Forensische Prinzipien: von *digital* zu *cyber*

Autoren:
Andreas Dewald
Felix C. Freiling

Friedrich-Alexander-Universität Erlangen-Nürnberg

Forensische Prinzipien: von *digital* zu *cyber*

Autoren:

Andreas Dewald

Felix C. Freiling

---

2. Auflage

Friedrich-Alexander-Universität Erlangen-Nürnberg

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

AUFSTIEG DURCH BILDUNG
OFFENE HOCHSCHULEN

© 2016 Andreas Dewald, Felix Freiling
Friedrich-Alexander-Universität Erlangen-Nürnberg
Department Informatik
Martensstr. 3
91058 Erlangen

2. Auflage (9. Dezember 2016)

Didaktische und redaktionelle Bearbeitung:
Michael Gruhn

Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Verfasser unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 16OH12022 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Inhaltsverzeichnis

Einleitung **4**
I. Abkürzungen der Randsymbole und Farbkodierungen . . . 4
II. Zu den Autoren . . . 5
III. Lehrziele . . . 6

Forensische Prinzipien: von *digital* zu *cyber* **7**
1 Klassische Forensische Wissenschaften . . . 7
1.1 Forensische Wissenschaften . . . 7
1.2 Spuren und ihre Entstehung . . . 13
1.3 Rekonstruktion eines Tathergangs . . . 21
1.4 Zusammenfassung . . . 24
2 Digitale Spuren . . . 24
2.1 Definition und Abgrenzung . . . 25
2.2 Entstehung digitaler Spuren . . . 29
2.3 Eigenschaften digitaler Spuren . . . 32
2.4 Assoziation mittels digitaler Spuren . . . 39
2.5 Assoziation als zentraler Aspekt der forensischen Informatik . . . 47
2.6 Verwandte Literatur . . . 51
2.7 Zusammenfassung . . . 52

Verzeichnisse **53**
I. Abbildungen . . . 53
II. Beispiele . . . 53
III. Definitionen . . . 53
IV. Exkurse . . . 53
V. Kontrollaufgaben . . . 53
VI. Tabellen . . . 53
VII. Literatur . . . 54

Einleitung

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K

II. Zu den Autoren

Andreas Dewald ist IT-Security Researcher bei der ERNW Research GmbH und assoziierter Post-Doc an der Friedrich-Alexander Universität Erlangen-Nürnberg (FAU), wo er von 2012 bis Januar 2016 als Forscher und Dozent tätig war. Von 2013 bis 2016 leitete er dort die Forschungsgruppe “Applied Forensic Computing” nachdem er seine Promotion im Dezember 2012 mit der Dissertation “Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik” als Doktor der Ingenieurwissenschaften (Dr.-Ing.) abgeschlossen hatte. Bis Oktober 2013 betreute er von Seiten der FAU den ersten deutschen Master-Studiengang in digitaler Forensik, der in einem Kooperationsprojekt an der Hochschule Albstadt-Sigmaringen angeboten wird.

Felix Freiling ist Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Schwerpunkte seiner Arbeitsgruppe in Forschung und Lehre sind offensive Methoden der IT-Sicherheit, technische Aspekte der Cyberkriminalität sowie digitale Forensik (IT-Beweismittelsicherung und -analyse). In den Verfahren zur Online-Durchsuchung, zur Vorratsdatenspeicherung und zum BKA-Gesetz vor dem Bundesverfassungsgericht diente Felix Freiling als sachverständige Auskunftsperson.

III. Lehrziele

Dieses Mikromodul dient als Einführung in die Grundprinzipien forensischer Arbeit und bettet die digitale Forensik in den Kanon klassischer forensischer Wissenschaften ein.

Nach erfolgreicher Bearbeitung dieses Mikromoduls können Sie die die Grundkonzepte forensischer Wissenschaften (Spuren, klassifizierende und individualisierende Merkmale, Assoziation) in praktischen Fallkonstellationen erkennen und die Begriffe auch im Kontext digitaler Spuren anwenden.

Forensische Prinzipien: von *digital* zu *cyber*

1 Klassische Forensische Wissenschaften

Bevor wir uns mit digitaler Forensik als solcher beschäftigen können, betrachten wir zunächst Forensik im Allgemeinen, denn die Entwicklung forensischer Wissenschaften begann lange vor der Erfindung des digitalen Computers. Auch wenn Methoden der digitalen Forensik mittlerweile Eingang in den Kanon der allgemein akzeptierten forensischen Wissenschaften gefunden haben, sprechen wir manchmal von der *klassischen* Forensik, wenn wir explizit die forensischen Wissenschaften vor der Einführung des Computers meinen, also die *nicht-digitale* Forensik. Bezeichnungen wie *analoge* Forensik (als Gegenpol zu *digital*) oder *virtuelle* Forensik bzw. *Cyberforensik* (als Gegenpol zu *physisch*) führen unserer Erfahrung nach in die Irre und werden nicht verwendet.

1.1 Forensische Wissenschaften

Das Attribut *forensisch* stammt vom lateinischen Wort *forum* (Marktplatz) ab. Früher war der Marktplatz der Schauplatz von Gerichtsverfahren. Mit forensisch wird jeder Bezug zu Aspekten des Rechtssystems bezeichnet. Die forensische Wissenschaft (häufig abgekürzt als *Forensik*) ist demnach die Anwendung wissenschaftlicher Methoden auf Fragen des Rechtssystems, etwa zur Untersuchung und Verfolgung von Straftaten.

Im üblichen Sprachgebrauch verleiht das Attribut *wissenschaftlich* vielen Sachverhalten eine hohe Glaubwürdigkeit. Im gleichen Zuge kann man einen Vorgang leicht diskreditieren, wenn man ihn als unwissenschaftlich bezeichnet. Viele Menschen, auch viele Wissenschaftler, verbinden Wissenschaft mit Wahrheit. In diesem Abschnitt möchten wir ein differenziertes Verständnis für Wissenschaft wecken, nämlich Wissenschaft als einen nie endenden Prozess, der nur eingeschränkt etwas mit einer universellen Wahrheit zu tun hat (unabhängig davon, ob diese überhaupt existiert). Anschließend gehen wir auf besondere Aspekte forensischer Wissenschaften ein.

Die wissenschaftliche Methode

Mit Wissenschaft bezeichnen wir die Methode, mit der der Mensch versucht, die Welt um sich herum zu beschreiben und zu verstehen. Wir möchten dabei allgemeine Regeln und Prinzipien aufstellen, die die Welt erklären. Beispiele hierfür sind die Naturgesetze in der Physik, etwa der Zusammenhang zwischen Masse, Beschleunigung und Geschwindigkeit. Derartige Regeln können auf verschiedene Arten hergeleitet werden. Ein häufiger Ansatz besteht darin, dass wir wiederkehrende Muster in unserer Umwelt wahrnehmen und diese in Form allgemeiner Regeln beschreiben. Wenn man glaubt, eine allgemeine Regel entdeckt zu haben, kann man diese Regel durch Experimente prüfen. Hier schließt man vom Speziellen auf das Allgemeine. Experimente müssen dabei nicht zwangsläufig quantitative, also messbare Daten hervorbringen. Auch qualitative Daten, die durch bloße Beobachtung entstehen, können wichtig sein. Bei physikalischen Experimenten muss man beispielsweise nicht immer die Geschwindigkeit eines Objektes exakt messen, es reicht häufig aus zu beobachten, ob ein Objekt schneller ist als das andere.

Ein zentraler Bestandteil der wissenschaflichen Methode sind *Hypothesen*. Hypothesen sind Aussagen, deren Gültigkeit untersucht werden kann. Dies geschieht beispielsweise durch Experimente. Das Aufstellen von Hypothesen ist also genauso wichtig wie ihre Überprüfbarkeit. Das zentrale Merkmal von Überprüfbarkeit ist die Falsifizierbarkeit einer Hypothese [Popper, 1962]. Es muss also ein Experiment

existieren, dessen möglicher Ausgang die Hypothese widerlegt. In der Realität ist es generell unmöglich, ein Prinzip als allgemeingültig nachzuweisen. Man kann höchstens daran scheitern, es zu widerlegen. Solange ein Prinzip trotz vielfacher Anstrengung nicht widerlegt wurde, wird es akzeptiert und gilt in diesem Sinne innerhalb der wissenschaftlichen Gemeinschaft als richtig. Diese Art von systematischem Zweifel garantiert eine möglichst hohe Objektivität wissenschaftlicher Erkenntnisse.

Insbesondere in forensischen Wissenschaften werden häufig Zusammenhänge als richtig dargestellt, wie etwa die Behauptung, dass die Kugel am Tatort von einer bestimmten Waffe abgefeuert wurde. Als (forensischer) Wissenschaftler muss man sich jedoch immer vor Augen halten, dass man diese Tatsache im Sinne wissenschaftlicher Arbeit nicht beweisen kann. Nur wenn man wiederholt und mit adäquaten Methoden daran scheitert, den Zusammenhang zu widerlegen, kann man schließlich zur Überzeugung gelangen, dass die Kugel tatsächlich durch die Waffe abgefeuert wurde. In anderen Kontexten kann man durch bestimmte Tests die Wahrscheinlichkeit bestimmter Tatbestände beziffern, etwa bei der DNA-Analyse. Hier kann man auch durch den Vergleich der Wahrscheinlichkeiten bestimmter Sachverhalte einschätzen, welcher Tatbestand am wahrscheinlichsten ist. Aber selbst eine hohe Wahrscheinlichkeit bestätigt nicht die Richtigkeit einer Hypothese.

Hypothesen und Experimente müssen nachvollzogen und durch die Fachgemeinschaft begutachtet werden können. Dies ist ein weiterer wesentlicher Bestandteil der wissenschaftlichen Methode. Die Präsentation von wissenschaftlichen Ergebnissen (Hypothesen und Experimente) geschieht in der Regel auf wissenschaftlichen Konferenzen oder in Fachzeitschriften. Dabei werden die Resultate vor der Veröffentlichung durch unabhängige und anerkannte Experten bewertet. Ergebnisse, die diesen Auswahlprozess überstanden haben, werden in den Fundus des akzeptierten Wissens aufgenommen. Die Veröffentlichung dient dazu, die Ergebnisse der Fachgemeinschaft dauerhaft zugänglich zu machen. Auf dieses veröffentlichte Wissen wird in neuen Arbeiten dann in Form von Zitaten Bezug genommen. Auch haben Veröffentlichungen, die keinem Begutachtungsprozess unterliegen, wie etwa „Whitepapers“ oder Einträge in Diskussionsforen im Internet, einen deutlich geringeren wissenschaftlichen Wert. Erst durch die Aufarbeitung der Ergebnisse im Rahmen einer begutachteten Publikation werden diese wirklich von der Fachgemeinschaft wahrgenommen. Wissenschaft ist darum immer auch ein Produkt von mehreren Personen, nicht von Einzelnen. Der Stand der Technik ist das Produkt einer gemeinsamen Überzeugung, die im fachlichen Austausch entsteht. Diese reflektierte Überzeugungskraft ist ein wesentlicher Faktor, warum Wissenschaftlern hohe Glaubwürdigkeit zugemessen wird. Schließlich geht es vor Gericht auch darum, eine Person (den Richter) oder eine Menge von Personen (die *jury*) von einem gewissen Sachverhalt zu überzeugen.

Zur Dauerhaftigkeit wissenschaftlicher Erkenntnisse

Die eben gemachten Ausführungen zeigen, dass der *Stand der Wissenschaft* immer nur die jeweils aktuell akzeptierte „Wahrheit“ wiedergibt, also die zur Zeit präziseste Beschreibung der Regeln, die die Welt regieren. Diese Beschreibung ändert sich immer dann, wenn es neue Erkenntnisse gibt, die bestehende Prinzipien widerlegen. Die Wissenschaft ist auch von zeitlichen Strömungen und Moden abhängig, vor allem in vielen Geisteswissenschaften wie etwa der Philosophie oder der Literaturwissenschaft, wodurch ein Mehrwert gerade durch die Einbringung der eigenen Subjektivität entsteht. Dennoch ist der Wissensstand auch in diesen Bereichen nicht vollkommen beliebig. Dies liegt auch an der Natur der wissenschaftlichen Methode, die eher dazu tendiert, Erkenntnisse zu *verfeinern* statt sie

grundlegend zu widerlegen. Einige historische Ausnahmen („Die Erde ist eine Scheibe.“) bestätigen die Regel.

Wie weiter unten deutlich werden wird, gibt es auch in den forensischen Wissenschaften zwar immer wieder große Umbrüche, die unser Verständnis für bestehende Sachverhalte grundlegend verändern. Die Entdeckung verschiedener Blutgruppen etwa erlaubte es, die Zuordnung von Blutspuren zu bestimmten Personen auszuschließen. Zuletzt revolutionierte die Akzeptanz von DNA-Tests vor Gericht die Arbeit von Ermittlern. DNA-Tests sind aber auch gleichzeitig ein Beispiel für die erstaunliche Dauerhaftigkeit des wissenschaftlichen Fortschritts, denn erst mit der Einführung dieser Tests konnten Blutspuren von Personen mit der gleichen Blutgruppe unterschieden werden. Erkenntnisse, die allein auf Blutgruppen basierten, wurden nicht plötzlich falsch, denn unterschiedliche Blutgruppen ergeben auch unterschiedliche DNA-Profile. Durch den neuen Test konnten jedoch andere und genauere Unterscheidungen getroffen werden als vorher.

Forensische Wissenschaften, Kriminalistik und Kriminologie

Man unterscheidet häufig zwischen reinen und angewandten Wissenschaften. Reine Wissenschaften versuchen, Erkenntnisse über die Welt um ihrer selbst Willen zu erzielen. Ein gutes Beispiel ist die reine Mathematik, die die Gesetzmäßigkeiten von Zahlen untersucht, ohne eine konkrete Anwendung im Blick zu haben. Forensische Wissenschaften sind jedoch in der Regel angewandte Wissenschaften – ähnlich wie weite Bereiche der Medizin oder der Ingenieurswissenschaften. Der Grund hierfür wurde eingangs erwähnt und wird später noch eingehed erläutert: Ausgangspunkt der Arbeit eines forensischen Wissenschaftlers ist in der Regel immer eine juristische Fragestellung, deren Beantwortung durch die wissenschaftlichen Methoden einer Disziplin unterstützt werden soll. Dies manifestiert sich auch darin, dass forensische Wissenschaftler eher analysieren als experimentieren.

Dennoch ergeben sich immer wieder auch Fragestellungen, die die Natur forensischer Wissenschaften an sich oder einer speziellen forensischen Wissenschaft betreffen. Und grundsätzliche Untersuchungen in einem Fach, etwa zu mechanischen Ursache/Wirkungsbeziehungen in der Physik oder zur prinzipiellen Lösbarkeit algorithmischer Probleme in der Informatik, helfen auch immer, den Einsatz der jeweiligen wissenschaftlichen Methoden für forensische Zwecke zu verbessern. Die Inhalte dieses Mikromoduls etwa, das versucht, das gesamte Gebiet der forensischen Wissenschaften zu hinterfragen und zu systematisieren, ist eher Ausdruck eines allgemeinen Erkenntnisinteresses als angewandter Forschung.

Im späten 19. Jahrhundert prägte Hans Groß den Begriff *Kriminalistik* für die damals neu aufkommenden Untersuchungsmethoden der Polizei. In seinem *Handbuch der Kriminalistik* [Groß and Geerds, 1977] entwickelte Groß den Begriff zunächst als Oberbegriff für alle Arten von Polizeiwissenschaften, nämlich als „Lehre von der [...] Bekämpfung der Kriminalität durch die Strafverfolgungsorgane [...] in der Lebenswirklichkeit“ [Groß and Geerds, 1977, S. 5]. Auch Groß grenzte seinen Begriff von den rechtswissenschaftlichen Fragestellungen ab, die mit der Bekämpfung von Kriminalität einhergehen (Fragen des Strafrechts und des Strafprozessrechts). Im Fokus des Interesses standen für ihn aber immer die einzelne Straftat sowie die technischen und organisatorischen Maßnahmen, die man ergreifen muss, um diese Tat aufzuklären oder zu verhindern. Hierunter fallen vier Bereiche [Groß and Geerds, 1977, S. 8]:

1. Die *Verbrechenstechnik*, also die Phänomenologie kriminellen Verhaltens, legt ein starkes Gewicht auf die *mehr handwerkliche Seite der Tatausführung*

und weniger etwa auf die Beweggründe des Täters. Man spricht in diesem Zusammenhang auch vom *Modus Operandi*.

2. Die *Kriminaltechnik* zielt auf die Erbringung von *Sachbeweisen* zur Aufklärung von Straftaten. Traditionell geht es hierbei um die Sicherung und Analyse physischer Spuren wie etwa Blutspuren, Schmauchspuren oder Fingerabdrücke.
3. Während die Kriminaltechnik die geeigneten Mittel und Untersuchungstechniken bereitstellt, geht es bei der *Kriminaltaktik* darum, wie man diese Mittel in einem größeren Zusammenhang sinnvoll und ökonomisch anwendet. In diesen Bereich gehören beispielsweise die Tatortarbeit, die Fahndung und die Vernehmung. Dabei muss auch die Frage nach der Zulässigkeit bestimmter Untersuchungsmethoden in einem gegebenen Kontext betrachtet werden.
4. Schließlich gibt es noch die *Organisation der Verbrechensbekämpfung* insgesamt, also die Art und Weise, wie etwa Aufgaben zwischen Behörden und einzelnen Personen aufgeteilt sind und wie sie zusammenarbeiten. Dazu gehören die Zusammenarbeit zwischen Polizei, Staatsanwaltschaft und Gerichten sowie die internationale Kooperation zwischen den Strafverfolgungsbehörden.

Die Kriminalistik orientiert sich insgesamt eher an den Natur- und Ingenieurswissenschaften und grenzt sich dadurch mehr oder weniger scharf von der *Kriminologie* ab, also der Lehre von den Ursachen und den Erscheinungsformen der Kriminalität, die eher den Sozialwissenschaften und der Psychologie zugeordnet wird.

Der Begriff der Kriminalistik wird heute mit unterschiedlichen Bedeutungsnuancen verwendet. Hervorzuheben ist jedoch, dass immer eine einzelne Straftat und die eher handwerkliche Seite der Tatausführung im Zentrum des Interesses steht und dass sowohl repressive als auch präventive Maßnahmen darunter fallen [Weihmann, 2007].

E

Exkurs 1: Die „sozialistische“ Kriminalistik

Aus deutscher Sicht ist bemerkenswert, dass sich der Kriminalistikbegriff nach dem zweiten Weltkrieg in den beiden deutschen Staaten unabhängig und zum Teil sehr unterschiedlich entwickelte. So wurden zentrale Begriffe wie *Spur*, *Individualisierung*, *Assoziation* und *Transfer* (auf die später noch detailliert eingegangen wird) in der „sozialistischen Kriminalistik“ [Schurich and Scharf, 1979] der DDR unabhängig von der westlichen Literatur entwickelt (siehe etwa Schurich [1974, 1982], Schurich and Scharf [1979]). Bis in die 1990er Jahre war die Kriminalistik zudem an der Humboldt Universität zu Berlin als eigenständiges wissenschaftliches Fach mit mehreren Professuren vertreten, während in der Bundesrepublik die Kriminalistik allenfalls als Teilgebiet der Rechtswissenschaften in Erscheinung trat. Problematisch erscheint hingegen der Begriff der *Version*, der heute oft mit dem Begriff der Hypothese gleichgestellt wird, in der DDR jedoch einen Wahrheitsanspruch hatte, der dem oben skizzierten (und hier angenommenen) Wissenschaftsbild widerspricht [Weihmann, 2008].

Wir werden den Begriff der Kriminalistik im Folgenden meiden und stattdessen von forensischen Wissenschaften sprechen. Hierdurch treten einerseits die Bezüge zu anderen Wissenschaften wie der Biologie oder der Informatik deutlicher zu Tage. Andererseits reflektiert dies auch den angelsächsischen Sprachgebrauch vor

allem in den USA, wo eher von *forensic science* gesprochen wird und selten von *criminalistics*. Allerdings tritt dadurch die Beziehung zwischen ermittelnder Polizeiarbeit und Spurenanalyse etwas in den Hintergrund, was gerade von Vertretern einer „allgemeinen" forensischen Wissenschaft kritisch gesehen wird [Margot, 2011]. Wie oben bereits erwähnt, tut man gut daran, die eigenen wissenschaftlichen Erkenntnisse nicht als einzig wahr zu beurteilen; was (eine) Wissenschaft ist und was nicht, hängt auch von gesellschaftlichen Entwicklungen ab und kann sich ändern. Wesentlich ist das Erkenntnisinteresse der beteiligten Personen, ein Phänomen besser zu verstehen oder eine Straftat aufzuklären.

Forensische Wissenschaft und das Rechtssystem

Ohne das Rechtssystem gäbe es keine forensischen Wissenschaften. Die Ziele und Fragestellungen beider Bereiche sind jedoch grundsätzlich verschieden. In einem Rechtsstreit geht es ausschließlich darum, rechtliche Fragen zu beantworten. Diese beziehen sich darauf, ob ein Rechtsverstoß stattgefunden hat und falls ja, welcher. Schlussendlich kann die rechtlichen Fragen nur das Rechtssystem bzw. der Richter beantworten. Die Aufgabe forensischer Gutachter ist es, die rechtlichen Fragen in wissenschaftliche Fragen zu übersetzen. Wenn das nicht möglich ist, sind forensische Wissenschaftler fehl am Platze. Die Frage, ob ein Beschuldigter tatsächlich einen Mord begangen hat, kann beispielsweise in die Frage übersetzt werden, welche genetischen Sequenzen in den Blutspuren am Tatort gefunden werden können. Eine Antwort auf die wissenschaftliche Frage kann anschließend helfen, eine Antwort auf die rechtliche Frage zu finden. Allerdings hilft nicht jede wissenschaftliche Frage bei der Wahrheitsfindung. Der Nachweis, dass sich Blutspuren des Tatverdächtigen an seinen eigenen Schuhen befinden, hilft nicht notwendigerweise bei der Beantwortung der Frage, ob der Tatverdächtige den Mord begangen hat. Genauso wenig hilft es herauszufinden, dass sich auf der Tatwaffe mikroskopische Fasern aus der Kleidung des Opfers befinden, wenn der Tatverdächtige Kleidung trägt, die auch aus diesen Fasern besteht.

