	34	56

Speichern wir den Wert bezüglich Little-Endian, dann steht das niederwertigste Byte `56` an der niedrigsten Adresse, also an der absoluten Adresse 23 bzw. der relativen Adresse 0. Speichern wir den Wert bezüglich Big-Endian, dann steht das niederwertigste Byte `56` an der höchsten Adresse, also an der absoluten Adresse 25 bzw. der relativen Adresse 2.

K

Kontrollaufgabe 2.7: Umrechnung Hexadezimal- in Binärsystem

Berechnen Sie die Binärdarstellung der ganzen Zahl mit Hexadezimaldarstellung $0xAB12D$.

K

Kontrollaufgabe 2.8: Umrechnung Binär- in Dezimal-/Hexadezimalsystem

Es sei die ganze Zahl $n = 11010011_2$ im Binärsystem gegeben. Geben Sie n im Dezimal- sowie im Hexadezimalsystem an.

K

Kontrollaufgabe 2.9: Länge eines Strings mittels `echo`

Mit der folgenden Befehlssequenz schreiben Sie einen String in die Datei `text.txt`. Vergleichen Sie die Eingabelänge des Textes mit der tatsächlichen Dateilänge, was fällt Ihnen auf? Wie erklären Sie sich dies?

```
$ echo 'Hello world!' > text.txt

$ ls -l text.txt
-rw----- 1 peter pan 13 2016-04-16 13:45 text.txt

$ xxd text.txt
0000000: 4865 6c6c 6f20 776f 726c 6421 0a Hello world!.
```

Kontrollaufgabe 2.10: Länge eines Byte-Strings

Sie kopieren die Bytes $B_{100}\, B_{101}\, \cdots B_{1000}$ von einem Datenträger. Wie viele Bytes werden verarbeitet? Wie viele sind es im allgemeinen Fall $B_n\, B_{n+1}\, \cdots B_m$ mit $m \geq n$?

K

Kontrollaufgabe 2.11: ASCII-Kodierung

Wie lautet die ASCII-Kodierung des Worts *Forensics*?

K

Kontrollaufgabe 2.12: Little- vs. Big-Endian

Ein vorzeichenloser Integer mit einer Länge von 4 Byte wird innerhalb der Bytes $B_2\, B_3\, B_4\, B_5$ (d.h. ab Offset 2) gespeichert. Der Byte-String lautet

```
01A3 B267 287C E632
```

(Hinweis: Das erste Byte ist B_0)

Bestimmen Sie den dezimalen Wert des Integers sowohl in Big-Endian als auch in Little-Endian.

K

Verzeichnisse

I. Abbildungen

Abb. 1.1: Das Locardsche Austauschprinzip . . . 14
Abb. 2.1: Weg zur Assoziation . . . 19
Abb. 2.2: Beispiel für Interpretationsebenen: Bilddatei . . . 23
Abb. 3.1: Teilweise mittels File Carving wiederhergestelltes, fragmentiertes Bild . . . 43
Abb. 3.2: Autopsy 4.0.0 . . . 45
Abb. 3.3: Digital Forensic Framework . . . 46
Abb. 3.4: Kali Boot Modi [Quelle: http://de.docs.kali.org] . . . 47
Abb. 4.1: Klassischer Aufbau einer Festplatte . . . 52
Abb. 4.2: Ablauf der Post-Mortem-Datensicherung . . . 54
Abb. 4.3: Schreibzugriff ohne Software Writeblocker [7] . . . 56
Abb. 4.4: Schreibzugriff mit Software Writeblocker [7] . . . 56
Abb. 4.5: Lese- und Schreibzugriff mit Einsatz eines Hardware Writeblockers [7] . . . 57
Abb. 4.6: Links: Mobiler Hardware Writeblocker [22]; rechts: Imaging Bay [23] . . . 57
Abb. 4.7: HPA/DCO . . . 59
Abb. 4.8: Vereinfachter Aufbau einer Partitionstabelle . . . 62
Abb. 4.9: Extraktion von Partitionen . . . 63
Abb. 4.10: Genereller Aufbau einer DOS-Partitionierung . . . 64
Abb. 4.11: Komplexes Beispiel zum Aufbau einer DOS-Partition . . . 65
Abb. 4.12: Übersicht über eine GPT partitionierte Festplatte . . . 73
Abb. 5.1: Kategorisierung nach Carrier[7] . . . 81
Abb. 5.2: RAM Slack, Drive Slack and File Slack . . . 84
Abb. 6.1: Layout eines FAT12/16-Dateisystems . . . 93
Abb. 6.2: Layout eines FAT32-Dateisystems mit Wurzelverzeichnis am Anfang des Datenbereichs . . . 94
Abb. 6.3: Layout eines FAT32-Dateisystems mit Wurzelverzeichnis an einer beliebigen Stelle im Datenbereich . . . 94
Abb. 6.4: Datenverwaltung unter FAT . . . 101
Abb. 6.5: Datumangabe unter FAT . . . 108
Abb. 6.6: Uhrzeitangabe unter FAT . . . 108
Abb. 6.7: Verwaiste Verzeichniseinträge . . . 113
Abb. 6.8: Anlegen einer Datei . . . 117
Abb. 6.9: Löschen einer Datei . . . 118
Abb. 7.1: Layout eines NTFS-Dateisystems . . . 121
Abb. 7.2: Layout eines NTFS-Dateisystems . . . 125
Abb. 7.3: Übersicht über einen MFT-Eintrag . . . 128
Abb. 7.4: Detaillierte Darstellung eines MFT-Eintrag . . . 129
Abb. 7.5: Beispiel eines MFT Eintrags inkl. Attribute . . . 133
Abb. 7.6: Verzeichnisse in NTFS am Beispiel C:\Windows . . . 142
Abb. 7.7: $INDEX_ALLOCATION-Attribut von C:\Windows . . . 143
Abb. 7.8: NTFS Verschlüsselung . . . 154
Abb. 7.9: NTFS Entschlüsselung . . . 155
Abb. 7.10: Dateierstellung unter NTFS . . . 158
Abb. 7.11: Dateilöschung unter NTFS . . . 159
Abb. 8.1: S-A-P Vorgehensmodell. . . . 161
Abb. 8.2: Computer Forensic Field Triage Process Model [10]. . . . 163
Abb. 8.3: Cert-Taxonomie [10]. . . . 164
Abb. 8.4: BSI-Modell [10]. . . . 164
Abb. 8.5: “Treppenstufen” von Casey’s Modell nach [8]. . . . 166
Abb. 8.6: NIST-Modell. . . . 168

II. Beispiele

Beispiel 2.1: Übersetzung rechtliche Frage in forensische Frage . . . 17
Beispiel 2.2: Interpretationsebenen einer digitalen Spur . . . 22
Beispiel 2.3: Umrechnung Hexadezimal-, Binär-, Dezimalsystem . . . 31
Beispiel 2.4: Byte-Ordering (Big-Endian vs. Little-Endian) . . . 32
Beispiel 3.1: SHA-256 Hashwerte eines USB Sticks samt Partitionen . . . 38
Beispiel 3.2: Rekursive Berechnung von Hashwerten mit sha256deep . . . 39
Beispiel 3.3: Ausführung von dd . . . 40
Beispiel 3.4: dd Offset in der Eingabedatei . . . 40
Beispiel 3.5: dd Offset in der Ausgabedatei . . . 41
Beispiel 3.6: Konfigurationsdatei von Scalpel . . . 42
Beispiel 3.7: Nutzung des Tools strings . . . 44
Beispiel 3.8: Angabe des Offsets . . . 45
Beispiel 4.1: Masterkopie, Arbeitskopie . . . 55
Beispiel 4.2: Detektion einer HPA . . . 59
Beispiel 4.3: Einrichten/Entfernen einer HPA . . . 60
Beispiel 4.4: Linux-Umgang mit automatischer HPA-Erkennung . . . 60
Beispiel 4.5: Device Configuration Overlay . . . 61
Beispiel 4.6: Extraktion einer Partition . . . 63
Beispiel 4.7: DOS Partitionsschema . . . 66
Beispiel 4.8: Partitionslayout eines USB Sticks mittels fdisk . . . 69
Beispiel 4.9: Partitionslayout eines USB Sticks mittels mmls . . . 71
Beispiel 4.10: GPT als DOS partitionierter Datenträger . . . 73
Beispiel 4.11: Hexdump eins GPT Headers . . . 75
Beispiel 4.12: Hexdump eines GPT Partitionseintrags . . . 76
Beispiel 4.13: Anzeigen des GPT Partitionsschemas mittels mmls . . . 77
Beispiel 5.1: Ausgabe von Dateisystemdaten mittels fsstat . . . 83
Beispiel 5.2: Zugriff auf Datensektoren oder -cluster mittels blkcat . . . 86
Beispiel 5.3: Zugriff auf Metadaten einer Datei mittels istat . . . 89
Beispiel 5.4: Übersicht über Dateinamen eines Dateisystems mittels fls . . . 90
Beispiel 6.1: Ausgabe von FAT32-Dateisystemdaten mittels fsstat . . . 97
Beispiel 6.2: Umrechnung Cluster- zu Sektoradressen . . . 99
Beispiel 6.3: Länge einer Cluster Chain . . . 101
Beispiel 6.4: FAT-Einträge in FAT16 . . . 103
Beispiel 6.5: Cluster Chains in der Ausgabe von fsstat . . . 104
Beispiel 6.6: Verzeichniseintrag im FAT-Dateisystem . . . 106
Beispiel 6.7: Zeitstempel im FAT-Dateisystem . . . 109
Beispiel 6.8: Zugriff auf Root-Verzeichnis mittels Metadatenadresse . . . 111
Beispiel 6.9: Hexdump eines Verzeichnisses . . . 112
Beispiel 6.10: Verwaiste Verzeichniseinträge . . . 113
Beispiel 6.11: Suche nach gelöschten Verzeichnissen mit sigfind . . . 114
Beispiel 6.12: Langer Dateiname . . . 116
Beispiel 7.1: NTFS-Bootsektor . . . 127
Beispiel 7.2: MFT Entry Header: Signatur und Fixup Array . . . 130
Beispiel 7.3: MFT Entry Header: Zeiger auf Datenstrukturen . . . 132
Beispiel 7.4: Attribute der $MFT . . . 134
Beispiel 7.5: Attribut-Header eines residenten Attributs . . . 136
Beispiel 7.6: Attribut-Inhalt von $STANDARD_INFORMATION mittels istat . . . 138
Beispiel 7.7: Attribut-Inhalt von $FILE_NAME mittels istat . . . 140
Beispiel 7.8: Dateisuche in NTFS . . . 143
Beispiel 7.9: IROM und Node Header . . . 144
Beispiel 7.10: Index Record . . . 146
Beispiel 7.11: Alternate Data Streams . . . 149
Beispiel 7.12: Konzept der Cluster-Runs . . . 150
Beispiel 7.13: Attribut-Header eines nicht-residenten Attributs . . . 150