Übersetzt man die rechtliche Frage in eine wissenschaftliche Frage, verliert man jeden Bezug zu den Begriffen Schuld und Unschuld. Forensische Wissenschaften suchen immer nach Verbindungen zwischen Objekten, beispielsweise zwischen dem Blut, das sich am Tatort und der Tatwaffe befindet, und dem Blut des Opfers und des Tatverdächtigen. Über Schuld oder Unschuld entscheidet ausschließlich das Gericht.

Frühe literarische Bezüge

Seit ihren Anfängen umgibt die forensischen Wissenschaften eine Aura von Geheimnis und Zauberei. Dazu beigetragen haben auch die forensischen Praktiker, welche die Fähigkeit, von wenigen Spuren am Tatort nahezu den kompletten Fall zu rekonstruieren, als Ausdruck von Scharfsinnigkeit und Talent etablierten. Leider führte dies dazu, dass es immer schwieriger wurde, echte Experten von Scharlatanen zu unterscheiden, die mitunter andere Interessen als die Wahrheitsfindung hatten [Inman and Rudin, 2000, S. 22]. Die Selbstüberschätzung von forensischen Experten basiert vermutlich teilweise auf den Anfängen der Kriminalliteratur, die viele Fortschritte bei den polizeilichen Ermittlungsmethoden begeistert aufnahm und dramaturgisch überhöhte.

Das bekannteste Beispiel ist der geniale Spurenleser und Detektiv Sherlock Holmes, der im London des späten 19. und frühen 20. Jahrhunderts Straftäter mit Scharfsinnigkeit und einem Vergrößerungsglas überführt. Beispielsweise identifiziert Holmes in *The Red-Headed League* (deutscher Titel: Der Bund der Rotschöpfe) die gerauchte Zigarettenmarke anhand von Aschespuren oder die Herkunft einer

Person anhand von Dreckspuren am Mantel. Sir Arthur Conan Doyle (1859–1930), der literarische Vater dieser Detektivgeschichten, war bekannt dafür, dass er aktuelle Fortschritte der Polizeiwissenschaften regelmäßig studierte und in seine Romane integrierte. In *A Study in Scarlet* (deutscher Titel: Eine Studie in Scharlachrot) erfindet Holmes etwa einen verbesserten Test zum Nachweis von Blut. Auch forensische Wissenschaftler, wie der Franzose Edmund Locard, nehmen in ihren Arbeiten direkten Bezug auf Fälle aus der Holmes-Literatur [Inman and Rudin, 2000, S. 24].

In der Literaturwissenschaft gilt nicht Doyle, sondern Edgar Allen Poe (1809–1849) als der Erfinder des Genres der Detektivromane. In *A Study in Scarlet* bezieht sich Doyle direkt auf die durch Poe eingeführte Detektivfigur des Auguste Dupin. Typisch für die allwissende Attitüde der Holmes'schen Figur disqualifiziert dieser seinen literarischen Vorgänger als *minderwertig* (*inferior*). Gerade diese Haltung, welche die Person Holmes so interessant macht, ist leider ein schlechtes Vorbild für moderne forensische Experten, denen Bescheidenheit besser ansteht als Angeberei.

Auch Mark Twain, der nicht gerade für Detektivgeschichten bekannt ist, verfolgte die Entwicklungen der Polizeiwissenschaften mit großem Interesse. In *The Tragedy of Pudd'nhead Wilson*, geschrieben 1894, erzählt er die Geschichte eines Anwalts, der zwei Brüder vor der Verurteilung rettet, indem er nachweist, dass die blutigen Fingerabdrücke auf einem Messer nicht von diesen stammen [Inman and Rudin, 2000, S. 28]. Mit der detaillierten Beschreibung der Abdrücke und deren charakteristischen Eigenschaften ist Twain seiner Zeit voraus, denn es sollten noch einige Jahre ins Land gehen, bevor Fingerabdrücke als identifizierendes Merkmal vor Gericht akzeptiert wurden.

Analyse von Spuren zur Identifizierung von Personen

Die Besonderheit von Fingerabdrücken ist spätestens seit dem 17. Jahrhundert bekannt, aber ihr konkreter Nutzen bei der Identifizierung von Personen ist erst im späten 19. Jahrhundert deutlich geworden. Bis dahin galt die *Anthropometrie* als einzige Möglichkeit, die Identität einer Person eindeutig zu überprüfen. Dabei mussten mehrere Bereiche des Körpers genau vermessen werden. Die Kombination dieser Messwerte sei ein individualisierendes Merkmal, behauptete jedenfalls Alphonse Bertillon, der 1883 mit mehreren spektakulären Identifizierungen erst in Frankreich und dann weltweit dieser Methode zum Durchbruch verhalf [Inman and Rudin, 2000, S. 30].

Als im Jahre 1903 in einem Gefängnis in Kansas zwei Personen mit identischen anthropometrischen Merkmalen nur aufgrund ihrer unterschiedlichen Fingerabdrücke identifiziert werden konnten, war das Ende der Anthropometrie gekommen, und Fingerabdrücke wurden das primäre identifizierende Merkmal. Wegbereiter für die Wissenschaft der *Daktyloskopie* waren vor allem der englische Naturwissenschaftler Francis Galton, der 1892 ein Buch über die Aussagekraft und die statistischen Merkmale von Fingerabdrücken veröffentlichte, sowie der argentinische Kriminologe Ivan Vučetić (auch: Juan Vucetich), der ein standardisiertes Klassifikationssystem für Fingerabdrücke erfand. Seitdem sind vor allem bei den Möglichkeiten der Sicherung von Fingerabdrücken Fortschritte erzielt worden.

Ein weiterer Meilenstein bei der Analyse von Spuren war die Entdeckung verschiedener Blutgruppen um 1900 durch Karl Landsteiner, die erstmals die grobe Zuordnung von Blutspuren zu Personen erlaubte. Wenn eine Blutspur eine andere Blutgruppe hatte als eine bestimmte Person, konnte diese Person als Quelle dieser Spur ausgeschlossen werden. Durch einen von Paul Uhlenhuth 1901 entwickelten

Test war es zudem möglich, Tier- und Menschenblut eindeutig zu unterscheiden. Damit konnte die damals übliche Schutzbehauptung entkräftet werden, dass es sich bei bestimmten Spuren um Tierblut handle.

Ähnliche Fortschritte gab es im Verlauf des 20. Jahrhunderts auf vielen Gebieten der Medizin. Als Meilenstein für die Identifizierung von Personen gilt jedoch die DNA-Analyse, die in den 1980er Jahren von Sir Alex Jeffreys entscheidend vorangetrieben wurde. Der *DNA-Fingerabdruck* wird heute mit der gleichen Überzeugung als individualisierendes und identifizierendes Merkmal aufgefasst wie fast 100 Jahre zuvor der Fingerabdruck.

1.2 Spuren und ihre Entstehung

Eine Spur wird als ein *hinterlassenes Zeichen* angesehen. Das Wort *Spur* kommt ursprünglich aus dem Altgermanischen und bedeutet dort *Tritt* oder *Fußabdruck*. In der Jägersprache spricht man häufig auch von *spuren* und meint dabei das Ansetzen eines Hundes auf die Fährte [Weihmann, 2007].

Wir verwenden hier einen sehr allgemeinen Spurenbegiff und verbleiben zunächst in der physischen Welt, betrachten also physische (im Sinne von nicht-digitalen) Spuren. Eine *Spur* (*evidence*) ist dabei jedes Objekt, was ein Argument plausibler macht. In der juristischen Fachsprache spricht man statt von Spur auch häufig von *Beweismittel*. Eine Spur ist demnach ein Gegenstand zusammen mit einer Reihe von dokumentierten Behauptungen (*claim*) oder Annahmen (*assumption*) über diesen Gegenstand. Diese Behauptungen beschreiben im Wesentlichen die *Herkunft* (*provenance*) der Spur, etwa den Fundort und die Zeit des Auffindens.

In der realen Welt kann nahezu alles zur Spur werden. Weihmann [2007] verzeichnet in seinem Buch mehr als ein Dutzend verschiedener Arten von Spuren. Im Handbuch von Groß and Geerds [1977] umfasst der Abschnitt zu Spurenkunde und deren Untersuchung mehr als 200 Seiten. Die Palette reicht von Blut, Haaren und Sekreten über Wasser, Boden, Vegetation, Luft und Gas bis hin zu Metall, Kunststoff, Holz und Textilien. Etwas wird zur Spur, wenn es eine Beziehung zum untersuchten Sachverhalt, z. B. der Straftat, aufweist [Kirk, 1974, S. 6]. Kirk [1974, S. 1 ff.] macht deutlich, wie wichtig derartige Spuren bei Ermittlungen sein können, denn es ist nahezu unmöglich, Handlungen auszuführen, ohne irgendwelche Spuren zu hinterlassen. Kirk [1974, S. 2] schreibt:

> „Not only his fingerprints and his shoeprints, but also his hair, the fibers from his clothes, the glass he breaks, the tool marks he leaves, the paint he scratches, the blood or semen he deposits or collects – all these bear mute witness against him."

Wir betrachten im Folgenden allgemeine Eigenschaften von Spuren und die Prinzipien, die bei der Entstehung solcher Spuren eine Rolle spielen.

Spureninformation und Spurenträger

Betrachten wir zur Illustration als stereotype Spur einen blutigen Handschuh, der am Tatort eines Tötungsdelikts gefunden wird. Wenn an dem Handschuh DNA-Spuren des Täters zu finden sind, dann wird der Handschuh zur Spur. Hilfreich ist der blutige Handschuh, weil mit ihm die Verbindung von Täter zu Tatort gezogen werden kann. Diese Verbindung entsteht jedoch genau genommen aus den Informationen, die innerhalb der DNA gespeichert sind. Die DNA selbst (und schlussendlich auch der blutige Handschuh) sind nur die Träger dieser Information.

Allgemein unterscheidet man bei Spuren zwischen *(Spuren-)Information* (*information*) und *(Spuren-)Träger* (*support*). Die Information ist die „Bedeutung" der Spur, also das, was sie aussagt. Der Träger ist diejenige Materie, die diese Bedeutung trägt. Ein anderes Beispiel für den Unterschied zwischen Information und Träger ist ein Brief, der am Tatort gefunden wird. Der Träger ist das Papier und die Tinte, aus denen der Brief besteht. Die Information ist (unter anderem) die auf dem Brief codierte Bedeutung der Schriftzeichen.

In der klassischen Forensik ist die Unterscheidung zwischen Spurenträger und Spureninformation recht unintuitiv, weil eine starke Verbindung besteht zwischen Träger und Information (wie im Beispiel DNA zu Blut oder Text zu Brief): Information und Träger werden dort leicht als Einheit betrachtet, die nicht aufgetrennt werden kann. Aber schon bei einem Brief ist diese Verbindung schon etwas weniger stark. Betrachtet man beispielsweise ein Erpressungsschreiben, dann ist im Wesentlichen die Bedeutung der geschriebenen Worte (also die Spureninformation) für den Fall relevant und es ist egal, mit welcher Schreibmaschine, mit welcher Tinte oder auf welchem Briefpapier der Brief geschrieben wurde. Der Spurenträger kann jedoch weitere Informationen enthalten, etwa die Form der (Hand-)Schrift, die benutzt werden kann, um die Spur einer Person oder einer Schreibmaschinen zuzuordnen. Wir werden diesen Unterschied in Abschnitt 2, in dem es um digitale Spuren geht, noch klarer sehen.

Alle physischen Spuren sind — wie jede Materie — vergänglich. Genauer gesagt sind die Spurenträger vergänglich, auch wenn der Grad der Vergänglichkeit sehr unterschiedlich sein kann. Bei physischen Spuren haben wir heute ein recht gutes Verständnis von ihrer Vergänglichkeit.

Integrität und Authentizität von Spuren

Ermittler suchen am Tatort nach Spuren, die über den Tathergang Aufschluss geben können. Insbesondere Spuren, die unabsichtlich hinterlassen werden, wie etwa Fingerabdrücke, Fasern oder Sekrete, sind für die Ermittler interessant. Diese sind jedoch in der Regel schwer zu erkennen und müssen von Spezialisten gesucht und aufgenommen werden. Dieser Vorgang wird allgemein auch *Spurensicherung* genannt. Bei der Sicherung einer Spur entstehen die ersten Behauptungen, die in irgend einer Form an die Spur geheftet werden, etwa als Aufschrift auf einem Asservatenbeutel (*evidence bag*) oder als Eintrag in einem Durchsuchungsbericht.

Spuren können eine Theorie über einen Tathergang stützen oder widerlegen. Die Überzeugungskraft solcher Spuren hängt stark davon ab, wie „nahe" die (vor Gericht) vorgelegten Spuren an den Spuren sind, die am Tatort gefunden wurden. Allgemein versucht man diese Nähe mit zwei Begriffen zu fassen, nämlich mit der *Integrität* und *Authentizität* von Spuren:

- *Integrität* bedeutet grob gesprochen, dass die Spur seit ihrer Sicherung nicht verändert wurde. Integrität ist aber keine Eigenschaft, die sofort verloren geht, wenn sich die Spur verändert. Da alle Materie vergänglich ist, wird es auch nach kurzer Zeit schon Veränderungen am gesicherten blutigen Handschuh geben (beispielsweise trocknet das Blut). Veränderungen können sogar durch den Sicherungsprozess geschehen. Die Veränderungen sollten jedoch so gering wie möglich gehalten werden. Integrität bezieht sich hauptsächlich auf die *Spureninformation* und stellt somit sicher, dass die Information unverändert vorliegt.
- *Authentizität* bedeutet, dass die vorgelegte Spur tatsächlich die Spur ist, die durch die mit ihr verbundenen Behauptungen beschrieben wird. Wenn von der Spur behauptet wird, dass es sich dabei um den blutigen Handschuh

vom Tatort handelt, dann ist die Spur authentisch, wenn es sich tatsächlich um *den* blutigen Handschuh vom Tatort handelt. Bei physischen Objekten definiert sich Authentizität also hauptsächlich durch den *Spurenträger*.

B

Beispiel 1: Authentizität vs. Integrität

Um den Unterschied zwischen Authentizität und Integrität darzulegen, nehmen wir das oben eingeführte Beispiel des blutigen Handschuhs vom Tatort und betrachten zwei Fälle:

1. Angenommen die Spur behauptet, sie ist der blutige Handschuh vom Tatort, der *unter* der Leiche gefunden wurde. In Wirklichkeit ist sie ist aber der blutige Handschuh vom Tatort, der *auf* der Leiche gefunden wurde. Die Spur erfüllt (falls sie nicht verändert wurde) zwar Integrität aber nicht Authentizität.
2. Falls die Spur behauptet, der blutige Handschuh zu sein, der auf der Leiche gefunden wurde, und es sich tatsächlich um diesen Handschuh handelt, der jedoch nach der Sicherung einmal mit der Waschmaschine gewaschen worden ist, dann erfüllt die Spur Authentizität aber nicht Integrität (jedenfalls nicht in hohem Maße).

Beide Begriffe machen also nur Sinn, wenn eine Spur als Einheit von Information und Träger verstanden wird.

Nur die Kombination von Integrität und Authentizität erlaubt es sicherzugehen, dass die Spur tatsächlich sinnvoll und hilfreich für die Wahrheitsfindung interpretiert werden kann. Spuren müssen also authentisch sein und ein Mindestmaß an Integrität besitzen. Wenn die Integrität verloren geht (bzw. die Integrität unter ein bestimmtes Maß sinkt), dann kann man bestimmte Schlüsse nicht mehr aus den durch die Spur dargelegten Informationen ziehen: Wenn der Handschuh gewaschen worden ist, ist möglicherweise die DNA des Täters verschwunden (ganz zu schweigen von der Möglichkeit, dass fremde DNA auf den Handschuh gelangt ist). Ähnliches gilt für die Authentizität. Die Sicherung und spätere Behandlung von Spuren muss also so erfolgen, dass die Spuren möglichst wenig verändert werden. Um dies zu gewährleisten, wird der Tatort in der Regel großräumig abgesperrt und darf nur von befugten Personen betreten werden. Diese Personen tragen zudem häufig Schutzanzüge, um nicht versehentlich selbst Spuren am Tatort zu hinterlassen.

Authentizität und Integrität beruhen stark auf Annahmen, etwa dass die mit der Spur betrauten Personen ordnungsgemäß und verlässlich gearbeitet haben. Neben der Gefahr einer Modifikation bei der Spurensicherung müssen im weiteren Verlauf der Untersuchung alle weiteren Gefahren, welche die Spur verändern können, eingedämmt werden. Dies kann beispielsweise dadurch erreicht werden, dass möglichst wenige und auch nur fachlich besonders qualifizierte Personen Zugang zu der Spur haben. Dies wird in der so genannten *Verwahrungskette* (*chain of custody*) dokumentiert. Die Verwahrungskette ist Teil der Dokumentation der Spurenherkuft, also Teil der mit der Spur verbundenen Behauptungen. Sie dokumentiert lückenlos, wann welche Personen Zugang zur Spur hatten. Wenn keine Personen Zugang zur Spur haben sollen, wird diese in einer besonders geschützten Umgebung (Asservatenkammer) aufbewahrt. Aber auch hier muss man annehmen (und darauf vertrauen), dass die Verwahrung ordnungsgemäß und verlässlich organisiert worden ist.

Nach der Sicherung werden die Spuren näher untersucht. Diesen Vorgang nennt man *Spurenanalyse*, und er geschieht meist durch Spezialisten in speziellen Laboren. In der Praxis spricht man auch von *kriminaltechnischer Untersuchung*. Dort werden die Spuren durch Experten, in der Regel Wissenschaftler (Biologen, Physiker, Chemiker, Mediziner oder Informatiker) analysiert.

Klassifikation von Spuren

Nachdem fast jede Art von Materie zur Spur werden kann, gibt es auch viele verschiedene Möglichkeiten, physische Spuren zu klassifizieren. Lee and Harris [2000, S. 5ff] zählen allein sieben verschiedene Klassifikationsarten auf. Am häufigsten findet man die Klassifikation nach Straftat [Lee and Harris, 2000, Groß and Geerds, 1977], aber auch stärker naturwissenschaftlich orientierte Klassifikationsschemata werden verwendet, etwa die Klassifikation nach der chemischen oder biologischen Zusammensetzung.

Lee and Harris [2000, S. 5] unterscheiden darüber hinaus noch *transiente* Spuren: Das sind physische Spuren, die nur temporär existieren und demnach leicht verloren gehen können. Beispiele für transiente Spuren sind Gerüche, etwa von Benzin, Parfüm, Rauch oder Urin. Weitere Beispiele sind Temperaturen von Gegenständen, etwa die Temperatur eines Motors, die Wassertemperatur in einer Badewanne oder die Körpertemperatur einer Leiche. Transiente Spuren müssen ohne Zeitverzug entdeckt und wenn möglich auch gesichert werden. Da die Sicherung der Spur aufgrund ihrer Natur häufig schwer bis unmöglich ist, kann man die Existenz und die Beschaffenheit der Spuren nur schriftlich festhalten und von anderen Beobachtern am Tatort bestätigen lassen. Manche transiente Spuren können auch fotografiert oder auf Video aufgezeichnet werden.

Eine Spur weist notwendigerweise eine Beziehung zum untersuchten Sachverhalt auf. Bei vielen Gegenständen, wie beispielsweise bei einer Schusswaffe oder einem Brecheisen, ist diese Beziehung deutlich erkennbar. Kirk [1974, S. 6] weist jedoch darauf hin, dass die nützlichsten physischen Spuren so klein sind, dass man sie mit bloßem Auge nicht erkennt. Kirk nennt diese Klasse von Spuren *mikroskopische Spuren*. Die Besonderheit von mikroskopischen Spuren ist, dass sie sehr leicht übersehen werden (durch den Täter wie den Ermittler) und sehr schwer zu entfernen sind. Oft werden noch Monate oder Jahre nach einer Tatausführung mikroskopische Spuren am Tatort gefunden. Die Verfügbarkeit mikroskopischer Spuren ist also in der Regel höher als die Verfügbarkeit von großen, sichtbaren Spuren. So mag es möglich sein, die Beziehung zwischen einem Fahrzeug und dem Tatort anhand von sichtbaren Reifenspuren nachzuweisen. Viel wahrscheinlicher (und wirksamer) ist es aber, dass man eine Beziehung zwischen einem Opfer und dem Fahrzeug aufgrund von Haaren, Fasern oder Sekreten herstellen kann. So gehört ein Staubsauger mit einem speziellen Filter (siehe Abbildung 1) zum Standardwerkzeug der Spurensicherung am Tatort. Die aufgenommenen Partikel werden in einer Plastiktüte aufbewahrt und im Labor unter dem Mikroskop oder mit sonstigen Methoden analysiert.

Übertragung (Transfer)

Edmund Locard beschrieb als Erster eines der Grundprinzipien bei der Entstehung von Spuren. Inspiriert durch die Arbeiten von Groß und den Abenteuern von Sherlock Holmes begann er Anfang des 20. Jahrhunderts detaillierte Untersuchungsreihen zu mikroskopischen Spuren wie Staub oder Schmutz. In einem seiner Werke [Locard, 1920] (zitiert nach Inman and Rudin [2000, S. 44]), die auf Französisch erschienen, dokumentiert er die Beobachtung, dass niemand eine Straftat begehen kann, ohne zahlreiche Zeichen (*marques multiples*) zu hinterlassen,

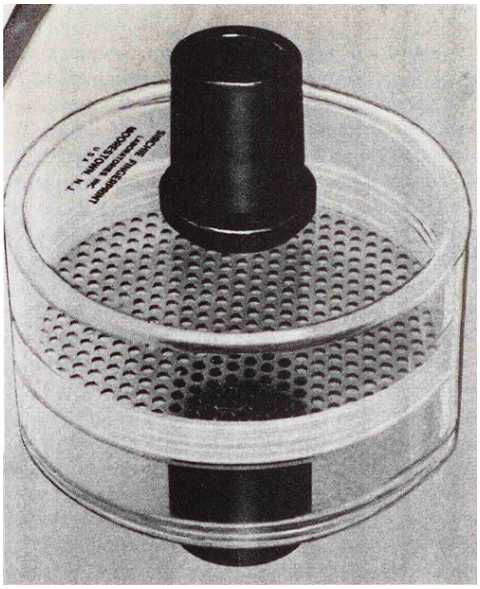

Abb. 1: Filter zur Sammlung mikroskopischer Spuren [Kirk, 1974, S. 25].