Beispiel 7.14: Kennzeichnung einer verschlüsselten Datei . . . 153
Beispiel 7.15: $EFS-Header . . . 156
Beispiel 7.16: DDF-/DRF-Header im $EFS-Attribut . . . 157

III. Definitionen

Definition 2.1: Digitales Austauschprinzip . . . 27
Definition 3.1: Hashfunktion . . . 37
Definition 3.2: Kryptographisch sichere Hashfunktion . . . 37

IV. Exkurse

Exkurs 7.1: Dateisystemimage mounten . . . 128
Exkurs 7.2: DCode und wichtige Zeitpunkte in NTFS . . . 139

V. Kontrollaufgaben

Kontrollaufgabe 1.1: Definition Forensik . . . 15
Kontrollaufgabe 1.2: Spuren, Indizien, Beweise . . . 15
Kontrollaufgabe 1.3: Locardsche Austauschprinzip . . . 15
Kontrollaufgabe 2.1: Weg zur Assoziation . . . 21
Kontrollaufgabe 2.2: Anforderungen an den Ermittlungsprozess . . . 21
Kontrollaufgabe 2.3: Digitale Spur . . . 26
Kontrollaufgabe 2.4: Vermeidbarkeit digitaler Spuren . . . 26
Kontrollaufgabe 2.5: Klassifikation digitaler Spuren . . . 26
Kontrollaufgabe 2.6: Post-Mortem- und Live-Forensik . . . 30
Kontrollaufgabe 2.7: Umrechnung Hexadezimal- in Binärsystem . . . 32
Kontrollaufgabe 2.8: Umrechnung Binär- in Dezimal-/Hexadezimalsystem . . . 32
Kontrollaufgabe 2.9: Länge eines Strings mittels echo . . . 32
Kontrollaufgabe 2.10: Länge eines Byte-Strings . . . 33
Kontrollaufgabe 2.11: ASCII-Kodierung . . . 33
Kontrollaufgabe 2.12: Little- vs. Big-Endian . . . 33
Kontrollaufgabe 4.1: Vorbereitung eines Datenträgers zur Datensicherung . . . 57
Kontrollaufgabe 4.2: Optionen von dd bei der Datensicherung . . . 57
Kontrollaufgabe 4.3: Größe einer HPA . . . 59
Kontrollaufgabe 4.4: Nicht-allokierte Bereiche . . . 63
Kontrollaufgabe 4.5: Extraktion von Partitionen/nicht-allokierten Bereichen . . . 64
Kontrollaufgabe 4.6: Maximale Größe eines DOS partitionierten Datenträgers . . . 68
Kontrollaufgabe 4.7: DOS Partitionstypen . . . 69
Kontrollaufgabe 4.8: Herausschreiben eines Bereichs mittels dd, mmcat . . . 72
Kontrollaufgabe 4.9: Hexdump eines Partitionseintrags . . . 72
Kontrollaufgabe 4.10: Hexdump eines Partitionseintrags einer erweiterten Partition . . . 72
Kontrollaufgabe 4.11: Maximale Größe eines GPT partitionierten Datenträgers . . . 73
Kontrollaufgabe 4.12: Datenstrukturen im GPT Header . . . 75
Kontrollaufgabe 4.13: Auslesen des Hexdumps der GPT Partitionstabelle . . . 75
Kontrollaufgabe 4.14: Backup Kopie des GPT Headers . . . 78
Kontrollaufgabe 4.15: Backup Kopie von Partitionseinträgen . . . 78
Kontrollaufgabe 5.1: Kategorisierung der Bitmap-Datenstruktur . . . 84
Kontrollaufgabe 5.2: Inkonsistenz von Zeitstempeln . . . 89
Kontrollaufgabe 5.3: Dateinamen zu gegebener Metadatenadresse finden . . . 91
Kontrollaufgabe 6.1: Layout eines FAT-Dateisystems . . . 100
Kontrollaufgabe 6.2: Lage eines FAT32-Zeigers . . . 102
Kontrollaufgabe 6.3: Erster Cluster der Cluster Chain . . . 103

Kontrollaufgabe 6.4: Lage und Größe des Wurzelverzeichnisses . . . 104
Kontrollaufgabe 6.5: Zeitstempel in FAT . . . 110
Kontrollaufgabe 6.6: Metadatenadressierung in FAT . . . 111
Kontrollaufgabe 6.7: Hexdump eines Verzeichniseintrags in FAT . . . 111
Kontrollaufgabe 6.8: Wiederherstellung einer verwaisten Datei . . . 114
Kontrollaufgabe 6.9: Wiederherstellung einer gelöschten Datei in FAT . . . 119
Kontrollaufgabe 6.10: Löschen und File Slack einer Datei in FAT . . . 119
Kontrollaufgabe 6.11: Sicheres Löschen einer Datei in FAT . . . 119
Kontrollaufgabe 7.1: Hexdump eines NTFS-Bootsektors . . . 127
Kontrollaufgabe 7.2: Backup-Kopie eines NTFS-Bootsektors . . . 128
Kontrollaufgabe 7.3: Dateiadresse . . . 132
Kontrollaufgabe 7.4: Dateiadressen der Dateisystemdateien . . . 133
Kontrollaufgabe 7.5: Fixup Array . . . 133
Kontrollaufgabe 7.6: Auffinden der MFT . . . 133
Kontrollaufgabe 7.7: Attribute Type Identifier . . . 137
Kontrollaufgabe 7.8: Dateisystemdatei $AttrDef . . . 138
Kontrollaufgabe 7.9: Zugriff auf Hexdump des $STANDARD_INFORMATION-Attributs . . . 140
Kontrollaufgabe 7.10: Zeitstempel in NTFS . . . 140
Kontrollaufgabe 7.11: Zugriff auf Hexdump des $FILE_NAME-Attributs . . . 141
Kontrollaufgabe 7.12: Dateiadresse im $FILE_NAME-Attribut . . . 141
Kontrollaufgabe 7.13: Auffinden gelöschter Verzeichnisse . . . 147
Kontrollaufgabe 7.14: Flag-Feld . . . 148
Kontrollaufgabe 7.15: Suche nach verschlüsselten Dateien . . . 157

VI. Tabellen

Tabelle 4.1: Datenstrukturen im MBR . . . 67
Tabelle 4.2: Aufbau eines Eintrags der Partitionstabelle . . . 67
Tabelle 4.3: Exemplarische DOS Partitionstypen . . . 69
Tabelle 4.4: Datenstrukturen im GPT Header (EOS = End Of Sector) . . . 74
Tabelle 4.5: Felder eines Eintrags einer GPT Partitionstabelle . . . 76
Tabelle 5.1: Gebräuchliche Zeitstempel in Dateisystemen . . . 87
Tabelle 6.1: Essenzielle Daten an Offset 0 bis 35 des FAT-Bootsektors für alle FAT-Varianten . . . 96
Tabelle 6.2: Essenzielle Daten ab Offset 36 des FAT32-Bootsektors . . . 97
Tabelle 6.3: Datenstruktur in dem FSINFO-Sektor . . . 97
Tabelle 6.4: Bedeutung der Zeigerwerte in einer FAT . . . 102
Tabelle 6.5: Struktur eines Basisverzeichniseintrages bei FAT . . . 105
Tabelle 6.6: Attribute in einem Verzeichniseintrag . . . 106
Tabelle 6.7: Offsets der Zeitstempelfelder bei FAT . . . 107
Tabelle 6.8: Offsets eines Langen Dateinamens (LFN) . . . 115
Tabelle 7.1: Clustergröße in NTFS in Abhängigkeit von der Dateisystemgröße [14] . . . 121
Tabelle 7.2: Dateisystemdateien in NTFS . . . 124
Tabelle 7.3: Essentielle Daten eines NTFS-Bootsektors . . . 126
Tabelle 7.4: Datenstrukturen eines MFT Entry Headers . . . 131
Tabelle 7.5: Standardattribute in NTFS . . . 134
Tabelle 7.6: Datenstrukturen eines Attribut-Headers für ein residentes Attribut . . . 135
Tabelle 7.7: Datenstrukturen eines $STANDARD_INFORMATION-Attributs . . . 139
Tabelle 7.8: Datenstrukturen eines $FILE_NAME-Attributs . . . 141
Tabelle 7.9: $INDEX_ROOT-Metadaten (IROM) . . . 144
Tabelle 7.10: Metadaten im Knoten-Header (Node Header, NH) . . . 144
Tabelle 7.11: Index-Record-Metadaten (IREM) . . . 146
Tabelle 7.12: Spezifikation der Index-Einträge für ein $FILE_NAME-Attribut . . . 146
Tabelle 7.13: Datenstrukturen eines Attribut-Headers für ein nicht-residentes Attribut . . . 150
Tabelle 7.14: Spezifikation des $EFS-Headers im $LOGGED_UTILITY-Attribut . . . 156
Tabelle 7.15: Spezifikation des DDF-/DRF-Headers im $EFS-Attribut . . . 156