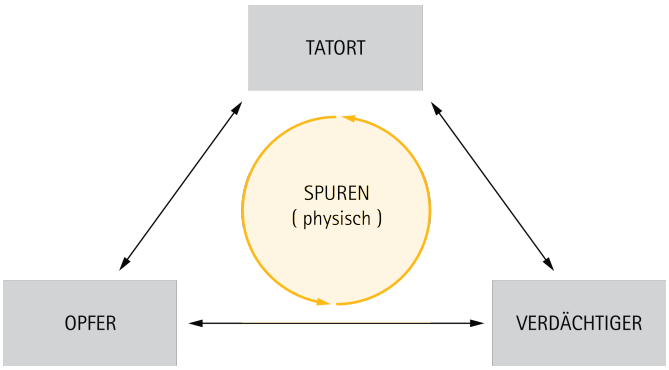

Abb. 2: Schematische Darstellung von Locards Austauschprinzip.

entweder dadurch, dass er etwas am Tatort hinterlässt oder dadurch, dass er etwas vom Tatort mitnimmt. Aus dieser Beobachtung entstand das auch populärwissenschaftlich gut dokumentierte und nach ihm benannte *Locardsche Austauschprinzip* (*Locard's exchange principle*). Es wird häufig als Dreieck zwischen Täter, Opfer und Tatort visualisiert (siehe Abbildung 2).

Heute basiert ein wesentlicher Teil der Theorie forensischer Wissenschaften auf den Einsichten von Locard. Das Austauschprinzip wurde jedoch bis heute zu einer allgemeineren Theorie der *Übertragung* weiterentwickelt. Heute sieht man die Übertragung von Materie als einen wesentlichen, aber nicht als den einzigen Weg an, wie Spuren entstehen. Auf die Grundlagen dieser Theorie gehen wir im Folgenden ein.

Zerteilbarkeit (Divisibility)

Bei genauerer Betrachtung basiert das Locardsche Austauschprinzip auf einem weiteren Prinzip: Austausch passiert nämlich nur dann, wenn sich Objekte in kleinere Teile zerteilen lassen [Inman and Rudin, 2000, Kapitel 4]. Da alle Objekte in irgendeiner Form aus zerteilbarer Materie bestehen, erscheint diese Voraussetzung häufig als selbstverständlich und trivial. Wenn Objekte aber nicht zerteilbar wären, gäbe es auch keinen Austausch.

Die Materie, aus der Objekte bestehen, wird nach Regeln der Biologie, Chemie und Physik zusammengehalten. Wenn Kräfte auf ein Objekt einwirken, dann kann

es dazu kommen, dass sich das Objekt in seine Einzelteile zerteilt. Die Einzelteile behalten aber in der Regel charakteristische Eigenschaften des ursprünglichen Objekts. Diese Eigenschaften können chemischer oder biologischer Natur sein. Abbildung 3 zeigt aber auch ein Beispiel dafür, dass auch charakteristische Muster erhalten bleiben können, wie etwa Texturen.

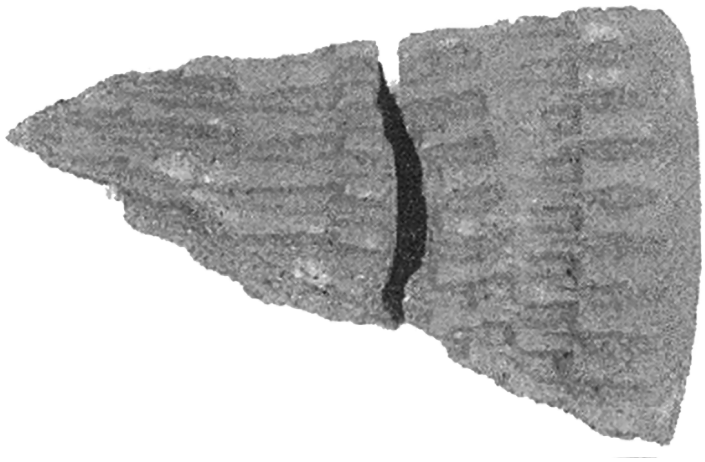

Abb. 3: Transfer von Texturen auf Bruchstücke eines Objekts [Inman and Rudin, 2000, S. 89].

Manchmal entstehen durch das Zerteilen auch neue charakteristische Eigenschaften. Als Beispiel werden häufig Riss- oder Bruchkanten angeführt (siehe Abbildung 4).

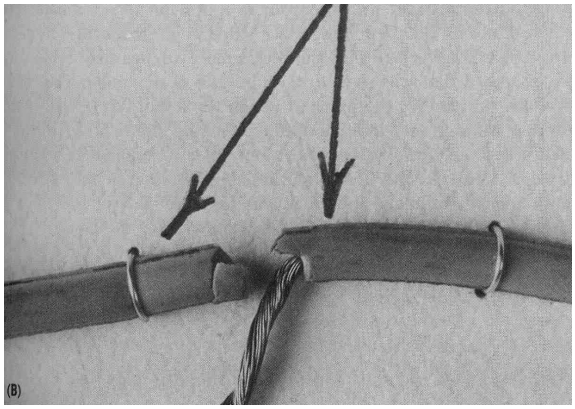

Abb. 4: Übereinstimmende Bruchkanten in einem Kabel [Kirk, 1974, S. 139].

Übertragung von Mustern

„Austausch“ im Sinne des Locardschen Austauschprinzips war immer eine Übertragung von Materie. Durch Abdrücke entsteht jedoch auch eine Form von Austausch, die nicht notwendigerweise Materie überträgt. Beispiele für diese Art von Austausch sind Fußabdrücke oder Reifenspuren. Auch wenn hierbei häufig auch Materie übertragen wird (beispielsweise Erde am Schuh oder am Reifen), so ist diese Materie nach längerer Zeit kaum mehr nachweisbar. Es bleiben die Muster, die sowohl am Schuh bzw. am Reifen als auch im Abdruck existieren.

Die Übertragung von Mustern wird auch mit *transfer of traits* bezeichnet [Inman and Rudin, 2000, S. 93]. Das Zerteilen von Objekten ist also nicht bei jedem Austausch notwendig: Wenn Materie übertragen wird, ist Zerteilung eine notwendige Voraussetzung; wenn Muster übertragen werden, dann nicht. Wir betrachten nun zwei typische Beispiele für diese Klasse von Spuren.

Das erste Beispiel ist in Abbildung 5 dargestellt. Es handelt sich um Kratzspuren eines Werkzeugs (z. B. Stemmeisen, Schraubenzieher, Axt) auf einem verformbaren

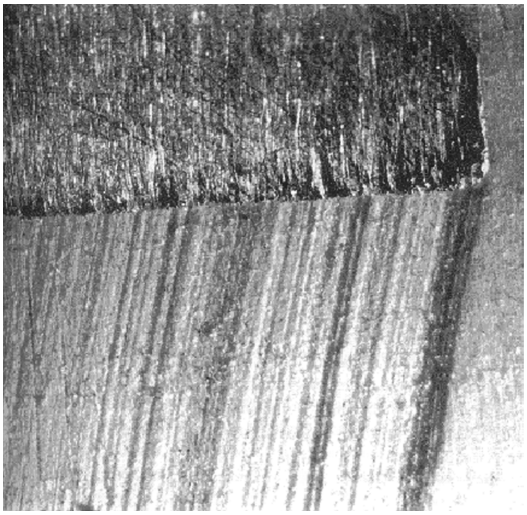

Abb. 5: Kratzspuren eines Werkzeugs (oben) auf einem verformbaren Material [Inman and Rudin, 2000, S. 97].

Untergrund. Durch die individuelle Verwendungsgeschichte eines Werkzeugs entstehen Verformungen, die für das einzelne Werkzeug jeweils charakteristisch sind. Durch diese Verformungen hinterlässt das Werkzeug bei der Verwendung charakteristische Spuren.

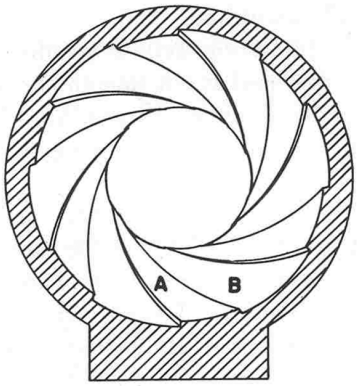

Abb. 6: Schematische Darstellung des Laufs einer Schusswaffe [Kirk, 1974, S. 387].

Als zweites Beispiel betrachten wir die Spuren, die bei der Verwendung von Schusswaffen an der Kugel entstehen. Der Lauf einer Schusswaffe enthält nämlich typischerweise ein spiralförmiges Rillenmuster (siehe Abbildung 6), das die Kugel vor dem Austritt aus dem Lauf in eine Rotation versetzt. Diese Rotation verleiht der Kugel eine deutlich bessere Flugstabilität. Da das Rillenmuster bei der Waffenherstellung mechanisch erzeugt wird und sich durch Abnutzung ändert, existieren auch bei baugleichen Waffen Unterschiede, die sich beim Schuss auf die Kugel übertragen.

Um eine am Tatort gefundene Kugel einer sichergestellten Waffe zuzuordnen, werden weitere Schüsse mit der Waffe abgegeben und die abgeschossenen Kugeln mit der fraglichen Kugel vom Tatort verglichen. Hierbei kommt ein spezielles Vergleichsmikroskop zum Einsatz, das in Abbildung 7 schematisch dargestellt ist. Unter dem Mikroskop wird die Frage untersucht, ob es Übereinstimmungen zwischen den Linienmustern auf beiden Kugeln gibt. Etwaige Übereinstimmungen können dann anhand von Fotos dokumentiert werden (siehe Abbildung 8).

Ein besonderes Beispiel ist in Abbildung 9 dargestellt. Abgebildet ist die stark vergrößerte Draufsicht einer Kugel, auf der der Abdruck eines Webmusters erkennbar ist. Dieses Muster konnte dem Stoff einer Polizeiuniform zugeordnet werden.

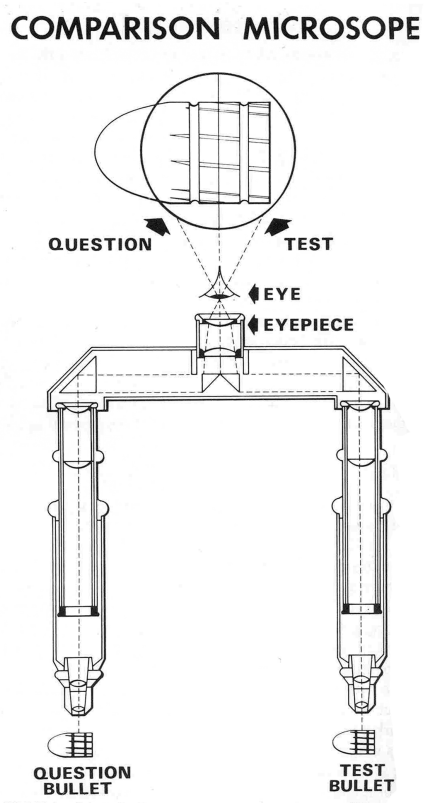

Abb. 7: Schema eines Vergleichsmikroskops [Kirk, 1974, S. 364].

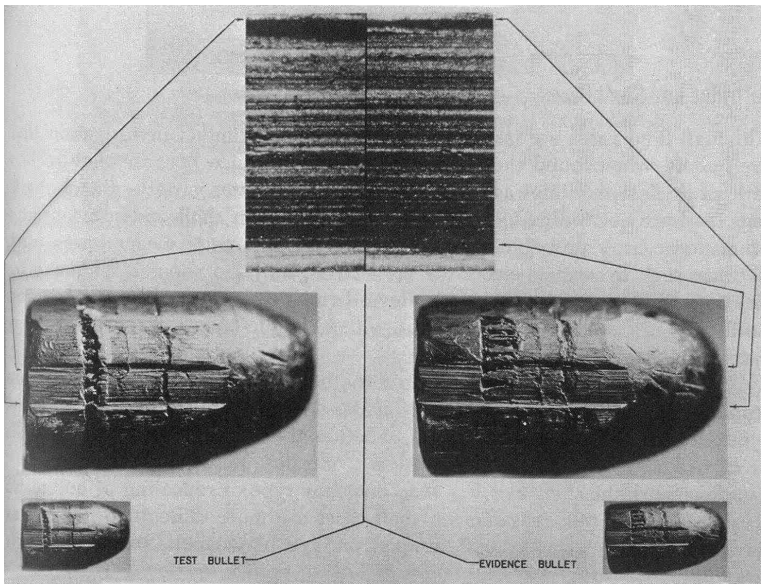

Abb. 8: Vergleich von Spuren auf Kugeln [Kirk, 1974, S. 397].

Außerdem wurden anhaftende Fasern des Uniformstoffes an dieser Kugel sichergestellt. Dies ist also ein Beispiel, bei dem sowohl die Übertragung von Materie als auch von Mustern stattgefunden hat.

Theorie des Transfers

Zusammenfassend gibt es also zwei Formen des Transfers [Inman and Rudin, 2000, Kapitel 4.D]:

1. Übertragung von Materie (*physical transfer*). Hierbei geht man in der Regel davon aus, dass sich unter einer gewissen Energieeinwirkung ein Objekt zer-

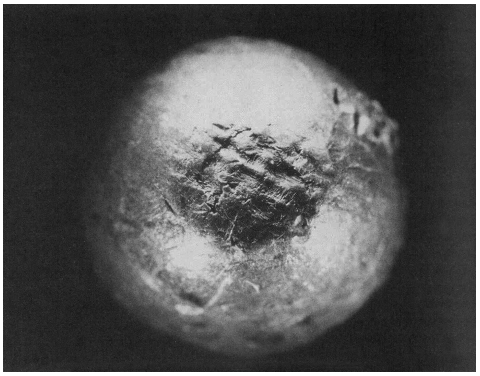

Abb. 9: Beispiel für gleichzeitigen Austausch von Muster und Materie [Kirk, 1974, S. 122].

teilt und Einzelteile davon von einer Quelle auf ein Ziel übertragen werden. Typischerweise fällt die Energie beim Kontakt an.

2. Übertragung von Mustern (*transfer of traits*). Hierbei werden charakteristische Formeigenschaften von einem Objekt auf ein anderes übertragen, ohne dass notwendigerweise Materie ausgetauscht wird.

Die Übertragung von Materie oder Mustern ist an einem Tatort in der realen Welt nie vollständig zu vermeiden. Wie zuvor bereits erwähnt, ist insbesondere die Verfügbarkeit von mikroskopischen Spuren in der Praxis sehr hoch [Kirk, 1974, S. 2]. Ein uneingeschränkter Ermittler hat (jedenfalls theoretisch) die Möglichkeit, den Tatort aus unendlich vielen Perspektiven zu betrachten. Somit besteht in der realen Welt immer eine bestimmte Wahrscheinlichkeit, dass diese Spur auch entdeckt wird [Böhme et al., 2009, S. 92f]. In der realen Welt ist deshalb eine Tat ohne Spuren (*perfektes Verbrechen*) theoretisch ausgeschlossen.

1.3 Rekonstruktion eines Tathergangs

Ziel des Ermittlers ist immer die Rekonstruktion des *wahren* Tathergangs unter Einbeziehung der aufgefundenen Spuren. Praktisch werden jeweils Hypothesen über eine Menge von möglichen Tathergängen aufgestellt, die den aufgefundenen Spuren nicht widersprechen. Gemäß der zuvor geschilderten Theorie nimmt man an, dass alle Spuren ausschließlich auf den Prinzipien der Zerteilbarkeit und des Transfers beruhen. Spuren sind dann jeweils Hinweise auf einen *Kontakt* zwischen zwei Objekten.

Ereignisse

Wenn festgestellt wurde, dass zwei Objekte in Kontakt waren, spricht man von einem *Ereignis* (*event*). *Rekonstruktion* bedeutet nun, alle ermittelten Ereignisse in einen räumlichen und zeitlichen Zusammenhang zu bringen.

Beispiele für Ereignisse sind etwa:

- Person P war am Ort X (etwa weil Fingerabdrücke von P am Ort X gefunden wurden).
- Ein Schuh S war am Ort Y (etwa weil S einen charakteristischen Sohlenabdruck an Ort Y hinterlassen hat).
- Ein Auto A war am selben Ort, an dem auch Person Q war (etwa weil man Blutspuren von Q auf der Motorhaube von A gefunden hat).

Alle diese Ereignisse müssen individuell hergeleitet und begründet werden. Die Basis dafür ist der Vorgang der Assoziation.

Assoziation

Assoziation bezeichnet den Vorgang, bei dem der Kontakt zwischen zwei Objekten festgestellt wird. Als Ergebnis der Assoziation steht ein Ereignis. Als Beispiele für eine Assoziation können genannt werden:

- Die Zuordnung eines konkreten Schuhs zu einem konkreten Schuhabdruck.
- Die Zuordnung einer konkreten Kugel zu einer konkreten Waffe.
- Die Zuordnung einer konkreten Blutspur zu einer konkreten Person.
- Die Zuordnung eines konkreten Fingerabdrucks zu einer konkreten Person.

Ein wesentlicher Bestandteil der Assoziation ist die Quantifizierung der Irrtumswahrscheinlichkeit. In den klassischen forensischen Wissenschaften wird die Quantifizierung von Assoziationsaussagen unterschiedlich gehandhabt. Häufig haben sich in der Praxis Richtwerte herausgebildet, die allgemein als Nachweis einer Assoziation akzeptiert werden (ohne exakte Quantifizierung). Ein Beispiel ist der Bereich der Daktyloskopie. Hier werden Fingerabdrücke auf bestimmte Merkmale hin untersucht (beispielsweise das Zusammenlaufen oder Auseinandergehen von Hautrillen an bestimmten Punkten des Fingers). Fingerabdrücke werden als übereinstimmend angesehen, wenn es eine bestimmte Mindestanzahl (z. B. acht oder zwölf) übereinstimmender Merkmale und keine widersprüchlichen Merkmale gibt. Eine echte Quantifizierung hingegen würde eine Aussage machen, bei wie vielen Personen eine spezifische Kombination von Merkmalen vorkommt. Weisen sowohl die Abdrücke am Tatort als auch die Abdrücke eines Verdächtigen diese Merkmalskombination auf, dann kann man die Irrtumswahrscheinlichkeit der Assoziation bestimmen. Weist beispielsweise eine Person in 10.000 Personen die Merkmalskombination auf, dann beträgt die Irrtumswahrscheinlichkeit $1:10.000$. Repräsentative Studien über die Verteilung von Merkmalen in der Bevölkerung sind jedoch rar.

Besonders gut untersucht sind Merkmalsverteilungen und entsprechende Wahrscheinlichkeiten im Bereich der DNA-Analyse. Hier gibt es relativ viele und umfassende Studien über die Verteilung von bestimmten Merkmalen in der menschlichen Erbsubstanz. Liegt genügend DNA-Material vor, kann man Wahrscheinlichkeiten berechnen, die eine bestimmte Person exakt identifizieren (beispielsweise bei einer Irrtumswahrscheinlichkeit von $1:25$ Milliarden) [Benecke, 2001, S. 7f]. Es besteht aber auch bei der DNA-Analyse die Gefahr einer fälschlichen Assoziation, nämlich durch verunreinigte, vertauschte oder falsch beschriftete Spuren.

Bei vielen Fällen in der Praxis ist es schwierig, die Irrtumswahrscheinlichkeit der Assoziation anzugeben. Trotzdem sollte bei jeder Assoziation hinterfragt werden, auf welcher Basis der Schluss erfolgte.

Der Weg zur Assoziation

Die Assoziation und das daraus resultierende Ereignis sind nur das Endergebnis einer Folge von Schritten, die nach und nach die Mengen der zueinander passenden Objekte derart einschränken, dass am Ende nur zwei Objekte übrig bleiben. In der Literatur [Inman and Rudin, 2000, Kapitel 6] werden die folgenden Schritte definiert: Identifizierung, anschließend Klassifizierung und Individualisierung einer Spur.

Bei der *Identifizierung* (*identification*) wird die prinzipielle Tauglichkeit der Spur als Beweismittel geprüft. Es wird gefragt: *Was ist es?* Beispielsweise muss eine Blutspur zunächst gefunden und dann als Blutspur erkannt werden. Identifikation

kann charakterisiert werden als die Einschränkung der potentiellen Spuren am Tatort „mit bloßem Auge“.

Bei der *Klassifizierung* einer Spur (*classification*) wird die Menge der Spuren weiter eingegrenzt durch eine genauere Analyse der Form, der Größe, des Gewichts, der Temperatur oder der Oberflächenstruktur des Gegenstandes. Hier wird gefragt: *Zu welcher Klasse von Gegenständen gehört das Objekt?* Charakteristisch für die Klassifizierung ist die Tatsache, dass man spezielle Werkzeuge wie eine Waage, ein Längenmaß, ein Mikroskop oder einen chemischen Test benötigt. Beispielsweise kann die Herkunft eines am Tatort gefundenen länglichen Gegenstandes zunächst als biologisch klassifiziert werden. Weitere Untersuchungen erlauben dann die genauere Klassifizierung als Haar. Anschließend kann man die Spur als menschliches Haar klassifizieren. Klassifizierungsmerkmale entstehen in der Regel aus *kontrollierten* Herstellungsprozessen, die dann jeweils charakteristisch für die Klasse von Objekten sind.

Mit *Individualisierung* (*individualization*) bezeichnet man die Zuordnung der Spur zu einer eng umgrenzten Menge von Objekten, die potentiell die Spur verursacht haben könnten. (Der Begriff wird oft fälschlicherweise verengt als die Zuordnung einer Spur zu einem Individuum verstanden.) Idealerweise führt die Individualisierung zu einer 1:1-Zuordnung zwischen Spur und dem Referenzobjekt, das die Spur verursacht hat. Die Merkmale, die eine Individualisierung erlauben, entstammen in der Regel *zufälligen* und *unkontrollierten* Prozessen, wie sie beispielsweise durch Abnutzung geschehen.

Wie eingangs geschildert, steht am Ende dieser Kette die Assoziation, also die möglichst genau quantifizierbare Feststellung des Kontakts zwischen zwei Objekten, beispielsweise die Zuordnung einer DNA-Spur am Tatort zu einer bestimmten Person.

Abbildung 10 fasst den Weg zur Assoziation nochmals zusammen. Im oberen Bereich der Abbildung ist der Tatort dargestellt. Am Tatort gibt es verschiedene Objekte, die zunächst als mögliche Spur identifiziert werden müssen. Im nun folgenden Prozess wird versucht, das Objekt am Tatort mit einer eng umgrenzten Menge an „passenden“ Objekten zu assoziieren. Dies geschieht durch eine schrittweise Eingrenzung der Objektmenge in der restlichen Welt mittels Klassifizierung und Individualisierung.

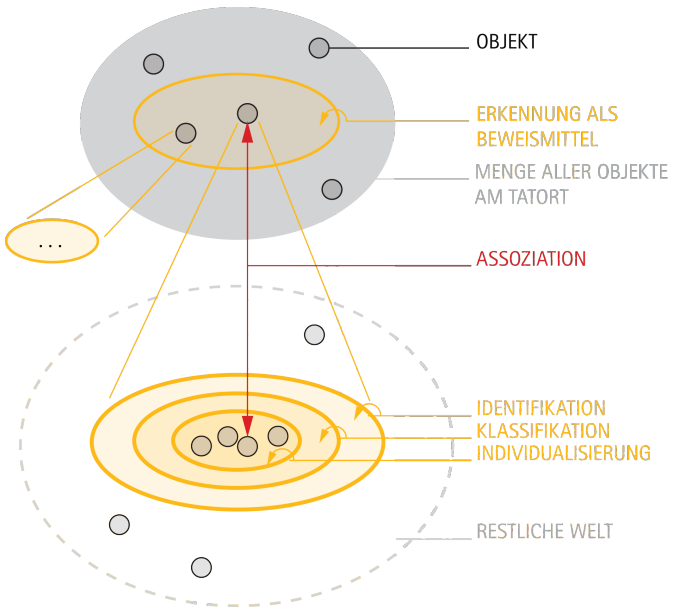

Abb. 10: Schematische Darstellung des Weges zur Assoziation.

Beispiele

Wir betrachten im Folgenden einige Beispiele, um die Schritte von der Identifizierung bis zur Individualisierung zu illustrieren.

- Am Tatort existiert der Abdruck eines Objektes im Sand. Die Identifizierung geschieht durch Hinschauen: Es handelt sich um einen Schuhabdruck. Die Klassifizierung geschieht mittels zusätzlicher Messinstrumente wie einem Metermaß und einem Herstellerverzeichnis (das Logo des Herstellers ist im Abdruck erkennbar): Es handelt sich um einen Herrenschuh der Größe 44 einer bestimmten Marke. Die Individualisierung erfolgt durch die Beobachtung von bestimmten Unregelmäßigkeiten im Abdruck, etwa Risse in der Sohle oder charakteristisch abgenutzte Stellen.
- Am Tatort einer Schießerei wird ein kleines metallisches Objekt gefunden. Es wird durch bloßes Hinschauen als Kugel einer Schusswaffe und damit als potentielle Spur identifiziert. Anschließend wird die Kugel von ihrer Größe und Beschaffenheit her als Pistolenkugel eines gewissen Kalibers klassifiziert. Die Individualisierung erfolgt durch die Beobachtung von charakteristischen Kratzspuren an den Seiten der Kugel.

Notwendigkeit von Identifizierung und Klassifizierung

Unter bestimmten Voraussetzungen ist es gar nicht notwendig, die volle Wegstrecke bis hin zur Individualisierung zu gehen. Abhängig vom Delikt und dem damit verbundenen Straftatbestand kann man manchmal schon nach der Identifizierung oder der Klassifizierung aufhören. Ein Beispiel hierfür ist die Identifizierung oder Klassifizierung von Objekten wie Betäubungsmitteln, deren Besitz möglicherweise bereits unter Strafe steht. Es ist dann für die Ermittlung meist nicht mehr relevant, von welchem Drogendealer oder aus welchem Drogenlabor das Objekt genau stammt. Ein anderes Beispiel ist der Besitz (gedruckter) kinderpornographischer Schriften. Für die Ermittlung der Umstände einer Straftat mag vielleicht relevant sein, woher die Schriften bezogen wurden (Individualisierung). Für die Anklage kann allerdings bereits die Klassifizierung eines Dokuments ausreichen.

1.4 Zusammenfassung

In diesem Abschnitt haben wir Grundbegriffe und Prinzipien der klassischen Forensik betrachtet. Implizit haben wir dabei vorausgesetzt, dass es sich bei Spuren immer um physische Spuren handelt. Im folgenden Abschnitt treten wir in die digitale Welt des Cyberspace ein und untersuchen, inwiefern die Begriffe der klassischen Forensik auf digitale Spuren und die Informatik anwendbar sind.

2 Digitale Spuren

Wir definieren nun den Begriff der *digitalen Spuren* und stellen diesen in den Kontext der klassischen Forensik. Wir möchten damit zeigen, dass sich die Informatik ohne Weiteres in die Tradition der klassischen forensischen Wissenschaften stellen lässt. Zwar verlangt die Untersuchung digitaler Spuren manchmal neue Methoden, aber die Informatik ist keineswegs eine neue forensische Wissenschaft, für die andere Gesetze als bei den übrigen forensischen Wissenschaften gelten. Fast alle Prinzipien, die man in der klassischen Forensik für physische Spuren entwickelt hat, lassen sich auch auf digitale Spuren anwenden. Die vermeintlichen Unterschiede bei der Behandlung digitaler Spuren führen lediglich zu einer Betonung bestimmter forensischer Prinzipien, die bei der Betrachtung von physischen Spuren nur am Rande vorkamen.

2.1 Definition und Abgrenzung

Eine der gängigsten Definitionen digitaler Spuren stammt von Casey [2004, S. 12] und lautet wie folgt:

D

Definition 1: digitale Spuren

Digitale Spuren (*digital evidence*) sind Spuren, die auf Daten basieren, welche in Computersystemen gespeichert oder übertragen worden sind.

So genau diese Definition erscheint, so unscharf bleibt sie bei näherer Betrachtung. Beispielsweise wird nicht klar, worin die „digitale" Natur der Spuren basiert. Basiert sie rein auf der Verarbeitung durch Computersysteme? Falls ja, würden auch analog arbeitende Computer [Giloi and Lauber, 1963] digitale Spuren erzeugen, was kontraintuitiv wäre. Basiert sie hingegen rein auf der diskreten (also digitalen) Codierung der Daten als Nullen und Einsen, dann wären auch handschriftliche Berechnung boolescher Ausdrücke digitale Spuren.

E

Exkurs 2: Analogrechner

Bei Analogrechnern nutzt man aus, dass bestimmte mathematische Probleme durch physikalische Phänomene approximierbar sind. Ein einfacher mechanischer Analogrechner ist beispielsweise der *Rechenschieber*, bei dem man mit Hilfe von Verschiebebewegungen logarithmischer Skalen multiplizieren und dividieren kann. Es existieren auch Analogrechner auf elektronischer Grundlage, etwa zum Lösen von Differentialgleichungen.

Um diese Situation etwas aufzuklären, kehren wir kurz zurück zur klassischen Forensik (Abschnitt 1). Denn digitale Spuren sind zunächst immer auch physische Spuren, wie beispielsweise die Magnetisierung auf der Oberfläche einer Festplatte, elektromagnetische Wellen auf einem Datenkabel oder der Ladezustand von Speicherzellen im Hauptspeicher. Insofern können alle Begriffe und Prinzipien der klassischen Forensik direkt auf digitale Spuren angewendet werden, wie wir nun näher ausführen.

Information und Träger bei digitalen Spuren

In der klassischen Forensik haben wir zwischen *Spureninformation* und *Spurenträger* unterschieden: Der Spurenträger „trägt" dabei die Spureninformation. Bei digitalen Spuren reduziert man die Spureninformation meist auf die *diskrete Repräsentation* der gemäß eines bestimmten Codierungsschemas auf dem Spurenträger gespeicherten Daten. Das Codierungsschema (also wann man eine Eins und wann man eine Null liest) ist dabei meist im Spurenträger gleich „mitverbaut", also in der Festplatte oder dem RAM-Chip. Durch diese Abstraktion wird die Bindung zwischen Spurenträger und Spureninformation extrem zerbrechlich: Die Spureninformation kann nämlich theoretisch auf einem beliebigen Spurenträger gespeichert werden. Dies korrespondiert mit der Beobachtung, dass man in der digitalen Welt Daten „perfekt kopieren" kann, also ohne die Möglichkeit, Original und Kopie später unterscheiden zu können.

Die schwache Verbindung von Spurenträger und Spureninformation im Falle von digitalen Spuren verdeutlicht den Unterschied zwischen beiden Konzepten: Der Spurenträger ist das „Speichermedium", die Spureninformation ist die auf dem Speichermedium „gespeicherte" Information. Bei der Reduktion auf digital (also

als Bits) codierte Informationen abstrahiert man von vielen weiteren Informationen, die der Spurenträger enthält.

B

Beispiel 2: Informationsverlust durch digitale Betrachtung

Digitale Datenübertragungen auf einem Kabel basieren auf Spannungsänderungen. So kann beispielsweise eine Spannung von 0 V eine Null repräsentieren und eine Spannung von 5 V eine Eins. Beim Anlegen der Spannung schwankt diese üblicherweise etwas, so dass bestimmte Spannungspegel angesetzt werden (etwa 0,5 V und 4,5 V), „ab denen“ der auf dem Kabel angelegte Spannungswert als Null oder Eins interpretiert wird. Der wirklich übertragene Wert (also die genaue Spannung) geht bei dieser Interpretation verloren. Ähnlich verhält es sich bei der Speicherung und Interpretation von Daten, die auf Festplatten oder im RAM-Speicher eines Rechners gespeichert werden. Die Interpretation beruht also auf Codierungsannahmen. Die resultierenden Daten jedoch sind (bei zuverlässiger Speicherung) exakt dieselben, die vorher gespeichert wurden.

Der Fokus auf die reine Spureninformation unter Vernachlässigung des Spurenträger ist aber keine spezielle Eigenart digitaler Spuren. Solange klar ist, welche Information auf dem Spurenträger wichtig ist, kann man diese Spureninformation natürlich auch auf einem anderen Spurenträger ablegen. Wenn vom Spurenträger „blutiger Handschuh“ lediglich die Täter-DNA relevant ist, dann kann man die Ergebnisse der DNA-Analyse in einem Bericht niederlegen. Die Spureninformation wechselt dann den Spurenträger: vom blutigen Handschuh auf ein Blatt Papier.

Integrität

Die Betonung der Spureninformation, wie sie digitalen Spuren eigen zu sein scheint, hat auch noch andere Konsequenzen. Zunächst müssen Begriffe wie Integrität und Authentizität neu betrachtet werden. Bezüglich Integrität ist die Frage relevant, ob ein digitales Objekt (beispielsweise eine Datei auf einem Datenträger) seit der Sicherung verändert worden ist. Bei einer engen Verbindung zwischen Spureninformation und Spurenträger kann man den Spurenträger selbst untersuchen und diesen aus weiteren Perspektiven betrachten, etwa die Tinte eines Briefes, die Handschrift auf einem Zettel, oder das Alter des Papiers. Bei der reinen Betrachtung der Spureninformation kann man auch eine Plausibilitätsprüfung des Inhalts durchführen und beispielsweise vergleichen, ob die Informationen widersprüchlich sind zu den mit der Spur verbundenen Behauptungen. Falls die Spur beispielsweise 2015 gesichert wurde, wäre es merkwürdig, wenn sich die Spureninformationen auf Ereignisse aus 2016 beziehen. Diese Form von Integritätsprüfung korrespondiert mit dem Begriff der *semantischen Integrität* aus der IT-Sicherheit [Gollmann, 2011].

Auch für die allgemeineren Begriffe Authentizität und Integrität bietet die IT-Sicherheit etablierte Definitionen an [Gollmann, 2011]. Dabei wird oft übersehen, dass die Prüfung von Authentizität und Integrität stark auf Annahmen basiert.

B

Beispiel 3: Integrität mittels Hashwerte

Eine *Hashfunktion* ist eine mathematische Funktion, die eine beliebig lange Bitfolge m auf einen Wert h mit fester Länge abbildet. Der Wert h wird häufig als *Hashwert* (*hash*, *digest*) von m bezeichnet. Der Hashwert h hat dabei die besondere Eigenschaft, „charakteristisch" für m zu sein (für einen genaueren Überblick siehe Menezes et al. [1997]).

Hashwerte besitzen viele Eigenschaften von *Fingerabdrücken*: Intuitiv kann man den Hashwert dazu verwenden, um m zu identifizieren. Auch kann man sich den Hashwert nicht aussuchen, er ist der Bitfolge m quasi angeboren.

Wenn man also die Integrität einer Bitfolge m prüfen will, so kann man den Hashwert h von m berechnen und diesen vergleichen mit einem andernorts hinterlegten Hashwert h'. Wenn h und h' übereinstimmen, dann liegt der Berechnung von h derselbe Bitstring zugrunde, der auch der Berechnung von h' zugrunde lag. Seit der Berechnung von h' hat sich also m nicht verändert.

Die eben im Beispiel beschriebene technische Auffassung von Integrität beruht auf der Annahme, dass der hinterlegte Hashwert verlässlich und korrekt berechnet wurde, beispielsweise zum Zeitpunkt der Sicherung der originalen Bitfolge, und dass der Hashwert selbst authentisch ist und nicht verändert worden ist [Lynch, 2000].

Authentizität

Authentizität ist bei digitalen Spuren noch etwas schwieriger zu definieren als bei physischen Spuren. Im Prinzip bedeutet Authentizität lediglich, dass die vorgelegte Spur tatsächlich die Spur ist, die durch die mit ihr verbundenen Behauptungen beschrieben wird. Bei physischen Spuren gibt es über den Spurenträger sehr viele Möglichkeiten, um diese Behauptungen anhand des Objekts selbst zu prüfen, etwa die Behauptung, dass es sich bei dem Objekt um einen „blutigen Handschuh" handelt. Bei digitalen Spuren verwendet man häufig den aus der IT-Sicherheit

etablierten Begriff der Authentizität [Gollmann, 2011], wie er durch digitale Signaturen realisiert werden kann.

B

Beispiel 4: Authentizität durch digital signierten Hashwert

Um Nachrichten digital zu signieren, kann man ein asymetrisches Verschlüsselungsverfahren verwenden. Bei einem asymetrischen Verschlüsselungsverfahren besitzt jede Person einen öffentlichen Schlüssel und einen privaten Schlüssel. Der öffentliche Schlüssel ist allen anderen Personen bekannt. Von den privaten Schlüsseln kennt jede Person nur den eigenen (für den Überblick siehe auch Menezes et al. [1997]). Mit dem privaten Schlüssel kann man Nachrichten signieren. Die Eigenschaften dieser Operation sind analog zum Setzen der eigenen Unterschrift unter die Nachricht. Jede andere Person kann prüfen, ob die Unterschrift von der angegebenen Person stammt, und auch nur diese Person kann die Unterschrift geleistet haben. Aus Effizienzgründen signiert man jedoch meist nur den Hashwert der Nachricht. Man kann folglich eine digitale Spur als authentisch ansehen, wenn wir einen korrekten Hashwert besitzen, der von der Person digital signiert wurde, die die Spurensicherung durchgeführt hat.

Auch bei der eben geschilderten Prüfung der Authentizität machen wir viele Annahmen. Zuvorderst vertrauen wir in die Verlässlichkeit der Person, die die Sicherung (mitsamt digitaler Signatur) durchgeführt hat. Das bedeutet vor allem auch, dass nur diese Person ihren privaten Schlüssel kennt und niemand anderes. Auch vertrauen wir in die mathematische Sicherheit des digitalen Signaturverfahrens. Unter der Annahme, dass das Signaturverfahren nicht gebrochen worden ist, wissen wir dann lediglich, dass jemand die Unterschrift geleistet hat, der den zu einer Person gehördenden privaten Schlüssel kennt — nicht mehr und nicht weniger.

Digitale Signaturen sind also keineswegs mit handgeschriebenen Unterschriften zu vergleichen. Eine handgeschriebene Unterschrift kann viele verschiedene Bedeutungen haben [Lynch, 2000]: Mit einer Unterschrift kann man anzeigen,

- dass man der Autor des Dokumentes ist,
- dass man das Dokument oder einen Teil des Dokumentes zur Kenntnis genommen hat,
- dass man das Dokument erhalten hat, oder
- dass man dem Inhalt des Dokumentes zustimmt.

Bei Unterschriften geht es also nicht immer nur um ihre Bedeutung sondern auch um den Wirkungsbereich, auf den sie sich beziehen. Dies ist schwer mit digitalen

Signaturen nachzubilden, vor allem, wenn sich Dokumente über die Zeit verändern (zum Beispiel durch Umformatierung).

Exkurs 3: Urkundenwesen

Der Übergang von physischen Dokumenten zu rein digitalen Archiven wird seit langem im Bereich der Buchwissenschaften diskutiert, speziell im *Urkundenwesen* (*diplomatics*) [Duranti, 1998]. Dort spielen Authentizität und Integrität von Dokumenten eine entscheidende Rolle [Lynch, 2000], etwa bei Besitzurkunden oder bei Verträgen. Die Bezüge zur digitalen Forensik sind bereits lange etabliert und fruchtbar [Dardick et al., 2014, Rogers, 2013, Sect. 3.8].

E

2.2 Entstehung digitaler Spuren

Wir möchten nun untersuchen, inwieweit sich die in Abschnitt 1 geschilderten grundlegenden Entstehungsprinzipien von Spuren in die digitale Welt übertragen lassen und widmen uns zunächst den Phänomenen der Zerteilbarkeit und des Transfers in der digitalen Welt. Anschließend befassen wir uns mit dem Konzept der Assoziation.

Zerteilbarkeit und Transfer in der digitalen Welt

Intuitiv kann die digitale Welt als Zustandsautomat beschrieben werden. Auch wenn dieser Automat in die reale Welt eingebettet ist, bleiben dessen Zustände diskret. In diesem Sinne gibt es in der digitalen Welt auch keine Materie: Alle dort manipulierten Artefakte sind schlussendlich Daten, die in diskreter Kodierung im Speicher eines Rechners liegen. Eine Zerteilbarkeit von Materie (*divisibility*), die die Grundlage für den physischen Transfer (*transfer of matter*) in der realen Welt bildet, gibt es somit nicht im selben Maße (immerhin werden Ladungen und Magnetisierungspotentiale hin- und hergeschoben). Es gibt in der digitalen Welt also keine Analogie für das Konzept des Austauschs im Sinne von Locards Austauschprinzip (siehe Abschnitt 1).

Übertragung von Materie ist, wie wir ebenfalls aus Abschnitt 1 wissen, jedoch nur *eine* Art von Transfer, die im Rahmen einer Handlung erfolgen kann. Die andere Art der Übertragung ist die Übertragung von Mustern (*transfer of traits*). Diese Art der Übertragung findet in der physischen Welt immer dann statt, wenn Information von einem Objekt zum anderen übertragen wird. Dieser Vorgang hat eine offensichtliche Analogie in der digitalen Welt, wo der Austausch von *Informationen* (Dateien, E-Mails etc.) eine so zentrale Rolle spielt.

Aber nicht nur zwischen Rechnern werden Informationen ausgetauscht, auch innerhalb eines einzelnen Rechner werden Informationen zwischen Objekten im Speicher ausgetauscht.

B

Beispiel 5: Übertragungen in der digitalen Welt

Beispiele für solche Übertragungen in der digitalen Welt sind etwa folgende Operationen:

- Maschineninstruktion im Prozessor, zum Beispiel: `mov eax, ebx`
- Zuweisung in einer Programmiersprache, zum Beispiel: `x := y`
- Kopieroperation auf einem Computer, zum Beispiel in einem Kommandofenster (Shell): `copy file1.txt file2.txt`
- Kopieroperationen über das Netz, zum Beispiel in einem Kommandofenster:
  `scp file1.txt user@host.de:/`

K

Kontrollaufgabe 1: Übertragung von Mustern

Diskutieren Sie, inwiefern es sich bei den folgenden Aktionen um eine Übertragung von Mustern handelt:

a) Programmieranweisung: x := x + 5

b) Shell-Eingabe: del file1.txt

c) Programmieranweisung: x := 1

d) Maschineninstruktion: nop

Im Prinzip ist jede Datenverarbeitung Musterübertragung: Wenn ein Datum aus einem Teil des Speichers geladen, mit anderen Informationen verknüpft und anschließend wieder im Speicher abgelegt wird, dann drücken sich die Muster der Eingangsdaten im Muster der Ausgangsdaten ab. Bei Kopieroperationen ist direkt intuitiv ersichtlich, wie sich Muster von der Quelle zum Ziel hin verlagern. Betrachtet man jedoch auch den Gesamtzustand des Rechnersystems, dann bleiben viele Speicherbereiche (im RAM und auf der Festplatte) von der aktuellen Operation unberührt. Auch hier pflanzen sich Muster im Verlauf der Zeit fort. Wir werden später sehen, dass man auf Basis dieser Musterübertragung, einen „Kontakt“ oder eine „gemeinsame Quelle“ zweier (digitaler) Objekte feststellen kann, genau wie in der klassischen Forensik auch.