Tabelle 8.1: Einordnung der Modell-Phasen zu den abstrakten Tätigkeiten 171

VII. Literatur

[1] Rick Ayers, Sam Brothers, und Wayne Jansen. Sp 800-101. guidelines on movile device forensics. Technical report, Gaithersburg, MD, United States, 2014.

[2] Harald Baier und Christian Dichtelmüller. Datenreduktion mittels kryptographischer Hashfunktionen in der IT-Forensik: Nur ein Mythos? In *DACH Security 2012*, pages 278–287, September 2012.

[3] Frank Breitinger und Harald Baier. Similarity Preserving Hashing: Eligible Properties and a new Algorithm MRSH-v2. In *Proceedings of the 4th ICST Conference on Digital Forensics and Cyber Crime* (*ICDF2C*), pages 167–182, 2012.

[4] Frank Breitinger, Knut Petter Åstebøl, Harald Baier, und Christoph Busch. `mvhash-b` – a new approach for similarity preserving hashing. In *Proceedings of the 7th IEEE Conference on IT Security Incident Management & IT Forensics* (*IMF*), pages 33–44, 2013.

[5] Frank Breitinger, Huajian Liu, Christian Winter, Harald Baier, Alexey Rybalchenko, und Martin Steinebach. Towards a process model for hash functions in digital forensics. In *Proceedings of the 5th ICST Conference on Digital Forensics and Cyber Crime* (*ICDF2C*), pages 170–186, 2013.

[6] Dominik Brodowski und Felix C. Freiling. Cyberkriminalität - Computerstrafrecht und die digitale Schattenwirtschaft. Technical report, http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf, 2011.

[7] Brian Carrier. *File System Forensic Analysis*. Addison Wesley Professional, 2005.

[8] Eoghan Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press, 2011.

[9] Andreas Dewald und Felix C. Freiling. *Forensische Informatik*. Books on Demand Verlag, 2011.

[10] Bundesamt für Sicherheit in der Informationstechnik. Leitfaden "IT-Forensik". Technical report, http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile, zuletzt aufgerufen am: 18.06.2014.

[11] Alexander Geschonneck. *Computer Forensik*. dpunkt Verlag, 2014.

[12] Jesse Kornblum. Identifying almost identical files using context triggered piecewise hashing. In *Proceedings of the 6th Digital Forensic Research Workshop* (*DFRWS*), pages 91–97, 2006.

[13] Alfred Menezes, Paul van Oorschot, und Scott Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[14] Microsoft. The NTFS File System. https://technet.microsoft.com/en-us/library/cc976808.aspx, 2016. besucht am 02.06.2016.

[15] Microsoft. Maximum Volume Sizes. https://technet.microsoft.com/en-us/library/cc938432.aspx, 2016. besucht am 02.06.2016.

[16] National Institute of Standards and Technology (NIST). Secure Hash Standard – FIPS 180-4 – SHA-2. *http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4*, 2012.

[17] National Institute of Standards and Technology (NIST). Approximate Matching: Definition and Terminology. *http://csrc.nist.gov/publications/drafts/800-168/sp800_168_draft.pdf*, 2014.

[18] National Institute of Standards and Technology (NIST). National Software Reference Library – Reference Data Set (NRSL-RDS), Release 2.48. *http://nsrl.nist.gov*, 2015.

[19] Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, und Steve Debrota. Computer forensics field triage process model. http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=document_general_info&cPath=11&products_id=228, 2006. aufgerufen am 14.07.2015.

[20] Vassil Roussev. Data Fingerprinting with Similarity Digests. In *Proceedings of the 6th Annual IFIP WG 11.9 International Conference on Digital Forensics*, pages 207–226, 2010.