Geschlossenes vs. offenes System

Die Beschränkung auf die (digital codierte) Spureninformation birgt eine weitere Problematik, die uns im Verlauf dieses Abschnitts noch mehrfach begegnet, denn die Beschränkung ist fundamental: Mit der Abkehr vom Spurenträger schließt man unendlich viele Blickrichtungen aus, die weitere Spureninformationen tragen könnten. Dies kann fatale Folgen haben. Hätte man beispielsweise schon in den 1960er Jahren alle Spuren „digitalisiert“ und die Spurenträger vernichtet, dann wären alle DNA-Spuren verloren gegangen, weil die Bedeutung dieser Spurenart zu der Zeit noch unbekannt war.

Die Betrachtung digitaler Spuren verleitet dazu, ausschließlich in digitalen Dimensionen zu denken und die Bedeutung und die Einflüsse der physischen Welt auf diese Spuren zu vernachlässigen. Die digitale Welt/der Cyberspace wird dadurch als *geschlossenes System* wahrgenommen. Die implizite Annahme lautet dabei, dass der Austausch zwischen digitaler Welt und nicht-digitaler Welt nur über wohldefinierte Schnittstellen geschieht. Der Blick auf die digitale Welt und auch auf die Spuren darin ist jedoch dadurch stark eingeschränkt. Es gibt aber deutlich mehr Übergänge in die digitale Welt als nur die Tastatur des Computers. Wie wir vor allem im Bereich der Multimediaforensik sehen werden, schlagen sich physische Phänomene direkt in digitalen Spuren nieder, die mit entsprechenden Techniken ausgewertet werden können. Notwendig dafür ist lediglich eine gewisse Grundkomplexität des digitalen Raumes, die jedoch heute problemlos auch von kleinsten Computern erreicht wird.

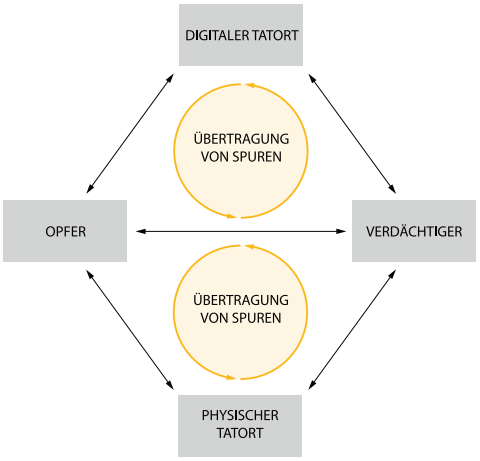

Abb. 11: Die Erweiterung von Locards Austauschprinzip auf den digitalen Tatort nach Casey [2011, Abb. 1.1].

Konsequenterweise erweitert Casey [2011, S. 17] das ursprüngliche Austauschprinzip von Locard, das nur eine *physical crime scene* vorsah, um eine *digital crime scene*, in dem ein Austausch von digitalen Spuren stattfinden kann (siehe Abbildung 11). Diese Gegenüberstellung verdeutlicht aber auch, dass ein digitaler Austausch von Spuren einhergehen kann mit einem physischen Austausch von Spuren, etwa wenn ein Schalter oder eine Taste physisch betätigt und dadurch Software gestartet wird, oder wenn (wie im Beispiel der Multimediaforensik) Umgebungseinflüsse durch entsprechende Sensorik die Spurenentstehung beeinflusst.

Abstraktionsschichten

Ein relevanter Aspekt digitaler Spuren beruht auf der Tatsache, dass digitale Spuren meist in einer für Menschen nicht direkt zugänglichen Form vorliegen. Wie auch bei vielen Arten von physischen Spuren, die man oft nicht mehr mit bloßem Auge erkennen kann, müssen digitale Spuren in der Regel immer zunächst extrahiert und in eine lesbare Form übersetzt werden. Diese Aufbereitung erfordert den Einsatz von Werkzeugen, die eine Abstraktion bzw. Interpretation der physischen Spuren zeigen. Charakteristisch für moderne Computersysteme ist zudem, dass es

meist mehrere Abstraktionsebenen gibt, auf denen die Daten dargestellt werden können.

B

Beispiel 6: Abstraktionsschichten digitaler Spuren

Als Beispiel betrachten wir die Abstraktionsschichten, die durchlaufen werden, wenn eine E-Mail-Nachricht als digitale Spur untersucht wird:

1. Interpretation der Magnetisierung der Festplatte (Bits)
2. Interpretation der Bits durch eine Zeichenkodierung
3. Interpretation der Zeichen durch ein Dateisystem
4. Interpretation der Daten im Dateisystem als zusammengehörige Datei
5. Interpretation der Datei als E-Mail

Jede einzelne dieser Abstraktionsebenen kann Quelle für Interpretationsfehler sein. Daher ist es bei einer forensischen Untersuchung digitaler Spuren insbesondere erforderlich, die Plausibilität jeder einzelnen Interpretation bzw. Abstraktion zu prüfen.

2.3 Eigenschaften digitaler Spuren

In diesem Abschnitt betrachten wir verschiedene Eigenschaften digitaler Spuren, nach denen man diese klassifizieren kann. Viele dieser Eigenschaften haben Parallelen zu Eigenschaften von Spuren der klassischen Forensik.

Flüchtigkeit

Die Klassifizierung nach Flüchtigkeit ist aus Sicht der digitalen Forensik nützlich, da wie in der klassischen Forensik Spuren je nach Flüchtigkeit unterschiedliche Vorgehensweisen und Techniken zur Sicherung und Analyse erfordern. Flüchtigkeit bezieht sich einerseits auf den Spurenträger (d.h. die Art und Weise, wie Daten abgespeichert werden), andererseits auch auf die Geschwindigkeit der Datenverarbeitung. Generell unterscheiden wir zwei bzw. drei Arten der Flüchtigkeit. Zunächst gibt es den Unterschied zwischen persistenten und flüchtigen Spuren. Flüchtige Spuren können dann nochmals unterteilt werden.

Persistente Spuren sind Spuren, die über einen vergleichsweise großen Zeitraum ohne Stromzufuhr erhalten bleiben. Persistente Spuren entstehen typischerweise auf Festplatten, CD/DVDs, Solid-State-Speichern (USB-Sticks, CF-/SD-Karten etc.) und Magnetbändern. Derartige Spuren können nahezu beliebig lange nach der Tat analysiert werden, ohne Gefahr zu laufen, dass Daten mit der Zeit verloren gehen.

Flüchtige Spuren benötigen eine Stromzufuhr, um erhalten zu bleiben. Wir unterscheiden diese Klasse von Spuren noch zusätzlich in *flüchtige Spuren im weiteren Sinne und im engeren Sinne*. Im weiteren Sinne sind Spuren flüchtig, wenn sie nur mit einer entsprechenden Stromzufuhr dauerhaft gespeichert werden. Manchmal werden diese Spuren darum auch als *semi-persistent* bezeichnet. Bei unterbrochener Stromzufuhr bleiben sie nur kurze Zeit erhalten. Typischer Vertreter dieser Klasse von Spuren sind Daten im Hauptspeicher (RAM) eines Rechners. Diese Spuren müssen entweder im laufenden Betrieb analysiert werden oder es muss zur späteren Analyse eine Kopie der Daten auf einem persistenten Datenträger erstellt werden. Im engeren Sinne flüchtig sind Spuren, die im laufenden Betrieb und *trotz*

dauerhafter Stromzufuhr nur temporär vorhanden sind. Beispiele sind Netzwerkdaten oder die Inhalte von Prozessorregistern. Diese Spuren müssen entweder im laufenden Betrieb analysiert werden, oder sie werden aufgezeichnet und auf einem persistenten Datenträger gespeichert. Beispielsweise kann durch das Mitschneiden von Netzwerkverkehr eine Protokolldatei der transportierten Daten über einen gewissen Zeitraum angefertigt werden.

Technische Vermeidbarkeit

Bei der Betrachtung von Spuren in Dateisystemen beobachtete Carrier [2005], dass die Veränderungen bestimmter Daten dazu führen können, dass das System nicht mehr richtig funktioniert. Beispiele hierfür sind Verweise auf Datenblöcke im Dateisystem. Ohne derartige Verweise wären die Inhalte einer Datei nicht auffindbar. Carrier [2005] bezeichnet diese Daten als *essentiell* (*essential data*). Andere Daten, wie etwa der eigentliche Dateiinhalt, können eine nahezu beliebige Form haben, ohne dass dies das Systemverhalten entscheidend beeinflussen würde. Sollen unter Benutzung des Systems Spuren manipuliert werden, so erzeugt die Veränderung essentieller Daten einen hohen Aufwand, weil die Manipulationen unter Umständen zunächst wieder rückgängig gemacht werden müssen, bevor das System benutzt werden kann. Wir können also festhalten, dass die Manipulation essentieller Daten mit einem deutlich höheren Aufwand verbunden ist als die Manipulation nicht-essentieller Daten. Diese Beobachtung kann bei der Einschätzung des Beweiswertes gesicherter Spuren helfen.

Aufbauend auf Carrier [2005] formalisierten Freiling and Gruhn [2015] den Begriff der essentiellen Daten und entdeckten zwei Varianten in Bezug auf eine vom System bereitzustellende Funktionalität (beispielsweise Dateien abzuspeichern):

- *Strikt essentielle Daten* (*strictly essential data*) sind für alle betrachteten Systeme essentiell, sie sind also der Kern dessen, was die Funktionalität ausmacht. In Dateisystemen sind beispielsweise die Blockverweise strikt essentielle Daten.
- *Partiell essentielle Daten* (*partially essential data*) sind nur für manche Systeme essentiell, für andere nicht.

Man kann den Begriff der (strikt/partiell) essentiellen Daten sogar noch konzeptionell verallgemeinern und unterscheiden zwischen technisch vermeidbaren und technisch unvermeidbare Spuren.

Definition 2: Technisch vermeidbare Spuren

Technisch vermeidbare Spuren sind Spuren, die um ihrer selbst Willen erzeugt wurden.

D

Technisch vermeidbare Spuren sind nicht kritisch für das Funktionieren des Systems. Die Entstehung solcher Spuren kann lokal in der Regel durch eine Änderung der Systemkonfiguration eingeschränkt oder gänzlich unterbunden werden. Ein Beispiel für derartige Spuren sind Log-Dateien. Auch Daten, die im Rahmen einer Vorratsdatenspeicherung anfallen, gehören in diese Kategorie, da sie um ihrer

selbst Willen erzeugt werden – auch wenn der Benutzer selbst nicht in der Lage ist, ihre Erzeugung zu verhindern.

D

Definition 3: Technisch unvermeidbare Spuren

Technisch unvermeidbare Spuren sind Spuren, die unweigerlich anfallen und daher nicht durch einfache Änderungen an der Konfiguration eines Systems vermieden werden können.

Eine Veränderung technisch unvermeidbarer Spuren ist in der Regel nicht durch die Bordmittel des Betriebssystems erreichbar. Beispiele für derartige Spuren sind gelöschte Dateien im Dateisystem, alte Stackframes im Hauptspeicher oder Inhalte des DNS-Caches.

Aus Sicht des Ermittlers sind technisch unvermeidbare Spuren besonders interessant, da ihnen in der Regel ein höherer Beweiswert zugerechnet werden kann. Dies liegt daran, dass es deutlich aufwändiger ist, technisch unvermeidbare Spuren zu manipulieren als technisch vermeidbare Spuren. Insofern existiert eine Analogie zwischen technisch unvermeidbaren digitalen Spuren und mikroskopischen physischen Spuren. Technisch vermeidbare Spuren liegen zumeist als Inhaltsdaten in Form von Dateien vor. Sie gehören demnach meist zu den nicht-essentiellen Daten im Dateisystem und gelten allein dadurch bereits als weniger glaubwürdig. Technisch unvermeidbare Spuren benötigen aber eine besondere Expertise bei der Sicherung und Analyse.

Manipulierbarkeit

Wenn man die Betrachtung digitaler Spuren auf die Spureninformation reduziert, dann können digitale Spuren prinzipiell leicht manipuliert werden. Dies kann sowohl absichtlich als auch unabsichtlich geschehen. Die Manipulation digitaler Spuren hinterlässt auf der Ebene der digitalen Spureninformation nicht notwendigerweise sichtbaren Zeichen.

B

Beispiel 7: Manipulation digitaler Spuren

Als Beispiel für die Manipulation digitaler Spuren betrachten wir einen Rechner, der mittels einer Live-CD bootet. Die Live-CD greift nicht auf die Festplatte des Rechners zu, sondern operiert rein von einer RAM-Disk. Mit einem entsprechenden Werkzeug (Hexeditor) wird anschließend ein einzelnes Bit auf der Festplatte verändert. Daraufhin wird der Rechner heruntergefahren und die Live-CD aus dem Laufwerk entfernt.

Diese nicht (direkt) nachvollziehbare Manipulation von Spuren ist im Bereich der klassischen Forensik eher untypisch, denn dort geht man davon aus, dass jede Handlung eine Spur hinterlässt. Es ist aber festzuhalten, dass eine Person, die Spuren nicht-nachvollziehbar manipulieren möchte, immer sehr viele Annahmen

über die Umgebung machen muss, egal ob in der physischen oder der digitalen Welt, wie das folgende Beispiel verdeutlicht.

B

Beispiel 8: Manipulation digitaler Spuren

Ein Rechner wird wiederum mit einer Live-CD gebootet. Nach dem Systemstart wird mittels einer VoIP-Software (zum Beispiel Skype) ein verschlüsseltes Telefonat mit einer anderen Person geführt. Die Kenndaten der anderen Person werden dabei im laufenden Betrieb eingegeben. Nach dem Telefonat wird der Rechner heruntergefahren und die Live-CD entfernt. Damit die Handlung unentdeckt bleibt, müssen folgende Annahmen getroffen werden:

- Es wird lediglich die Festplatte des Rechners auf Spuren untersucht.
- Die Systembenutzung selbst hinterlässt keine zusätzlichen digitalen Spuren (etwa im BIOS).
- Im Netzwerk fallen keinerlei Spuren an, bzw. die dortigen Spuren werden nicht untersucht.
- Die Systembenutzung selbst (also die Tatsache, dass die Person den Rechner überhaupt benutzt) ist keine Spur (etwa, weil es sich um den persönlichen Rechner der Person handelt).
- Das Vorhandensein einer Live-CD mit vorkonfigurierter VoIP-Software ist selbst keine Spur.

Beachten Sie, dass die letzten beiden Spuren keine digitalen Spuren sind.

Wie bereits weiter oben auf Seite 30 erwähnt, basiert die Meinung, dass es im Bereich der digitalen Spuren grundsätzlich nicht-nachvollziehbare Manipulation gibt, auf der Annahme, dass es sich bei dem System um ein *geschlossenes System* handelt. Wie das Beispiel eben zeigt, entstehen Spuren aber auch außerhalb des eigentlich benutzten Systems. In der Praxis werden Rechner in der Regel nicht isoliert genutzt, sondern treten in Verbindung mit anderen Rechnern. Es entstehen also dort und auch im Netz selbst Spuren (beim Internet-Service-Provider oder im Router), die untersucht werden können. Außerdem ist das digitale System immer in die physische Welt eingebettet, in der auch Spuren entstehen, etwa in Form von Fingerabdrücken auf der Tastatur.

Die perfekte Manipulierbarkeit digitaler Spuren ist also ähnlich problematisch wie die perfekte Manipulierbarkeit physischer Spuren. Wenn man hingegen *ausschließlich* digitale Spuren betrachtet (also die reine Spureninformation), dann ist eine perfekte Manipulation denkbar. Diese beruht dann aber auf einer Selbstbeschränkung des Ermittlers. Wenn, wie im zuvor beschriebenen Beispiel, mit einer Live-CD nur ein einzelnes Bit verändert wird, dann können zusätzliche digitale Spuren vermieden werden, weil dieses Bit eben nur zwei Zustände annehmen kann (und keine Zwischenzustände, die auf eine Manipulation hindeuten könnten). In der digitalen Welt gibt es nur endlich viele Perspektiven, aus denen ein Ermittler eine digitale Spuren betrachten kann – im Gegensatz zur physischen Welt.

Ähnlich verhält es sich mit einer besonderen Form der Manipulation: der Vernichtung bzw. Löschung von digitalen Spuren. Vor allem das selektive Löschen einzelner Dateien ist in der Praxis schwieriger als gedacht. Zum Beispiel sind Dateien, die mit den Bordmitteln des Betriebssystems gelöscht werden, in der Regel noch lange Zeit auf der Festplatte rekonstruierbar [Carrier, 2005].

Kopierbarkeit

Digitale Rechensysteme kodieren Daten im binären Zahlensystem. Da Computer alle Informationen schlussendlich im Binärformat speichern, kennen sie nur *eindeutig unterscheidbare Zustände*. In Anlehnung an die ursprüngliche Bedeutung des Wortes *diskret* als *abgesondert* verwendet man in der Informatik auch gerne den Begriff der *diskreten* Zustände. Diese Bezeichnung betont, dass es zwischen zwei binären Werten keine Zwischenwerte gibt. Folglich befindet sich ein Computer zu jedem Zeitpunkt in einem klar definierten Zustand. Dies steht im Gegensatz zu einer grundlegenden Erfahrung, die man in der realen Welt macht: Materie ist (nahezu) beliebig zerteilbar. Der Zustand der realen Welt ist also alles andere als *diskret* im Sinne der Informatik, während der Zustand eines Computers durch die zu jedem Zeitpunkt immer bis ins letzte Bit exakt definiert ist. Im Prinzip kann man alles, also auch alle Arten von Naturphänomenen, wie beispielsweise Bilder oder Geräusche in einer vorher festgelegten Genauigkeit als binäre Zahl kodieren. Dies gilt umso mehr für schriftlich niedergelegte Informationen, Konzepte und Ideen. Die diskrete Form all dieser Artefakte macht es möglich, *perfekte Kopien* zu erzeugen, Kopien also, die von ihrem digitalen Inhalt nicht vom Original zu unterscheiden sind.

Wie bereits oben auf Seite 25 diskutiert, basiert diese Eigenschaft auf der Reduktion der gespeicherten Daten auf die digitale Repräsentation. Aufgrund ihrer digitalen Natur kann man also auch digitale Spureninformationen im Gegensatz zu physikalischen Spuren exakt duplizieren und somit alle Untersuchungen anhand einer Kopie durchführen. Genau genommen kopiert man aber lediglich die digitale Spureninformation, der Spurenträger verändert sich. Dies steht im gefühlten Gegensatz zu vielen physischen Spuren wie etwa Blut oder DNA-Spuren, die für eine Untersuchung chemisch analysiert und darum teilweise zerstört werden müssen.

Wenn man digitale Spuren kopiert, muss man jedoch sicherstellen, dass im Rahmen des Kopiervorgangs die Integrität gewahrt bleibt, also keine Veränderungen an den Spuren stattfinden. Die Übereinstimmung des Originals mit der Kopie lässt sich aber vergleichsweise einfach nachweisen, etwa durch einen bitweisen Vergleich mit dem Original. Wie oben auf Seite 26 angemerkt, verwendet man in der Praxis oft *kryptographische Hashfunktionen*, die einen kompakten Fingerabdruck eines Datenträgers erstellen können (für einen Überblick siehe Menezes et al. [1997]).

K

Kontrollaufgabe 2

Klassifizieren Sie die folgenden Beispiele digitaler Spuren mittels der Attribute essentiell/nicht-essentiell bzw. technisch vermeidbar/technisch unvermeidbar:

a) Kopien besuchter Webseiten im Cache von Web-Browsern
b) Liste der Besuchten Webseiten von Web-Browsern (Chronik/History)
c) Temporäre Dateien des Betriebssystems
d) Log-Dateien des Betriebssystem oder bestimmter Anwendungen
e) Sicherheitskopien von Daten (Backups)
f) Metadaten im Dateisystem (zum Beispiel Zeitstempel)
g) Wahlwiederholungsfunktion am Telefon
h) Abrechnungsdaten des Mobilfunkanbieters

Semantik

Auch wenn eine formale Unterscheidung schwierig ist, ist es aus Praxissicht sinnvoll, digitale Spuren noch in Bezug auf ihre Semantik auf Anwendungsebene zu klassifizieren. Wir unterscheiden hierzu allgemein die folgenden fünf Arten digitaler Spuren in Form von digitalen Daten.

- Primärdaten
- Sekundärdaten
- Programmdaten
- Konfigurationsdaten
- Logdaten

Die Daten dieser Klassen unterscheiden sich, wie wir im Folgenden erläutern werden, typischerweise in ihrem Inhalt, Entstehungszeitpunkt, Speicherort und zum Teil auch in ihrer Aussagekraft im Kontext einer digital-forensischen Untersuchung. Das bedeutet, dass je nach Art der in einem konkreten Fall gesuchten Spuren eine oder mehrere bestimmte Klassen von Daten zu untersuchen sind. Diese Unterscheidung ist orthogonal zu den anderen Klassifikationskriterien und kann in bestimmten Anwendungsgebieten verfeinert werden (siehe etwa die fünf Datenkategorien von Festplattendaten von Carrier [2005]).

Primärdaten

Der Begriff *Primärdaten* enstammt ursprünglich der Statistik und bezeichnet dort jene Daten, die unmittelbar aus einer Datenerhebung gewonnen werden. Im Falle der forensischen Analyse bezeichnet der Begriff Primärdaten solche Daten, zu deren Verarbeitung eine Anwendung implementiert wurde. Primärdaten sind also in Bezug auf eine konkrete Anwendung jene Daten, die von dieser Anwendung primär verarbeitet werden. Vereinfacht ausgedrückt dient beispielsweise eine konkrete Bildverarbeitungssoftware dazu, Bilddateien zu verarbeiten. Bilddateien sind in diesem Fall Primärdaten. Ein weiteres Beispiel sind E-Mails als Primärdaten eines E-Mail-Clients wie Mozilla Thunderbird[1].