[21] Vassil Roussev. Scalable Data Correlation – Managing TB-scale investigations with similarity digests. In *Proceedings of the 8th Annual IFIP WG 11.9 International Conference on Digital Forensics*, pages 19–34, 2012.

[22] Guidance Software. T35u forensic bridge. https://www.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges/t35u.aspx#product-gallery, , letzter Zugriff: 22.04.2014, 2014.

[23] Guidance Software. T3iu forensic sata imaging bay. Technical report, https://www.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges/t3iu.aspx, 2014.

[24] Martin Steinebach. Robust Hashing for Efficient Forensic Analysis of Image Sets. In *Proceedings of the 3rd ICST Conference on Digital Forensics and Cyber Crime (ICDF2C)*, pages 180–187, 2011.

[25] T13. AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS). http://t13.org/Documents/UploadedDocuments/docs2006/D1699r3f-ATA8-ACS.pdf, December 2008.

[26] Jonathan Zdziarski. *iPhone Forensics : Recovering Evidence, Personal Data, and Corporate Assets*. O'Reilly Media, 2008.

Stichwörter

Änderung der Offsets 63
Übersetzung rechtliche Frage in forensische Frage 17
Übersicht 54, 125
FSINFO 96
$BITMAP 137
$DATA 148
$INDEX_ALLOCATION 142
$INDEX_ROOT 142
$INDEX_ROOT-Metadaten (IROM) 144
$LOGGED_UTILITY_STREAM 137
$MFTMirr 125
$MFT 124
$UsnJrnl 126
blkcat 85
dcfldd 41
fdisk 68
fls 90
fsstat 83
hdparm 59
istat, icat, ils 88
jls, jcat 91
mmls 70
sigfind 114
$LogFile 126
12 Phasen Modell von Casey 166
32-Byte-Datenstruktur 105
7 W-Fragen 19

Abgrenzung zur Anwendungsforensik 80
Adressierung 94
Alloziert vs. nicht-alloziert 84
Alternate Data Stream 148
Analyse 167, 169
Analyse des nicht-allozierten Bereichs 85
Analysephase 162
Analysewerkzeuge 63
Anforderung des BSI-Leitfaden 58
Anforderungen an den Ermittlungsprozess . . . 20
Anforderungen an Tools 35
Anforderungen kryptographischer Hashfunktionen 37
Anlegen einer Datei 84
Anlegen einer Datei im FAT Dateisystem 117
Anlegen eines Verzeichnisses 111
Anschuldigung 166
Anwendungsdaten 91
Anwendungsfall Wechseldatenträger 93
Arbeitgeber 14
Arbeitskopie 54
ASCII 31
Assoziation 18
ATA-Befehle im Kontext der DCO 61
ATA-Befehle im Kontext der HPA 58
Attribut-Header, Attribut-Body 133
Attribute 105
Attributlänge 135
Attributname 136
Aufbau dieses Abschnitts 21
Aufbau eines $INDEX_ROOT-Knotens 143
Aufbau eines Cluster-Runs 151
Aufbau eines Index-Records 145
Aufbau eines MFT-Eintrags 128
Aufbereitung von Metadaten, Timelining 35
Ausgabe der Cluster Chains mit fsstat 104
Ausgangspunkt ist Frage des Rechts 17
Aussagekraft von Zeitstempeln 139
Auswertung 167
Autopsy GUI 46
Avalanche Effect 38

Backup Bereich 77
Backup-Kopie des Bootsektors 82, 127
Basiseintrag 115, 125
Bedeutung eines FAT-Eintrags 102
Behandlung von Spuren 18
Beispielangabe 152
Beispieldatenträger 59
Beispiele 56, 79
Berechnung von Hashwerten mehrerer Dateien 39
Bergung 167
Bericht 168
Beschlagnahmung 167, 169
Beweis 13
Beweismittel 18
Bezeugen 168
Bezug zur Aussagekraft einer digitalen Spur . . 25
Big-Endian 31
Binärsystem 30
Bitgenaue Kopie 54
Bitmap-Struktur 84
Boot Code, Windows Signatur, Magic Number 67
Bootsektor 82, 126
BSI Modell 163
Byte-Ordering 31
Byte-String 30

Carriers Referenzmodell 80
CFFTPM 163
Chain of Custody 14
CHS-Adressierung 52
Cluster Chain 100
Cluster Runlist 150
Clusteradresse, Dateigröße 106

Dateiadresse 130, 141
Dateianalyse 170

Dateiausschluß 170
Dateigröße, Dateiname 141
Dateiname 81, 89, 105
Dateiname beginnt mit $ 124
Dateisuche 170
Dateisystem Block 80
Dateisystem- vs. erweiterte Partition 64
Dateisystem-Anwendungsdaten 82
Dateisystemdateien 124
Dateisystemdaten 81
Dateisystemgröße 96
Dateisystemslack 95
Dateiwiederherstellung mit WinHex 48
Datenüberlastung 28
Datenanalyse 165
Datensammlung 165
Datenstrukturen im MBR 66
Datenstrukturen nicht-residenter Attribute . . . 150
Datenträgerblock 80
Datenträgersammlung 170
Datenträgersicherung 170
Datenuntersuchung 165
Datumangabe 107
Default-$DATA-Attribut 148
Definition des BSI 11
Definition nach Casey 21
Design 121
Designprinzipien 123
Details zu Attributen 137
Detektion einer HPA 58
Detektion eines DCO 61
Determinismus 28
Device Configuration Overlay 51, 61
Digital Forensics Framework 46
Digitale Forensik 21
Digitale Spur 21
Digitale Spuren 13
Digitales Austauschprinzip 27
Digitales Austauschprinzip? 14
Dokumentation 14, 36, 166, 170
DOS Partition 64
DOS Partitionstabelle 64
Drei Schritte zur Assoziation 19

EFS 153
Ein-/Ausschalter 56
Eine Frage des Rechts 11
Einfacher Aufbau 93
Einrichten/Entfernen einer HPA 60
EnCase Forensics 48
Entfernung zum Tatort 23
Entschlüsselung 155
Entstehung von Spuren 17
Ereignis 18
Erhebung 169
Erkennung bekannter Objekte: Whitelisting, Blacklisting 38

Essentielle Daten 82
Essentielle Daten eines NTFS-Bootsektors 126
Essenzielle Datenstrukturen 66
Everything is a file 121
Exaktes Duplizieren 27
Extraktion von Partitionen 63

Fallstricke der Zeitstempel 88
FAT-Adressen 0, 1 102
FAT-Bereich 95
FAT-Slack 103
FAT12, FAT16, FAT32 101
FAT12/16 vs. FAT32 95
FAT32-spezifische Werte 96
Fehlende Spezifikation 123
Fehlende Standardisierung 66
Fehlinterpretation 23
Feste Größe 139
Feststellung eines Ereignisses 18
File Allocation Table, FAT 93
File Carving 41
File Slack 85
Fixup Array 129
Flüchtige Spuren 24
Flüchtigkeit einer digitalen Spur 24
Flags, Attribut-ID 136
Folgerung 27
Foremost, Scalpel 42
Forensic science 11
Forensik 11
Fragmentierung 85, 86
Funktionsweise 42

Güterabwägung 167
Ganze Zahl 30
Geschützter MBR 73
GPT Header 74
Größe MFT-Eintrag 126
Gründe für eine Partitionierung 62
Grundlegendes 138, 140
Grundlegendes zum Attribut-Header 135
GUID 72

Hardware Writeblocker 56
Hashfunktionen in der digitalen Forensik 37
Hexadezimalystem 30
Hinweise 155
Host Protected Area 51, 58

Identifikation 19
Immaterielle Spuren 13
Index Nodes 158
Index-Einträge 145
Index-Record 126, 142
Index-Record-Metadaten (IREM) 145
Index: Baumstruktur 142
Individualisierung 19
Individualisierung einer Assoziation 28

Indiz = gewürdigte Spur . . . 13
Inhaltsdaten . . . 81
Integrität . . . 37
Integrität von Spuren . . . 53
Interpretation der Offsets . . . 68
Interpretationsebenen . . . 22
IT-Forensik vs. Computerforensik . . . 12
IT-forensische Tools . . . 35
IT-forensischer Nutzen eines Dateisystems . . . 80

Journal . . . 123
Journale . . . 91

Kali Linux . . . 46
Kapselung von Informationen . . . 133
Kategorien . . . 81
Kennzeichnung . . . 153
Klassifikation . . . 19
Klassifikationsschemata . . . 23
Knoten-Header (NH) . . . 144
Kodierung der Zeitstempel . . . 107
Koexistenz HPA/DCO . . . 61
Konzept . . . 142
Konzept der Cluster-Runs . . . 149
Korrektheit . . . 36
Korrektheit von Werkzeugen . . . 23
Kryptographische Verfahren . . . 155
Kurzer Dateiname: SFN . . . 115

Länge der Cluster Chain . . . 101
Löschen einer Datei . . . 84, 103
Löschen einer Datei im FAT Dateisystem . . . 117
Löschen eines Objekts . . . 112
Lage des File System Slack . . . 96
Lage des Fixup Arrays . . . 129
Lage des reservierten Bereichs . . . 95
Lange Dateinamen . . . 123
Langer Dateiname: LFN . . . 115
Layout . . . 93
LBA . . . 80
LBA-Adressierung . . . 53
Legalität der Untersuchung . . . 19
Legt Layout fest . . . 95
Links . . . 123
Little-Endian . . . 31
Live-Forensik . . . 29
Locardsches Austauschprinzip . . . 14
Logische Datei Adresse . . . 80
Logische Dateisystem Adresse . . . 80
Logische Partitions Adresse . . . 80
Lokale digitale Spuren . . . 22
Low-Level-Formatierung . . . 52