Sekundärdaten

Sekundärdaten werden dazu erstellt und genutzt, um die Verarbeitung von Primärdaten zu vereinfachen. Hierbei kann es sich entweder um Daten handeln, die die Verarbeitung der Primärdaten durch die Anwendung unterstützen (*System-Sekundärdaten*) oder um Sekundärdaten, die dem Benutzer die Bearbeitung der Primärdaten erleichtern (*Benutzer-Sekundärdaten*).

Übliche Beispiele für System-Sekundärdaten sind Caches, Indizes oder Journale, welche die Performanz einer Anwendung bei der Verarbeitung der Primärdaten erhöhen. Systemsekundärdaten werden daher sehr häufig als Nebeneffekt der Verarbeitung von Primärdaten erstellt – meist ohne Absicht oder Kenntnis des Benutzers.

Im Gegensatz dazu werden Benutzer-Sekundärdaten verwaltet, um den Benutzer bei der Arbeit mit Primärdaten durch eine Anwendung zu unterstützen. Diese Daten werden von der Anwendung zur Gewährleistung ihrer Kernfunktionalität, also für die Bearbeitung der Primärdaten, an sich nicht benötigt. Beispiele für

[1] http://www.mozilla.org/thunderbird/

Benutzer-Sekundärdaten sind Lesezeichen in Webbrowsern, Adressbücher in E-Mail-Clients oder Listen zuletzt benutzter Dokumente.

Programmdaten

Programmdaten sind jene Daten, welche eine Anwendung selbst ausmachen und werden häufig auch als *Programmcode* bezeichnet. Hierbei kann es sich sowohl um eine ausführbare Binärdatei oder Bibliothek, als auch um Bytecode oder auch Quelltext (im Falle einer interpretierten Programmiersprache) handeln. Programmdaten verändern sich meist während der Ausführung der Anwendung nicht – mit einigen Ausnahmen wie beispielsweise einer Updatefunktionalität.

Konfigurationsdaten

Konfigurationsdaten wiederum bestimmen die Art und Weise, in der eine Anwendung Primärdaten verarbeitet. Eine charakteristische Eigenschaft von Konfigurationsdaten ist, dass diese Daten sich meist unmittelbar nach der Installation einer Anwendung oder auf explizite Anforderung des Benutzers verändern und sonst über die meiste Zeit konstant bleiben.

Es gibt außerdem Konfigurationsdaten, auf die nicht direkt Einfluss genommen werden kann. Beispielsweise werden bei der Installation einer Anwendung Verzeichnisstrukturen angelegt. Hierzu zählen beispielsweise Ordner, in denen bearbeitete Primärdaten standardmäßig gespeichert werden. Zudem gibt es für jedes Betriebssystem spezifische Verzeichnisse, in welchen die Programmdaten oder auch die Konfigurationsdaten selbst gespeichert werden. Solche Konfigurationsdaten bezeichnen wir als *implizite Konfigurationsdaten*.

Im Gegensatz zu den Konfigurationsdaten, die von der Anwendung festgelegt oder durch den Benutzer angepasst werden, gibt das verwendete Betriebssystem auch implizite Angaben vor. Hierzu zählen:

- Speicherort von temporären Daten
- Verzeichnisnamen, zum Beispiel Name des Standardordners für Programmdaten oder Benutzerverzeichnisse
- Betriebssystemabhängige Verwaltungsstrukturen

Diejenigen Konfigurationsdaten, die explizit vom Benutzer verändert werden können, um das Verhalten der Anwendung zu steuern, bezeichnen wir im Gegensatz zu den impliziten Konfigurationsdaten als *explizite Konfigurationsdaten*.

Logdaten

Viele Anwendungen sichern ein Protokoll von ausgeführten Aktionen, Fehlermeldungen oder Informationen zur Fehlerbehebung als *Logdaten*. Diese Daten ermöglichen es beispielsweise einem Administrator das Verhalten der Anwendung nachzuvollziehen. Jedoch sind Logdaten für die Anwendung selbst in keiner Weise von Belang und entstehen nur, wenn die entsprechende Log-Funktionalität willentlich implementiert wurde. Auch für einen gewöhnlichen Benutzer, der ausschließlich an der Verarbeitung der Primärdaten interessiert ist, bieten diese Daten keinen Mehrwert. Falls solche Daten vorhanden sind, bieten sie jedoch wertvolle Rückschlüsse über vergangene Aktivitäten des Systems und sind daher im Kontext einer forensischen Untersuchung von besonderer Relevanz.

2.4 Assoziation mittels digitaler Spuren

In den klassischen forensischen Wissenschaften (siehe Abschnitt 1) bezeichnet der Begriff *Assoziation* den Vorgang, bei dem zwei Objekte in Beziehung zueinander gesetzt werden. In der physischen Welt war dies zumeist ein „Kontakt“ zwischen zwei Objekten, durch den man eine Zuordnung machen konnte (etwa Projektil zu Waffe, Schuhabdruck zu Schuh). Als Ergebnis der Assoziation steht ein *Ereignis*, das ein Puzzleteil zur Rekonstruktion des Tathergangs beiträgt.

Wir haben oben gesehen, dass viele Aspekte digitaler Spuren ein Analogon zu Aspekten physischer Spuren haben. Im Folgenden zeigen wir, dass auch der Prozess der Assoziation analog zu jenem aus der klassischen Forensik durchschritten werden kann. Ziel ist die Assoziation zweier Datenobjekte (Bitfolgen) auf Basis von Musterübertragung.

Identifizierung

Bei der *Identifizierung* wird die prinzipielle Tauglichkeit der Spur als Beweismittel geprüft. Die Spur selbst kann eine beliebige Bitfolge sein, die potentiellen Tatbezug aufweist, etwa weil sie auf einer Festplatte liegt, die am Tatort gefunden wurde. Aber nicht alle Bitfolgen müssen auch Spuren sein. Die Identifizierung unterscheidet diese beiden Fälle. Ziel der weiteren Schritte ist nun, das „Gegenstück“ der gefundenen Spur zu finden, also beispielsweise die Quelle, aus der die Bitfolge stammt, oder die Umstände/Aktionen, die beim Entstehen der Bitfolge stattgefunden haben müssen.

Klassifizierung

Bei der *Klassifizierung* einer Spur wird die Menge der Gegenstücke weiter eingegrenzt durch eine genauere Analyse klassifizierender Merkmale. Charakteristisch für die Klassifizierung ist die Tatsache, dass man meist spezielle Werkzeuge benötigt, um solche Merkmale auszumachen. Klassifizierungsmerkmale entstehen aus *kontrollierten* Herstellungsprozessen, die dann jeweils charakteristisch für die Klasse von Objekten sind. Im Falle digitaler Spuren sind etwa Dateinamenssuffixe (die den Typ einer Datei andeuten) klassifizierende Merkmale. Oder die Entropie einer Datei kann ein klassifizierendes Merkmal sein.

Individualisierung

Mit *Individualisierung* bezeichnet man die Zuordnung der Spur zu einer eng umgrenzten Menge von Gegenstücken, die potentiell in Verbindung zur Spur stehen. Idealerweise führt bereits die Individualisierung zu einer 1:1-Zuordnung zwischen Spur und dem Gegenstück. Die Merkmale, die eine Individualisierung erlauben (*individualisierende Merkmale*), entstammen definitionsgemäß *zufälligen* und *unkontrollierten* Prozessen.

Individualisierende Merkmale im Bereich der digitalen Spuren sind beispielsweise Nutzungsspuren, die durch menschliche Benutzer verursacht worden sind, also Inhalte von Dokumenten oder Logdateien menschlicher Interaktionen. Auch Spuren von Systemaktivitäten könn individualisierend sein, beispielsweise die Namen von temporären Dateien oder die Wahl zufälliger Schlüssel bei der Datenübertragung.

Assoziation

Auf Basis der vorherigen Schritte steht im Optimalfall am Ende dieses Prozesses eine *Assoziation* zwischen dem am „Tatort“ identifizierten Objekt A und einem anderen Objekt B, welches mit der Spur in Zusammenhang steht.

In der digitalen Welt kann man nur den Kontakt von *digitalen* Objekten feststellen. Formal werden hierbei Ähnlichkeiten in den Speicherinhalten zugrunde gelegt, die den Zustandsraum des Computers ausmachen. Findet man beispielsweise eine inhaltsgleiche Datei an zwei Orten (im gleichen Dateisystem oder auf Festplatten unterschiedlicher Rechner), dann kann man die Hypothese einer *gemeinsamen Quelle* aufstellen.

Um die Art der Assoziation in der digitalen Welt besser zu veranschaulichen, betrachten wir nun anhand verschiedener Beispiele diesen Prozess. Hierbei möchten wir insbesondere zeigen, wie sich die Theorie von Inman and Rudin [2000] auf digitale Spuren anwenden lässt und zum Teil implizit bereits angewandt wird.

Wir beginnen bewusst mit zwei sehr einfachen Beispielen, bei denen es um den Kontakt zwischen physischen Objekten geht. Daher ist der Kontakt in diesen Beispielen offensichtlich und die Assoziation intuitiv nachvollziehbar, auch wenn der eigentliche Vorgang der Assoziation in der digitalen Welt stattfindet. Daraufhin folgt in Abschnitt 2.4 ein etwas weniger offensichtlicher Fall einer Assoziation, die ausschließlich zwischen digitalen Objekten besteht. Am Ende bringen wir ein akademisches Beispiel, das den Vorgang auf den minimalen Kern reduziert.

Beispiel: Multimediaforensik

Als erstes Beispiel für eine Assoziation in der digitalen Welt möchten wir ein Beispiel aus dem Bereich der *Multimediaforensik* heranziehen. In der Multimediaforensik werden solche digitalen Spuren betrachtet, die durch einen Sensor aus der physischen Welt aufgezeichnet werden, wie beispielsweise Digitalfotografien. Artefakte, die hierbei vom Sensor in diesen Daten hinterlassen werden, können genutzt werden, um Fragen nach Konsistenz und Ursprung der Daten zu beantworten. Die Feststellung der Herkunft, also beispielsweise Aussagen wie „Bilddatei A wurde mit Digitalkamera B aufgenommen“, ist ein offensichtliches Beispiel für die Herstellung einer Assoziation, in diesem Fall zwischen einem digitalen Medienobjekt und dem Sensor, der es ursprünglich aufgezeichnet hat. Anhand dieses Beispiels vollziehen wir nun die Schritte der *Identifikation*, *Klassifikation* und *Individualisierung* hin zur *Assoziation*.

Identifikation

In diesem Beispiel fassen wir eine Datei auf einer sichergestellten Festplate oder einem bestimmten Server im Internet als „am Tatort“ aufgefundenes Objekt A auf. Diese Datei wird als potentielle Spur identifiziert. Gesetzt den Fall, es handelt sich bei der betrachteten Ermittlung um einen Fall des Besitzes illegaler pornografischer Schriften, so ist bereits allein die Existenz dieser Datei möglicherweise ausreichend, um Objekt A als potentielles Beweismittel einzustufen.

Klassifizierung

Anschließend wird das identifizierte Objekt A (die Datei) auf klassifizierende Charakterisika untersucht. In diesem konkreten Beispiel würde dies zu dem Resultat führen, dass Objekt A eine Bilddatei einer bestimmten Größe (Auflösung) in einem bestimmten Dateiformat (beispielsweise JPEG) ist. Eine kurze Analyse der Datei (beispielsweise durch Auswertung der EXIF-Daten) führt zu dem Schluss, dass

das Bild wahrscheinlich durch eine Digitalkamera (das zu findende Objekt *B*) aufgezeichnet wurde. Durch Auswertung weiterer Klassencharakteristika, wie beispielsweise kleinen aber systematischen Abweichungen der Lichtempfindlichkeit einzelner Sensorelemente, ist es häufig möglich, die Klasse anhand einer einzelnen Fotografie auf den Hersteller und unter Umständen sogar auf das Modell der Kamera einzuschränken [Chen et al., 2008].

Individualisierung

Wurden mehrere Digitalkameras im Haus eines Verdächtigen sichergestellt, so ist es im nächsten Schritt möglich, das exakte Rauschverhalten einer jeden Kamera zu untersuchen. Dies geschieht durch die Aufnahme einer Reihe von Bildern unter kontrollierten Bedingungen in einem Labor, aus denen sich das individuelle Rauschmuster der jeweiligen Kamera extrahieren lässt [Chen et al., 2008, Lukás et al., 2005]. Durch Überprüfung von Objekt *A* auf die charakteristischen Muster dieser Kameras, kann dann die Menge der für die Aufzeichnung von Objekt *A* in Frage kommenden Digitalkameras im Optimalfall auf ein einzelnes Gerät eingegrenzt werden.

Assoziation

Nach den vorhergehenden Schritten ist es nun durch die individuellen (genauer: individualisierenden) Merkmale jeder Kamera möglich, mit hoher Sicherheit eine Assoziation zwischen dem identifizierten Bild (Objekt *A*) und einer bestimmten Digitalkamera herzustellen.

Beispiel: USB-Speichergeräte

Als nächstes Beispiel betrachten wir die Assoziation zwischen einem Wechseldatenträger und einem bestimmten Computer. Speichergeräte werden heute meist über den *Universal Serial Bus* (USB) an einen Computer angeschlossen. Bekanntermaßen sammeln Betriebssysteme Informationen über an das System angeschlossene Datenträger. Tatsächlich nutzen Betriebssysteme die individuellen Charakteristika eines Speichergerätes, um beispielsweise den korrekten Gerätetreiber auszuwählen [Carvey and Altheide, 2005]. Diese Tatsache kann es ermöglichen, Aussagen wie „USB-Stick *A* war schon einmal mit Computer *B* verbunden“ zu treffen.

Identifikation

Objekt *A* ist hier ein kleines Plastikobjekt mit einem Metallende, welches am Tatort aufgefunden wird. Wir nehmen für dieses Beispiel an, dass es sich um eine Ermittlung wegen Datendiebstahl handelt. Dies sollte ausreichen, um Objekt *A* als potentielles Beweismittel zu identifizieren.

Klassifizierung

Eine weitergehende Untersuchung auf klassifizierende Merkmale des Gerätes ergibt, dass es sich bei Objekt *A* tatsächlich um ein USB-Massenspeichergerät einer bestimmten Marke handelt. Die Klasse der Objekte *B*, zu denen Objekt *A* assoziiert werden könnte, umfasst zu diesem Zeitpunkt die Menge aller Computersysteme, die über eine USB-Schnittstelle verfügen.

Individualisierung

Stellen wir uns eine Menge von Computern verschiedener Verdächtiger vor, welche ebenfalls sichergestellt wurden, und stellen wir uns vor, dass auf all diesen

Geräten Microsoft Windows als Betriebssystem eingesetzt wird. Sobald ein USB-Speichergerät an ein Windows-System angeschlossen wird, erstellt das Betriebssystem eine sogenannte *Geräteinstanzkennung* (*device instance identifier*) auf Basis unterschiedlicher auf dem Gerät hinterlegter Werte, wie beispielsweise einer eindeutigen Seriennummer. Derartige Informationen stehen auf nahezu allen Geräten zur Verfügung. Diese Geräteinstanzkennungen werden unter Windows in der *Windows Registrierung* (*Registry*) unter folgendem Schlüssel gespeichert:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBStor
```

Diese Daten können unter Einsatz entsprechender Software extrahiert werden [Carvey and Altheide, 2005]. Weitere individualisierende Merkmale könnten in einer bestimmten Menge von Dateien bestehen, die sich sowohl auf Objekt *A*, als auch auf Objekt *B* befinden.

Assoziation

Das Auffinden der einzigartigen Gerätekennung eines USB-Speichergerätes an einer bestimmten Stelle auf einem Computersystem ist ein starkes Indiz dafür, dass dieses konkrete Gerät (Objekt *A*) in der Vergangenheit einmal an diesen konkreten Computer (Objekt *B*) angeschlossen war.

Beispiel: Browser Cache

Aus Performanz-Gründen sichern Webbrowser meist lokale Kopien besuchter Webseiten in Cache-Dateien, um diese bei einem erneuten Aufruf der Webseiten nicht nochmals herunterladen zu müssen. Diese Dateien gehören zu den System-Sekundärdaten (siehe Abschnitt 2.3) und können von forensischen Wissenschaftlern genutzt werden, um zu rekonstruieren, welche Webseiten von einem Benutzer eines Computers in der Vergangenheit aufgerufen wurden. Das bedeutet, dass Cache-Dateien es ermöglichen, eine Verbindung zwischen einem bestimmten Computer (Objekt *A*) und einer konkreten Webseite (Objekt *B*) herzustellen. Der Prozess der Assoziation kann in einem solchen Fall (und wird in den meisten Fällen bereits implizit) auf folgende Art und Weise angewandt werden.

Identifikation

Auf den ersten Blick könnte der forensische Wissenschaftler Dateien unter einem bestimmten Pfad im Dateisystem vorfinden, von dem bekannt ist, dass er üblicherweise von einem bestimmten Webbrowser für die Sicherung von Cache-Dateien genutzt wird. Für den *Microsoft Internet Explorer* ist dies beispielsweise das folgende Verzeichnis:

```
%systemdir%\Documents and Settings\%username%\Local
   Settings\Temporary Internet Files\Content.ie5
```

Daher könnte der Forensiker in diesem Schritt zu dem Schluss kommen, dass diese Dateien potentiell zum Browser-Cache gehören könnten und sie daher als potentielle Spuren identifizieren.

Klassifizierung

Im nächsten Schritt benötigt der Forensiker typischerweise irgendeine Art von (Software-) Werkzeug, um weitere Schlüsse ziehen zu können. Abhängig von dem Webbrowser, der die Cache-Dateien erzeugt hat, kann beispielsweise ein

spezieller Parser für das konkrete Dateiformat erforderlich sein, um zu verifizieren, dass die identifizierten Dateien tatsächlich zum Cache des betreffenden Browsers gehören.

Diese Spuren entstehen durch einen bekannten und kontrollierten Herstellungsprozess, da dieser Webbrowser bekanntermaßen immer (so lange nicht manuell anderweitig konfiguriert) Cache-Dateien unter diesem bestimmten Pfad und Dateinamen in diesem konkreten Format speichert. Dies ist ein wichtiges Kriterium für die Unterscheidung der Klassifizierung und der Individualisierung. Das Ergebnis dieses Schrittes ist, dass diese Dateien tatsächlich Cache-Dateien dieses Webbrowsers sind.

Individualisierung

Schließlich werden die eigentlichen Inhalte der als Cache klassifizierten Dateien untersucht. Hierzu kommen meist wiederum Werkzeuge zum Einsatz, wie in diesem Fall möglicherweise eine Bildbetrachtungssoftware zur Darstellung gecachter Bilddateien oder ein Webbrowser, um zwischengespeicherte HTML-Dateien zu rendern. In diesem Schritt versucht der Forensiker herauszufinden, um welche konkreten Inhalte es sich handelt. In Abhängigkeit vom bereits erwähnten Dateiformat der Dateien und dem eingesetzten Betriebssystem, können auch weitere Informationen, wie beispielsweise Zeitstempel oder der Name des Benutzers, der das Cachen der Webseite verursacht hat, zur Verfügung stehen. Auch die Herkunft der Inhalte, also die URL von der sie durch den Browser heruntergeladen wurden, können ausgelesen werden.

Diese Art von Spuren unterliegt für gewöhnlich einem unbewussten Entstehungsprozess, da die Tatsache, dass ein Benutzer mit diesem konkreten Benutzernamen das Cachen dieser konkreten Webseite mit diesen Inhalten zu genau dieser Zeit anstößt, höchst individuell ist. Daher ist es als unwahrscheinlich anzusehen, dass sich ein zweiter Computer (insbesondere im Kreis der Verdächtigen) findet, der exakt die gleichen (und nur diese) Spuren aufweist. Als Ergebnis der Individualisierung würde der forensische Wissenschaftler feststellen, dass auf dem untersuchten System dieser konkrete Webbrowser zur spezifizierten Zeit diese Inhalte geladen und daher gecacht hat.

Bei Browsern neuester Generation könnte diese Aussage zum Teil nur weniger scharf formuliert werden, da zum Teil Inhalte von Webseiten im Voraus geladen werden, wenn sie von der aktuell betrachteten Seite verlinkt werden.

Assoziation

Als Ergebnis der vorausgegangenen Schritte ist der Forensiker in der Lage, eine Assoziation zwischen einem konkreten Benutzer des untersuchten Systems und einer Webseite herzustellen. Außerdem kennt er den Zeitpunkt des Ereignisses (den Aufruf der Website) und die geladenen Inhalte.

Beispiel: Copy/Move Operationen im Hauptspeicher

Die vorhergehenden Beispiele berührten immer in irgendeiner (wenn auch schwachen) Form einen „physischen Kontakt“, sei es unmittelbar sichtbar wie im ersten Beispiel oder durch eine Netzverbindung wie im dritten Beispiel. In diesem Beispiel möchten wir zeigen, dass sich auch der reine Transfer von Mustern in Form einer Kopieroperation eines Computers (also auf niedrigster Ebene einer *copy*- oder *move*-Maschineninstruktion) in den Prozess der Assoziation fügt. Allerdings müssen hierzu zunächst einige Annahmen über die Systemumgebung getroffen

beziehungsweise definiert werden, um die zweifelsfreie Herstellung einer Assoziation zu ermöglichen. Daher ist das letzte Beispiel eher künstlicher Natur und weniger intuitiv verständlich als die anderen Beispiele. Auch scheint es auf den ersten Blick mit der Praxis wenig zu tun zu haben. Jedoch ist es mit Bedacht auf den minimalen Kern reduziert und zeigt die Assoziation eines Speicherbereiches (Objekt A) mit einem anderen Speicherbereich (Objekt B) eines Computers als integralen Bestandteil aller zuvor aufgeführten Beispiele.

Im Gegensatz zu realen Computern erlaubt der hier betrachtete, abstrakte Automat drei anstatt nur zwei unterschiedliche Werte für jede Speicherstelle: Neben den gebräuchlichen binären Werten 0 und 1, führen wir einen expliziten NIL-Wert $\perp$ ein. Unser Automat ist mit einem 2-Bit read-only Speicher (ROM) ausgestattet: Das erste Bit, welches wir mit A bezeichnen, speichert den Wert 0, während die zweite Speicherstelle B den Wert 1 enthält. Weiterhin operiert der Rechner auf einem 1-Bit random-access Speicher (RAM) R, der mit dem Wert $\perp$ initialisiert ist. Wir nennen die aktuelle Zuweisung von Werten zu diesen drei Speicherstellen den *Zustand* des Automaten.

Der einzige Befehl, der auf dieser Maschine ausgeführt werden kann, ist der *move*-Befehl `mov`, der den Wert einer Ursprungs-Speicherstelle in eine Ziel-Speicherstelle kopiert. Die Syntax dieses Kommandos lautet wie folgt: `mov` ⟨`Quelle`⟩, ⟨`Ziel`⟩. Als Ursprungs-Speicherstelle kann jede der 3 Speicherstellen des Automaten (A, B und R) genutzt werden. Als Ziel der Operation kann aber ausschließlich der RAM R zum Einsatz kommen, da der ROM-Speicher feste Werte enthält und nicht beschrieben werden kann. Schließlich nehmen wir an, dass es keinerlei externe Einflüsse wie beispielsweise Strahlung gibt, welche Einfluss auf den Automaten nehmen und ohne Ausführung eines Befehls dessen Zustand verändern könnten. Abbildung 12 veranschaulicht zum einen den Initialzustand des Automaten in der linken Hälfte der Abbildung und zum anderen den Zustand, nachdem die Operation `mov` B, R ausgeführt wurde (rechter Teil der Abbildung).

Als Beispiel für die Assoziation betrachten wir nun den Fall, in dem wir den Automaten im Zustand nach der Ausführung besagten Kommandos vorfinden, wie er in Abbildung 12 dargestellt wird.

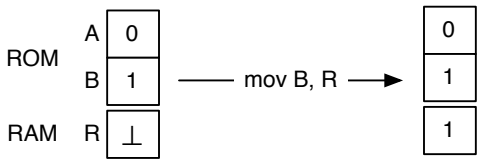

Abb. 12: Zustand des 3-Bit Automaten vor und nach der Ausführung eines `mov` Befehls.

Identifikation

Wenn wir den gegebenen Zustand untersuchen, können wir zunächst feststellen, dass der RAM im Gegensatz zum bekannten initialen Zustand des Systems nicht den Wert $\perp$ enthält. Daher ziehen wir die Schlussfolgerung, dass RAM R Spuren eines Ereignisses innerhalb des Systems aufweist und identifizieren diesen als potentielles Beweismittel für dieses Ereignis.

Klassifizierung

Im nächsten Schritt könnten wir die identifizierten Spuren als Bit $R \in \{0, 1\}$ klassifizieren und schlussfolgern, dass es eine Kopie einer Speicherstelle ist, welche nicht den Wert $\perp$ enthält. Obgleich möglicherweise nicht offensichtlich, so ist dies eine klassifizierende Eigenschaft, da bekannt ist, dass R in unserem System immer ein Bit enthält, nachdem ein `mov`-Kommando ausgeführt wurde. Weiterhin ist diese Eigenschaft noch nicht individualisierend, da wir weder das exakte Kommando

(mit Quell- und Zieloperator) kennen, noch die Speicherstelle bekannt ist, aus der dieser konkrete Wert stammt.

Individualisierung

Im Schritt der Individualisierung untersuchen wir wiederum den eigentlichen Inhalt des RAMs und stellen fest, dass R den konkreten Wert 1 enthält. Daher wissen wir nun, dass diese Spur ausschließlich eine Kopie einer anderen Speicherstelle, die diesen Wert enthält, sein kann.

Assoziation

Aufgrund des Vorwissens über unseren 3-Bit Automaten können wir schließen, dass das in R gespeicherte Bit ausschließlich von ROM B stammen kann, da dies die einzige Speicherstelle im System ist, die neben R den Wert 1 enthält. Daher können wir nun schlussfolgern, dass die Operation `mov` B, R ausgeführt wurde (was unser rekonstruiertes Ereignis ist) und diese Spur hinterlassen hat. Wir können weiterhin die Irrtumswahrscheinlichkeit für diese Aussage spezifizieren: Die Wahrscheinlichkeit, dass `mov` B, R nicht ausgeführt wurde, ist in diesem Modell 0, da es keinerlei äußere Einflüsse gibt und die einzige Möglichkeit, den Wert des RAMs zu verändern die Ausführung der `mov` Operation ist.

Es kann selbstverständlich sein, dass außerdem weitere Operationen stattgefunden haben, wie beispielsweise zuvor `mov` A, R. Es könnte sogar im Anschluss an das rekonstruierte Ereignis die Aktion `mov` R, R ausgeführt worden sein. Die Aussage, dass die Operation `mov` B, R ausgeführt wurde, wird hiervon jedoch nicht beeinträchtigt. Dies liegt an den stark individualisierenden Merkmalen der Aktion.

Quantifizierung der Irrtumswahrscheinlichkeit

Ein wesentlicher Bestandteil der Assoziation ist die Quantifizierung der Irrtumswahrscheinlichkeit. Die Irrtumswahrscheinlichkeit beziffert die „Überzeugungskraft“ der Assoziation im Gerichtsverfahren. Die Irrtumswahrscheinlichkeit beziffert die Wahrscheinlichkeit, dass kein Kontakt stattfand, obwohl dieser festgestellt wurde. Die Berechnung der Irrtumswahrscheinlichkeit ist wie auch im Bereich der klassischen Forensik immer abhängig vom Kontext. Meist müssen sehr viele Annahmen getroffen werden, um zu einer Berechnungsgrundlage zu kommen.

Statt quantitative Angaben machen zu wollen, definiert Casey [2011, S. 69f] sieben *qualitative* Grade von Wahrscheinlichkeit (*levels of certainty*). Diese Stufen verbindet er mit sprachlichen Ausdrücken, die in Gutachten oder vor Gericht verwendet werden können. Wir betrachten diese sieben Grade nun im Einzelnen:

- Das Ereignis ist *fehlerhaft / inkorrekt* (Grad C0).
  Die Spuren widersprechen bekannten Fakten oder stimmen nicht überein. Beispielsweise werden bestimmte Aktivitäten wie der Versand von Spam durch bekannte Formen von Schadsoftware durchgeführt. Die Behauptung, eine Person hätte absichtlich und manuell diese Spam-Nachrichten verschickt, wäre fehlerhaft.
- Das Ereignis ist *sehr unwahrscheinlich* (C1).
  Die Spuren sind fragwürdig.
- Das Ereignis ist *unwahrscheinlich* (C2).
  Es gibt nur eine Quelle für die digitale Spur und diese Quelle war nicht geschützt vor Manipulationen.

- Das Ereignis ist *möglich* (C3).
  Die Quelle(n) der digitalen Spur sind schwerer zu manipulieren als im Fall C2 aber es gibt entweder nicht genügend Spuren oder die Spuren sind inkonsistent.
- Das Ereignis ist *wahrscheinlich* (C4).
  Entweder ist die digitale Spur gegen Manipulationen geschützt gewesen, oder es existieren mehrere unabhängige und übereinstimmende digitale Spuren. Beispiele sind konsistente Spuren auf der Festplatte eines mutmaßlichen Erpressers: die Erpressungs-E-Mail als Kopie im Postausgang sowie mehrere Entwürfe derselben E-Mail und elektronische Kontoauszüge, die den Eingang des erpressten Geldes auf dem Konto des Beschuldigten dokumentieren.
- Das Ereignis ist *sehr wahrscheinlich* (C5).
  Es gibt mehrere unabhängige und übereinstimmende digitale Spuren, die zudem vor Manipulationen geschützt waren. Allerdings existieren kleinere Inkonsistenzen, beispielsweise leichte Abweichungen der Zeitstempel. Wenn etwa die IP-Quelladresse von bösartigem Netzwerkverkehr auf einen Anschluss X aufgelöst wird und zusätzlich durch die Überwachung von Netzwerkverkehr festgestellt wird, dass derselbe Verkehr vom Anschluss X kommt, dann ist es sehr wahrscheinlich, dass die Aktivitäten in der Tat über den Anschluss X ins Netz gelangten.
- Das Ereignis ist *sicher* (C6).
  Die digitalen Spuren waren vor Manipulationen geschützt oder haben hohe statistische Konfidenz. Beispiele sind Funde von inkriminierenden Dateien auf einer Festplatte, die neben einer visuellen Inspektion auch über ihre kryptographischen Fingerabdrücke (mittels kryptographischer Hashfunktionen) als solche identifiziert werden können.

Tabelle 1 stellt die deutschen und englischen Begriffe der verschiedenen Grade gegenüber. Für die Praxis erscheinen vor allem die Stufen C0 sowie C4 bis C6 relevant. Hier muss man allerdings differenziert argumentieren.

Tabelle 1: Deutsche und englische Begriffe für Qualitative Grade von Wahrscheinlichkeit nach Casey [2011].

Grad	Ausdruck (Deutsch)	Ausdruck (Englisch)
C0	inkorrekt	*erroneous / incorrect*
C1	sehr unwahrscheinlich	*highly uncertain*
C2	unwahrscheinlich	*somewhat uncertain*
C3	möglich	*possible*
C4	wahrscheinlich	*probable*
C5	sehr wahrscheinlich	*almost certain*
C6	sicher	*certain*

Casey [2011] betont, dass diese Stufen weiterhin subjektiv bleiben: Verschiedene Ermittler können auf Basis derselben Spuren zu unterschiedlichen Einschätzungen kommen. Insofern sei die Skala auch nur als ein erster Ansatz zu verstehen, welcher noch weiter erforscht werden muss. Generell basiert aber bereits die Quantifizierung einer relativ einfache Aussage wie „Der Nutzer hat Datei x über die Tauschbörse y bezogen“ auf einer Vielzahl von Annahmen. Sie alle aufzuzählen und darauf eine komplexe Berechnung aufzubauen, erscheint generell möglich, ist aber nur für sehr eingeschränkte und sehr exakt fassbare Aussagen sinnvoll [Overill et al., 2013, Overill and Silomon, 2012, Overill et al., 2010]. Zudem muss wie in der klassischen Forensik zwischen zwei Wahrscheinlichkeiten unterschieden werden:

1. Die Irrtumswahrscheinlichkeit bei der Interpretation einer digitalen Spur, und

2. die Wahrscheinlichkeit, mit der die digitale Spur unverfälscht vorliegt.

In der klassischen Forensik gibt es im Kontext der vermeintlich so objektiven DNA-Analyse immer wieder Pannen, die vor allem die zweite Wahrscheinlichkeit beeinflussen (etwa die Kontamination des Spurenträgers wie beim „Phantom von Heilbronn“ [Schüle, 2008]). Gerade die zweite Wahrscheinlichkeit muss bei der Anfälligkeit digitaler Spuren gegenüber Manipulationen besonders beachtet werden.

Sinnvoll ist die Quantifizierung der Irrtumswahrscheinlichkeit also nur bei sehr einfachen Fragestellungen, die man präzise als Assoziationen ausdrücken kann und für die einfache Basisannahmen getroffen werden können. Komplexere Aussagen werden insbesondere durch die Summe möglichst vieler unabhängiger (und untereinander konsistenter) Spuren überzeugend, auch wenn für sie keine exakte Irrtumswahrscheinlichkeit anzugeben ist. In diesem Sinne kann auch der oben beschriebene Ansatz von Casey interpretiert werden.

2.5 Assoziation als zentraler Aspekt der forensischen Informatik

Nachdem wir gesehen haben, dass das Konzept der Assoziation auch im Bereich der digitalen Spuren sinnvoll ist, setzen wir diese Einsicht in den Kontext allgemeiner Betrachtungen zur Praxis und zur Definition des Gebietes der forensischen Informatik.

Computerforensik

Die *Computerforensik* [Geschonneck, 2006] umfasst in ihrer aktuellen Form eine Vielzahl unterschiedlichster Aufgaben, wie beispielsweise

- die möglichst schnelle Bewertung eines Sicherheitsvorfalls anhand erster durch Techniken der *Live-Analyse* [Carrier, 2005, S. 13 ff.] erhobener Daten zur Planung der weiteren Untersuchung des Vorfalls.
- die Anfertigung einer forensischen Kopie physischer Speichermedien unter Einsatz spezieller Hard- und Software.
- die Umgehung von Schutzmechanismen digitaler Systeme, um eine Erhebung von Daten zu ermöglichen.
- die Extraktion kryptographischer Schlüssel aus Hauptspeicherabbildern, zur Erhebung verschlüsselter Daten.
- die Rekonstruktion gelöschter Daten anhand von Dateisystem Metadaten oder durch *Filecarving*.
- die Erstellung von Timelines untersuchter Systeme, also die Erfassung einer zeitlichen Abfolge vergangener Ereignisse auf dem untersuchten System.

Ein weiteres Problemfeld der Computerforensik entspringt der Notwendigkeit mit immer größeren Datenmengen umgehen können zu müssen [Bäcker et al., 2010]. Dies umfasst sowohl die reine Gewinnung, Speicherung und Verarbeitung der Daten, als auch die Aufgabe in der beständig steigenden Datenmenge diejenigen Objekte zu identifizieren, die für die Untersuchung inhaltlich relevant sind.

In den meisten Fällen sind Computerforensiker stark in den Ermittlungsprozess einbezogen oder leiten ihn sogar. Sie erheben erste Spuren, beziehen diese auf den konkreten Fall und ziehen daraus Schlüsse, um weitere Schritte festzulegen. Hierbei spielt sowohl die Erfahrung der Experten, als auch ihr Wissen über funktionale

Zusammenhänge und Prinzipien in digitalen Systemen eine wichtige Rolle. Dies gilt insbesondere im Zusammenhang mit *Incident Response* [Mandia et al., 2003] im Unternehmensumfeld, wo die Verantwortung für die gesamte Untersuchung in den Händen von sogenannten CERTs (*Computer Emergency Response Teams*) liegt. Aber auch in der Strafverfolgung werden viele Ermittlungen durch speziell ausgebildete Experten geleitet. *Alle* diese Tätigkeiten fallen heute in den Bereich der Computerforensik (siehe Casey [2011], Mandia et al. [2003], Garfinkel [2010]).

Vergleicht man nun die Computerforensik mit der in Abschnitt 1 beschriebenen Theorie klassischer Forensik, so lässt sich ein gewisses Missverhältnis zwischen der Art von Aufgaben, mit denen sich die Forensiker in den beiden Gebieten befassen, feststellen. Während in der Theorie von Inman and Rudin [2000] die Begriffe *Transfer* und *Assoziation* den zentralen Aspekt jeder forensischen Fragestellung darstellen, scheint die Computerforensik einen wesentlich weiter gefassten Fokus zu besitzen. Carrier and Spafford [2004] erklärt dies „historisch“ durch einen „wesentlich komplexeren Prozess, bei dem der Ermittler die Aktivitäten des Benutzers nachverfolgen muss und keine einfache Ja-oder-Nein-Antwort geben kann“ („*…much more involved process where the investigator must trace user activity and cannot provide a simple yes or no answer*“ [Carrier and Spafford, 2004]). Lässt sich die zentrale Theorie des Transfers jedoch auf die meisten Fragestellungen der Computerforensik nicht übertragen, so stellt sich die Frage, ob die Computerforensik überhaupt als forensische Wissenschaft (im Sinne von Inman and Rudin [2000]) bezeichnet werden kann.

Einen ersten Anhaltspunkt für eine beginnende Differenzierung in der Forschungsgemeinschaft der Computerforensik liefern Böhme et al. [2009], die feststellen, dass Multimediaforensik nicht gleich Computerforensik ist. Die Multimediaforensik befasst sich mit bestimmten Arten digitaler Spuren, wie digitale Fotos, Videos oder anderen Arten von Aufnahmen. Böhme et al. [2009] argumentieren, dass diese Multimediadaten mittels Sensoren aus der physischen Welt aufgezeichnet werden und nicht *vollständig* in einem digitalen System entstehen, wie es beispielsweise bei E-Mails, Text-Dokumenten oder Log-Dateien der Fall ist. In der Multimediaforensik spielen also individualisierende Merkmale der physikalische Aufzeichnungseinheit eine zentrale Rolle.

Forensische Informatik

Wir definieren allgemein *forensische Informatik* als die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems. Insbesondere stellt die forensische Informatik Methoden zur gerichtsfesten Sicherung und Verwertung digitaler Spuren bereit. Unsere Definition stellt die Informatik stärker als bisher in den Kontext anderer forensischer Wissenschaften. Die Betonung des wissenschaftlichen Aspekts ist außerordentlich wichtig, da eine forensische Beweisführung dazu führen kann, dass Menschen ihrer Freiheit beraubt werden. Nur eine verlässliche und objektive (wissenschaftliche) Methodik wird dieser Verantwortung gerecht. Die angewendete Methodik muss daher auch immer wieder neu hinterfragt und überdacht werden. Eine besondere Rolle spielt die Unterfütterung des Gebietes mit theoretischen Grundlagen der klassischen Forensik, und ein tieferes Verständnis der Art von Spuren, die in der forensischen Informatik untersucht werden.

Wir unterscheiden zwei Aspekte der forensischen Informatik und teilen die relevanten Methoden in zwei Gebiete:

1. Die forensische Informatik im *engeren Sinne* umfasst eine sehr fokussierte Menge von Fragestellungen und Methoden, welche sich im Kern mit der Herstellung von Assoziationen, wie sie zuvor geschildert wurden, befasst.

Weiter unten in Abschnitt 2.5 geben wir eine Reihe von Beispielen solcher Fragestellungen, um den Fokus dieses Gebietes zu veranschaulichen. Die Anwendung gemeinsamer Theorien mit anderen forensischen Wissenschaften macht dieses Teilgebiet der forensischen Informatik tatsächlich zu einer forensischen Wissenschaft.

2. Forensische Informatik *im weiteren Sinne* umfasst den gesamten Prozess der Durchführung einer digitalen Ermittlung, wie beispielsweise die Suche nach digitalen Spuren, das Rekonstruieren gelöschter Daten, der Umgang mit großen Speichermengen und so weiter.

Der Bereich der forensischen Informatik im weiteren Sinne integriert viele Themenbereiche der Informatik, die bisher unabhängig voneinander agierten, wie zum Beispiel die Massendatenanalyse (*data mining*, *big data*), das Netzwerk-Fingerprinting, Reverse Engineering, die Hauptspeicheranalyse, Seitenkanalanalyse und Datenschutztechniken.

In der Praxis deutet sich eine thematische Aufteilung der eingesetzten Techniken an, die sich an der Flüchtigkeit der betrachteten digitalen Spuren orientiert (vergleiche Abschnitt 2.3). So kann man drei Unterbereiche dieses Gebietes unterscheiden:

1. Sicherung und Analyse persistenter Spuren, also vornehmlich Festplatten. In Anlehnung an die englischsprachige Terminologie wird dies oft als die *Tot-Analyse* (*dead analysis*) oder *Post-Mortem-Analyse* bezeichnet.
2. Sicherung und Analyse von flüchtigen Spuren im weiteren Sinne, also der Inhalte von Hauptspeicher, Caches etc. (zumeist im Rahmen einer *Live-Analyse*).
3. Sicherung und Analyse von flüchtigen Spuren im engeren Sinne, meist Spuren im Netz. Dieser Teilbereich wird häufig als *Netzwerkforensik* bezeichnet.

Fragestellungen der forensischen Informatik im engeren Sinne

In Abschnitt 2.4 haben wir bereits gezeigt, dass man viele Ermittlungsfragestellungen auf Fragen nach Assoziationen reduzieren kann. Die strikte Anwendung der Theorie von Transfer und Assoziation zwingt den Forensiker, einzelne präzise Aussagen über seine Befunde zu formulieren. Da der Begriff des Transfers so grundlegend und bereits aus anderen forensischen Disziplinen bekannt ist, sind die Aussagen, welche am Ende des Prozesses zur Assoziation getroffen werden, auch für technisch meist weniger versierte Personen, wie beispielsweise Richter oder Rechtsanwälte, leicht verständlich. Die in Abschnitt 2.4 behandelten Beispiele untermauern dies. Die dort getroffenen Aussagen sind folgende:

1. Foto *A* wurde durch Digitalkamera *B* aufgenommen.
2. USB-Speichergerät *A* war an Computer *B* angeschlossen.
3. Computer *A* hat Website *B* aufgerufen.
4. Daten an Stelle *A* wurden von Speicherstelle *B* kopiert.

Staatsanwälte formulieren gerade solche Aussagen häufig als Fragen an die forensischen Wissenschaftler. Sie beruhen auf einzelnen und leicht nachvollziehbaren Assoziationen, aus welchen Staatsanwälte oder Richter Schlussfolgerungen ableiten können. Es gibt weit mehr Beispiele solcher Fragen, die im Kontext einer Ermittlung gestellt werden können. Hier folgen nur einige wenige Beispiele:

- Wurde Website *A* auf Rechner *B* aufgerufen?
- Wurde E-Mail *A* (Absender, Empfänger, Datum, Betreff, Inhalt, Datei-Anhänge) auf diesem Rechner verfasst und an Rechner *B* verschickt?
- War USB-Stick *A* einmal an Rechner *B* angeschlossen?
- Wurde Datei *A* (bitweiser Vergleich oder Hash-Vergleich) auf Rechner *B* kopiert oder heruntergeladen?
- Findet sich Stichwort *A* in Dokumenten auf Rechner *B*?
- Befinden sich auf Rechner *A* Videos mit Inhalt *B*?
- Wurde auf Rechner *A* Software *B*, wie beispielsweise eine bestimmte Filesharing- oder Datenvernichtungssoftware, eingesetzt?
- Wurde Rechner *A* durch Malware *B*, wie beispielsweise einen Banken-Trojaner, kompromittiert?
- Wurde mit Rechner *A* eine Instant Messenging-/VoIP- Kommunikation mit folgender/m Person/Synonym *B* geführt?

Derartige Hypothesen zu belegen oder zu widerlegen stellt den Kern dessen dar, was forensische Wissenschaftler in der forensischen Informatik tun sollten. Alle Untersuchungen und Analysen sollten auf die Beantwortung solcher Fragen nach Assoziationen in der digitalen Welt ausgerichtet sein. Die Beantwortung jeder dieser Fragestellungen erfordert ein hohes Maß an Spezialisierung und Fachkenntnis, um das in Gerichtsverfahren geforderte Niveau an Gewissheit zu erlangen. Dies ist der Teil der Computerforensik, der am deutlichsten in der Tradition anderer forensischer Wissenschaften steht.

Die Leitung einer Ermittlung und die Formulierung der durch forensische Wissenschaftler zu beantwortenden Fragen stellt den anderen Teil forensischen Informatik dar, der häufig ebenfalls als Computerforensik bezeichnet wird [Geschonneck, 2006] und durch entsprechend geschulte Polizeibeamte und Juristen durchgeführt werden kann: Diese Aufgabe erfordert ein gewisses Maß an Wissen über Verbrechen (Modus Operandi, Kriminologie usw.) und ein Basiswissen im Bereich der elektronischen Datenverarbeitung. Es besteht jedoch keine Notwendigkeit dafür, dass diese Personen forensische Wissenschaftler sein müssen und daher ein hohes Maß an technischer Expertise im Bereich der Informatik erwerben müssen. Hervorzuheben ist jedoch, dass beide Aspekte der forensischen Informatik gleichmaßen wichtig sind.

Die beschriebene Unterteilung der Computerforensik in diese beiden geschilderten Aspekte fördert eine wissenschaftlich ausgerichtete forensische Informatik und die Erreichung von Standards, wie sie in forensischen Wissenschaften anderer Bereiche bereits seit langem als normal angesehen werden.

Fragestellungen der forensischen Informatik im weiteren Sinne

Eine der wichtigsten Problemstellungen der forensischen Informatik im weiteren Sinne ist die Aufbereitung großer Datenmengen. Die dabei auftretenden Probleme sind außerordentlich vielfältig und aufwändig.

2.6 Verwandte Literatur

Zur Integration der Informatik in die Reihe forensischer Wissenschaften

Es gab bereits mehrere Ansätze, die praktische Computerforensik mit klassischen Theorien der Forensik zu vereinen. Vor allem ist hier die Arbeit von Carrier and Spafford [2003] zu nennen, die den *digitalen Tatort* (*digital crime scene*) in Analogie zum physischen Tatort definieren. Allerdings basieren deren Empfehlungen auf Büchern [James and Nordby, 2009, Saferstein, 2010] (in älteren Auflagen), deren Fokus eher in der Erläuterung konkreter Techniken als in der Untersuchung einheitlicher Theorien besteht. Ebenso ordnen Carrier and Spafford [2004] die Rekonstruktion von Ereignissen der digitalen Welt den entsprechenden Konzepten der physischen Welt zu. Das Konzept des Transfers klingt aber lediglich implizit bei der Betrachtung von Zustandsübergängen in Automaten an.

Pollitt [2008] war der erste, der die Theorie von Inman and Rudin [2000] auf die Computerforensik anwandte. Pollitt identifiziert bereits die Notwendigkeit zur Anwendung aus der klassischen Forensik bekannter Theorien auf das Gebiet der Computerforensik. Er skizziert, wie Inmans und Rudins Prozess der Assoziation in der digitalen Welt aussehen könnte. Das, wie in Abschnitt 1 geschildert, zugehörige Konzept des Transfers liegt jedoch außerhalb von Pollitts Fokus.

Weiterhin haben auch Cohen [2010, 2011] und Cohen et al. [2011] die digitale Forensik in den Kontext von Inman and Rudin [2000] gestellt. Deren Fokus liegt jedoch vielmehr auf dem Konzept des Transfers als auf dem der Assoziation und dem zugehörigen Prozess hin zur Assoziation. Eine vollständige Integration der forensischen Informatik in den Kontext der Theorie von Inman and Rudin [2000] wurde erstmals von Dewald and Freiling [2012] entwickelt (vgl. auch die erweiterte Version von Dewald and Freiling [2014]).

Zur Praxis der Computerforensik

Es gibt eine große Anzahl von Basiswerken der Computerforensik, die sich primär technischen Aspekten der Durchführung von Untersuchungen widmen.

Kruse II and Heiser [2001] beschreiben in ihrem Buch praxisnah die forensische Sicherung und Auswertung von Datenträgern unter Benutzung konkreter Werkzeuge. So werden die grundlegenden Funktionen dieser Software anhand von Bildschirmfotos oder der Aufrufsyntax von Kommandozeilen-basierten Anwendungen erläutert. Das Werk von Kruse II und Heiser beschreibt weiterhin die Untersuchung spezifischer Fall-Beispiele, gibt Ratschläge zur Analyse von Windows- und Unix-basierten Systemen und versteht sich als Handbuch für Ermittler im Bereich der Computerforensik.

Das Buch *Forensic Discovery* von Farmer and Venema [2005] gehört neben Casey [2011] sicherlich zu den wichtigsten englischsprachigen Standardwerken. Im ersten Kapitel liefern die Autoren auch einen Überblick über einige der wichtigsten praktischen Grundlagen, wie die *Reihenfolge der Flüchtigkeit* (*Order Of Volatility, OOV*), Abstraktionsebenen von Daten, die Manipulierbarkeit von Daten und die prinzipielle Wiederherstellbarkeit gelöschter Daten. Wirklich grundlegende Theorien sind in diesem eher praxisorientierten Leitfaden jedoch verständlicherweise nicht zu finden.

Paul [2009] betrachtet digitale Spuren vor allem im Lichte amerikanischer Rechtsprechung und geht zunächst auf juristische Anforderungen an digitale Spuren ein. Hier nennt Paul die in dieser Arbeit angesprochene wissenschaftliche Methode bei

der Erhebung digitaler Spuren als Forderung des amerikanischen Verfassungsgerichtes (des *supreme court*), welcher hierzu ebenfalls die Arbeit von Popper [1962] zitiert. Interessant sind weiterhin Pauls Ausführungen über Ereignisse (*events*) in digitalen Systemen, welche er als das grundlegendste Phänomen der digitalen Welt bezeichnet. Ereignisse — so Paul — sind die Ursache für die Modifizierung von Daten und der Entstehung von Spuren. Er erkennt weiter, dass ein solches Ereignis in der digitalen Welt zumeist nicht wirklich aus einem einzelnen Ereignis, sondern aus einer Folge vieler Einzelereignisse besteht.

> „Naturally, events precede or follow one another in time. One event may cause one or more subsequent events.“ [Paul, 2009, S. 27]

Diese Überlegungen sind denen dieser Arbeit im Ansatz durchaus ähnlich, leider bleiben dies jedoch die einzigen grundlegenden Betrachtungen in Pauls Buch.

Als deutschsprachiges Pendant zu Farmer and Venema [2005] kann das Buch *Computer Forensik* von Geschonneck [2006] angesehen werden. Auch dieses Werk ist primär als pragmatisch geprägtes Handbuch für die Durchführung spezifischer digital-forensischer Untersuchungen zu sehen und behandelt beispielsweise den korrekten Umgang mit digitalen Beweismitteln, deren gerichtsverwertbare Sicherung, die Anfertigung eines Datenträgerabbildes oder die Wiederherstellung gelöschter Daten anhand konkreter Dateisysteme. Geschonneck gibt weiterhin einen Überblick und eine kurze Einführung in die gängigsten freien und kommerziellen Software-Werkzeuge. Eine Betrachtung theoretischer Grundlagen fehlt hier jedoch.

2.7 Zusammenfassung

In diesem Abschnitt haben wir kurz die Entstehung digitaler Spuren betrachtet und ihre Eigenschaften untersucht. Daraufhin wurde die Herstellung von Assoziationen in der digitalen Welt als Kern der forensischen Informatik als forensische Wissenschaft identifiziert und mit der aktuellen Auffassung digitaler Forensik in der Praxis verglichen.

Verzeichnisse

I. Abbildungen

Abb. 1: Filter zur Sammlung mikroskopischer Spuren. . . . 17
Abb. 2: Schematische Darstellung von Locards Austauschprinzip. . . . 17
Abb. 3: Transfer von Texturen auf Bruchstücke eines Objekts. . . . 18
Abb. 4: Übereinstimmende Bruchkanten in einem Kabel. . . . 18
Abb. 5: Kratzspuren eines Werkzeugs (oben) auf einem verformbaren Material. . . . 19
Abb. 6: Schematische Darstellung des Laufs einer Schusswaffe. . . . 19
Abb. 7: Schema eines Vergleichsmikroskops. . . . 20
Abb. 8: Vergleich von Spuren auf Kugeln. . . . 20
Abb. 9: Beispiel für gleichzeitigen Austausch von Muster und Materie. . . . 21
Abb. 10: Schematische Darstellung des Weges zur Assoziation. . . . 23
Abb. 11: Die Erweiterung von Locards Austauschprinzip auf den digitalen Tatort nach Casey. . . . 31
Abb. 12: Zustand des 3-Bit Automaten vor und nach der Ausführung eines `mov` Befehls. . . . 44

II. Beispiele

Beispiel 1: Authentizität vs. Integrität . . . 15
Beispiel 2: Informationsverlust durch digitale Betrachtung . . . 26
Beispiel 3: Integrität mittels Hashwerte . . . 27
Beispiel 4: Authentizität durch digital signierten Hashwert . . . 28
Beispiel 5: Übertragungen in der digitalen Welt . . . 30
Beispiel 6: Abstraktionsschichten digitaler Spuren . . . 32
Beispiel 7: Manipulation digitaler Spuren . . . 34
Beispiel 8: Manipulation digitaler Spuren . . . 35

III. Definitionen

Definition 1: digitale Spuren . . . 25
Definition 2: Technisch vermeidbare Spuren . . . 33
Definition 3: Technisch unvermeidbare Spuren . . . 34

IV. Exkurse

Exkurs 1: Die „sozialistische“Kriminalistik . . . 10
Exkurs 2: Analogrechner . . . 25
Exkurs 3: Urkundenwesen . . . 29

V. Kontrollaufgaben

Kontrollaufgabe 1: Übertragung von Mustern . . . 30
Kontrollaufgabe 2 . . . 36

VI. Tabellen

Tabelle 1: Deutsche und englische Begriffe für Qualitative Grade von Wahrscheinlichkeit nach Casey [2011]. 46

VII. Literatur

Matthias Bäcker, Felix C. Freiling, and Sven Schmitt. Selektion vor der Sicherung - Methoden zur effizienten forensischen Sicherung von digitalen Speichermedien. *Datenschutz und Datensicherheit - DuD*, 34(2):80–85, 2010. ISSN 1614-0702. 10.1007/s11623-010-0040-4. Zitiert auf Seite 47.

Mark Benecke. *Genetischer Fingerabdruck*. ecomed Verlagsgesellschaft, 2001. Enzyklopädie Naturwissenschaft und Technik, 2. Auflage, 6. Ergänzungslieferung. Zitiert auf Seite 22.

Rainer Böhme, Thomas Gloe, Felix C. Freiling, and Matthias Kirchner. Multimedia forensics is not computer forensics. In *Proceedings of the 3rd International Workshop on Computational Forensics*, pages 90–103, Den Haag, 2009. Zitiert auf Seite 21.

Rainer Böhme, Felix C. Freiling, Thomas Gloe, and Matthias Kirchner. Multimedia forensics is not computer forensics. In *Proceedings of the 3rd International Workshop on Computational Forensics*, IWCF '09, pages 90–103, Berlin, Heidelberg, 2009. Springer-Verlag. ISBN 978-3-642-03520-3. Zitiert auf Seite 48.

Brian Carrier. *File System Forensic Analysis*. Addison-Wesley, 2005. Zitiert auf den Seiten 33, 35, 37 und 47.

Brian D. Carrier and Eugene H. Spafford. Getting physical with the digital investigation process. *Int. Journal of Digital Evidence*, 2(2), 2003. URL `http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf`. Zitiert auf Seite 51.

Brian D. Carrier and Eugene H. Spafford. Defining event reconstruction of digital crime scenes. *Journal of Forensic Science*, 49(6), 2004. Zitiert auf den Seiten 48 und 51.

Harlan Carvey and Cory Altheide. Tracking USB storage: Analysis of windows artifacts generated by USB storage devices. *Digital Investigation*, 2(2):94–100, 2005. Zitiert auf den Seiten 41 und 42.

Eoghan Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, 2004. 2. Auflage. Zitiert auf Seite 25.

Eoghan Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, 2011. 3. Auflage. Zitiert auf den Seiten 31, 45, 46, 48, 51 und 53.

Mo Chen, Jessica J. Fridrich, Miroslav Goljan, and Jan Lukás. Determining image origin and integrity using sensor noise. *IEEE Transactions on Information Forensics and Security*, 3(1):74–90, 2008. Zitiert auf Seite 41.

Fred Cohen. Toward a science of digital forensic evidence examination. In *IFIP Int. Conf. Digital Forensics*, pages 17–35, 2010. Zitiert auf Seite 51.

Fred Cohen. *Digital Forensic Evidence Examination*. ASP Press, 2011. Zitiert auf Seite 51.

Fred Cohen, Julie Lowrie, and Charles Preston. The state of the science of digital evidence examination. In *IFIP Int. Conf. Digital Forensics*, pages 3–21, 2011. Zitiert auf Seite 51.

Glenn S. Dardick, Barbara Endicott-Popovsky, Pavel Gladyshev, Thomas Kemmerich, and Carsten Rudolph. Digital Evidence and Forensic Readiness (Dagstuhl Seminar 14092). *Dagstuhl Reports*, 4(2):150–190, 2014. ISSN 2192-5283. doi: http://dx.doi.org/10.4230/DagRep.4.2.150. URL `http://drops.dagstuhl.de/opus/volltexte/2014/4549`. Zitiert auf Seite 29.

Andreas Dewald and Felix Freiling. Is computer forensics a forensic science? In *Proceedings of Current Issues in IT Security 2012*. Max-Planck-Institut für ausländisches und internationales Strafrecht, Universität Freiburg, May 2012. Zitiert auf Seite 51.

Andreas Dewald and Felix: Freiling. From computer forensics to forensic computing: Investigators investigate, scientists associate. Technical Report CS-2014-04, Friedrich-Alexander-University Erlangen-Nuremberg

(FAU), May 2014. Online: https://opus4.kobv.de/opus4-fau/files/4750/computer_forensics_is_not_forensic_science.pdf. Zitiert auf Seite 51.

Luciana Duranti. *Diplomatics: New Uses for an Old Science*. Scarecrow Press, 1998. Zitiert auf Seite 29.

Dan Farmer and Wietse Venema. *Forensic Discovery*. Addison-Wesley, 2005. Zitiert auf den Seiten 51 und 52.

Felix C. Freiling and Michael Gruhn. What is essential data in digital forensic analysis? In *Ninth International Conference on IT Security Incident Management & IT Forensics, IMF 2015, Magdeburg, Germany, May 18-20, 2015*, pages 40–48, 2015. doi: 10.1109/IMF.2015.20. URL http://dx.doi.org/10.1109/IMF.2015.20. Zitiert auf Seite 33.

Simson L. Garfinkel. Digital forensics research: The next 10 years. In *Proceedings of the Digital Forensics Research Conferencs (DFRWS)*, 2010. Zitiert auf Seite 48.

Alexander Geschonneck. *Computer Forensik*. dpunkt Verlag, 2006. 2. Auflage. Zitiert auf den Seiten 47, 50 und 52.

W. Giloi and R. Lauber. *Analogrechnen – Programmierung, Arbeitsweise und Anwendung des elektronischen Analogrechners*. Springer-Verlag, 1963. Zitiert auf Seite 25.

Dieter Gollmann. *Computer Security*. Wiley, third edition, 2011. ISBN 978-0-470-74115-3. URL http://www.wiley-vch.de/publish/dt/books/ISBN978-0-470-74115-3/. Zitiert auf den Seiten 26, 27 und 28.

Hans Groß and Friedrich Geerds. *Handbuch der Kriminalistik*, volume 1. Verlagsgesellschaft Manfred Pawlak, 1977. Zitiert auf den Seiten 9, 13 und 16.

Keith Inman and Norah Rudin. *Principles and Practice of Criminalistics: The Profession of Forensic Science*. CRC Press, 2000. Zitiert auf den Seiten 11, 12, 16, 17, 18, 19, 20, 22, 40, 48 und 51.

Stuart H. James and Jon J. Nordby, editors. *Forensic Science: An Introduction to Scientific and Investigative Techniques*. CRC Press, third edition, 2009. Zitiert auf Seite 51.

Paul L. Kirk. *Crime Investigation*. John Wiley & Sons, 1974. Herausgegeben von John I. Thornton, 2. Auflage. Zitiert auf den Seiten 13, 16, 17, 18, 19, 20 und 21.

Warren G. Kruse II and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Addison-Wesley Pub. Co. Inc., Boston, MA, USA, 2001. ISBN 978-0201707199. Zitiert auf Seite 51.

Henry C. Lee and Howard A. Harris. *Physical Evidence in Forensic Science*. Lawyers and Judges Publishing, 2000. Zitiert auf Seite 16.

Edmund Locard. *L'enquete criminelle et les methodes scientifique*. Ernest Flammarion, Paris, 1920. Zitiert auf Seite 16.

Jan Lukás, Jessica J. Fridrich, and Miroslav Goljan. Digital "bullet scratches" for images. In *ICIP (3)*, pages 65–68, 2005. Zitiert auf Seite 41.

Clifford A. Lynch. Authenticity and integrity in the digital environment: An exploratory analysis of the central role of trust. In Council on Library and Information Resources, editor, *Authenticity in a Digital Environment*, pages 32–50. Washington, D.C., 2000. Online: http://www.clir.org/pubs/reports/reports/pub92/pub92.pdf. Zitiert auf den Seiten 27, 28 und 29.

Kevin Mandia, Chris Prosise, and Matt Pepe. *Incident Response & Computer Forensics*. McGraw-Hill, 2003. 2. Auflage. Zitiert auf Seite 48.

Pierre Margot. Forensic science on trial — what is the law of the land? *Australian Journal of Forensic Sciences*, 43(2–3):89–103, 2011. URL http://dx.doi.org/10.1080/00450618.2011.555418. Zitiert auf Seite 11.

Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997. Zitiert auf den Seiten 27, 28 und 36.

Richard E. Overill and Jantje A. M. Silomon. Uncertainty bounds for digital forensic evidence and hypotheses. In *Seventh International Conference on Availability, Reliability and Security, Prague, ARES 2012, Czech Republic, August 20-24, 2012*, pages 590–595, 2012. doi: 10.1109/ARES.2012.17. URL `http://dx.doi.org/10.1109/ARES.2012.17`. Zitiert auf Seite 46.

Richard E. Overill, Jantje A. M. Silomon, and Kam-Pui Chow. A complexity based model for quantifying forensic evidential probabilities. In *ARES 2010, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow, Poland*, pages 671–676, 2010. doi: 10.1109/ARES.2010.42. URL `http://dx.doi.org/10.1109/ARES.2010.42`. Zitiert auf Seite 46.

Richard E. Overill, Jantje A. M. Silomon, Kam-Pui Chow, and Hayson Tse. Quantification of digital forensic hypotheses using probability theory. In *Eighth International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2013, Hong Kong, China, November 21-22, 2013*, pages 1–5, 2013. doi: 10.1109/SADFE.2013.6911547. URL `http://dx.doi.org/10.1109/SADFE.2013.6911547`. Zitiert auf Seite 46.

George L. Paul. *Foundations of Digital Evidence*. American Bar Association, Chicago, USA, 2009. ISBN 978-1604421040. Zitiert auf den Seiten 51 und 52.

Mark Pollitt. Applying traditional forensic taxonomy to digital forensics. In Indrajit Ray and Sujeet Shenoi, editors, *Advances in Digital Forensics IV*, chapter 2, pages 17–27. Springer Verlag, 2008. Zitiert auf Seite 51.

Karl Popper. *Conjectures and Refutations: The Growth of Scientific Knowledge*. Routledge, 1962. Deutsch: Vermutungen und Widerlegungen. Zitiert auf den Seiten 7 und 52.

Corinne Rogers. Digital records forensics: Integrating archival science into a general model of the digital forensics process. In *Proc. of the Second International Workshop on Cyberpatterns: Unifying Design Patterns with Security, Attack and Forensic Patterns*, pages 4–21. Oxford Brookes University, 2013. `http://tech.brookes.ac.uk/CyberPatterns2013/`. Zitiert auf Seite 29.

Richard Saferstein. *Criminalistics: An Introduction to Forensic Science*. Pearson, 10th edition, 2010. Zitiert auf Seite 51.

Christian Schüle. Die Unsichtbare. *Die Zeit*, (18), April 2008. Zitiert auf Seite 47.

F.-R. Schurich. Zur Definition des Begriffes "Spur". *Kriminalistik und forensische Wissenschaften*, (14):5–27, 1974. Zitiert auf Seite 10.

F.-R. Schurich. Kriminalistische Identifizierung und angrenzende Begriffe. *Kriminalistik und forensische Wissenschaften*, (46):7–22, 1982. Zitiert auf Seite 10.

F.-R. Schurich and H. Scharf. Zum Begriff der Widerspiegelung in der sozialistischen Kriminalistik. *Kriminalistik und forensische Wissenschaften*, (36):5–21, 1979. Zitiert auf Seite 10.

Robert Weihmann. *Kriminaltechnik I*. VDP, 2007. Band 2 der Lehr- und Studienbriefe Kriminalistik/Kriminologie, dritte Auflage. Zitiert auf den Seiten 10 und 13.

Robert Weihmann. Versionsbildung als Unterdrückungsinstrument der DDR-Diktatur. *Kriminalistik*, (1): 28–31, 2008. Zitiert auf Seite 10.