Magic Numbers . . . 41
Manipulationsresistenz . . . 36
Master Boot Record (MBR) . . . 64
Master File Table (MFT) . . . 128
Masterkopie . . . 54
Materielle Spuren . . . 13
Maximale Dateisystemgröße . . . 121
Metadaten . . . 81, 87
Metadatenadressen gemäß Sleuthkit . . . 110
MFT-Entry-Header . . . 129
MFT-Zone . . . 125
Millisekunden im Zeitstempel `created` . . . 109
Modi des Live Systems . . . 47

Namenskonflikte gelöschter Objekte . . . 112
Nicht-allokierte Bereiche . . . 63
Nicht-essentielle Daten . . . 82
Nicht-essentielle Daten eines NTFS-Bootsektors 127
Nicht-Lokale digitale Spuren . . . 22
Nist Modell . . . 168
NIST Tool Testing . . . 36
NIST-Datenbank für Tools . . . 35
Non-resident Flag . . . 136
NTFS . . . 121
Nummerierung der MFT-Einträge . . . 125

Operationale Vorbereitun . . . 165
Order of Volatility . . . 24
Organisation von Daten . . . 79

Partitionierung . . . 61
Partitionsbereich . . . 77
Partitionseintrag . . . 67
Partitionsschema . . . 62
Partitionstabelle . . . 62, 67, 75
Partitionstabelle einer erweiterten Partition . . . 65
Partitionstypen . . . 68
Performanz . . . 36
Persistente Spuren . . . 24
PhotoRec . . . 43
Post-Mortem- vs. Live-Datensicherung . . . 53
Post-Mortem-Analyse . . . 29
Präsentationsphase . . . 162
Praktiken der digitalen Forensik . . . 25
Primäre vs. sekundäre Partition . . . 65
Problem: Fragmentierung . . . 43
Prozessmodelle . . . 20

Reduktion . . . 167
Rekonstruktion einer Tat . . . 18
Rekursive Hashwertberechnung . . . 39
Reproduzierbarkeit . . . 36
Resident, nicht-resident . . . 134
Robustheit . . . 36

S-A-P Modell, 3 Phasen Modell . . . 161
Schutz des FEK . . . 154
Schwer zu vernichten . . . 28
Sehr großer Zustandsraum . . . 26
Sektorgröße, Clustergröße . . . 95
Semi-persistente Spuren . . . 24
Sequenznummer . . . 116

SHA-Familie 37
Sicherheitsschwelle 37
Sicherung 167
Sicherungsphase 161
Signatur 129
Software Writeblocker 55
Software- vs. Hardware-Writeblocker 55
Sortierte Verzeichnisse 142
Spezifikation eines residenten Attribut-Headers 135
Spur = hinterlassenes Zeichen 12
Spurenanalyse, KTU 18
Spurensicherung 18
Strategische Vorbereitung 164
Suche 167
Suche nach gelöschten Verzeichnissen 114
Suche nach Zeichenketten 43
Symmetrische vs. asymmetrische Verschlüsselung 153

Tatortsicherung 167
Technisch unvermeidbare Spuren 25
Technisch vermeidbare Spuren 24
Testen 55
Tool zur Datensicherung 40
TSK 45

UEFI 72
Uhrzeitangabe 108
Umordnung eines Verzeichnisses 147
Umrechnung Sektor-Cluster-Adressen 98
Umrechnung von Zahlensystemen 30
Untersuchung 169
Untersuchungsziele, Integrität von Spuren 13
UTF-16 115
UTF-8, UTF-16 31

Verschlüsselung 154
Vertrauenswürdigkeit 36
Vertraulichkeit 152
Verwaiste Verzeichniseinträge 113
Verzeichniseintrag 104
Vier Partitionstypen 65
Volume Slack 82
Vorgehensmodell 161
Vorgehensweise bei der Datensicherung 60
Vorteile von GPT 73

Wachsende Informationsmenge 11
Weitere Eigenschaften 149
Weitere Informationen im MFT-Entry-Header 131
Weiterer Aufbau 123
Whitelist 162, 167
Wiederholung 26
WinHex 48
Wo entstehen digitale Spuren? 21
Writeblocker 54
Wurzelverzeichnis 90

X-Ways 47

Zeichenkette 31
Zeiger auf Attributinhalt 136
Zeiger auf Datenstrukturen 131
Zeitstempel 87, 105
Zeitstempel in NTFS 138
Zitat zum Austauschprinzip 14
Zwei `$FILE_NAME`-Attribute 141