Klaus Vieweg (Hrsg.)

Festgabe Institut für Recht und Technik

Felix C. Freiling und Konstantin Sack

Zur Authentizität und Integrität bei (digitalen) Beweismitteln

Recht – Technik – Wirtschaft

Schriftenreihe
Herausgegeben von Professor Dr. Dr. Rudolf Lukes
Fortgeführt von
Professor Dr. Dr. Udo Di Fabio und
Professor Dr. Klaus Vieweg

Band 111

Carl Heymanns Verlag 2017

Festgabe Institut für Recht und Technik

Erlanger Festveranstaltungen 2011 und 2016

Herausgegeben von
Professor Dr. Klaus Vieweg
Friedrich-Alexander-Universität Erlangen-Nürnberg

Carl Heymanns Verlag 2017

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-452-28832-5

www.wolterskluwer.de
www.heymanns.de

Satz: R. John + W. John GbR, Köln
Druck und Weiterverarbeitung: Williams Lea & Tag GmbH, München

Gedruckt auf säurefreiem, alterungsbeständigem und chlorfreiem Papier.

Vorwort

Der vorliegende Band enthält die für den Druck überarbeiteten Vorträge, die aus Anlass des 20-jährigen und des 25-jährigen Bestehens des Erlanger Instituts für Recht und Technik gehalten oder zu diesem Anlass verfasst worden sind. Mit »Festgabe Institut für Recht und Technik« wurde ein Titel gefunden, der die beiden thematisch divergierenden Tagungen erfasst, denn alle Referenten sind dem Institut für Recht und Technik in dem Vierteljahrhundert seines Bestehens (und auch mir persönlich) verbunden – als Mitarbeiter, Kollegen und Freunde.

Die Tagung am 13./14. Mai 2011 im Erlanger Schloss hatte zum Thema »Recht und Technik – Entwicklungen und Perspektiven«. Sie dokumentierte die rasante technische Entwicklung seit dem Anfang der 1990er Jahre, die Reaktionen des Rechts und den einen oder anderen Blick in die Zukunft. Ehemalige Mitarbeiterinnen und Mitarbeiter referierten aus ihrem aktuellen beruflichen Bereich über die jeweiligen Brücken zwischen Recht und Technik, aber auch über etwaige Verbindungslücken. Ebenso zeichneten einige Kollegen aus ihren Forschungsbereichen Verbindungslinien zwischen der Technik und dem Recht auf.

Die Tagung am 20./21. Mai 2016 in der Erlanger Orangerie hatte das Thema »Interdisziplinarität« und griff damit die Forschungen im Institut für Recht und Technik auf, die immer über den »juristischen Tellerrand« geschaut haben. Das breite Spektrum der hier entstandenen Dissertationen belegt dies eindrucksvoll. Nicht nur zu den Technik- und Ingenieurwissenschaften, sondern auch zu anderen Wissenschaftsdisziplinen enthielten die Vorträge spannende Brückenschläge.

Die Vielfalt der Beiträge spiegelt auch die unterschiedlichen Präsentations- und Veröffentlichungsusancen der verschiedenen Disziplinen wider, die in dem Band beibehalten wurden. Die Beiträge der Tagung des Jahres 2011 sind auf dem damaligen Stand. Einige Autoren haben ihre Beiträge mit Aktualisierungshinweisen ergänzt.

Mein Dank gilt den Autoren, den Mitarbeiterinnen und Mitarbeitern, die wesentlich zum Gelingen der Tagungen beigetragen haben, sowie in besonderem Maße meiner langjährigen Sekretärin Sabine Trippmacher, die auch dieses Buch – wie viele andere zuvor – mit großer Sorgfalt lektoriert und für den Druck vorbereitet hat.

Erlangen, im September 2017 *Klaus Vieweg*

Inhalt

Festveranstaltung 20./21. Mai 2016: Interdisziplinarität

Festveranstaltung 20./21. Mai 2016:
Interdisziplinarität

Zur Authentizität und Integrität bei (digitalen) Beweismitteln*

Felix C. Freiling und Konstantin Sack

I. Einführung

Digital-forensische Auswertungen können heutzutage als Standard bei Ermittlungen von Strafverfolgungsbehörden angesehen werden. Dies trifft für weitgehend alle Straftatengruppen der Polizeilichen Kriminalstatistik zu und beschränkt sich nicht mehr nur auf die Computerkriminalität im engeren Sinne, wie beispielsweise Hacking. Analog zu physikalischen Beweismitteln, wie etwa einem blutigen Messer, werden in der Praxis zunehmend definierte spezielle Anforderungen an digitale Beweismittel gestellt, so dass diese im Strafprozess zugelassen und als Beweismittel gewürdigt werden können.

* Die Autoren danken Andreas Dewald und Sebastian Seyfarth für hilfreiche Kommentare zu früheren Versionen dieses Textes.

Das Hauptaugenmerk liegt hierbei auf der sog. *Verwahrungskette* (*chain of custody*) und der damit verbundenen Wahrung der *Authentizität* und *Integrität* der Beweismittel. Beide Begriffe sind gängig für Beweismittel in der Praxis und wurden vor allem in der englischsprachigen Literatur entwickelt. Im deutschen Rechtssystem sind diese Begriffe wohl aufgrund der zentralen Stellung des Richters und seiner freien Beweiswürdigung noch unterentwickelt und werden oft undifferenziert oder gar synonym verwendet. Dies ist bedauerlich, denn ein tieferes Verständnis der Begriffe erhöht das Bewusstsein bei der Erhebung, Verarbeitung und Interpretation von Beweismitteln. Ein tieferes Verständnis ist vor allem dann gefordert, wenn Beweismittel zunehmend auf digitalen Spuren basieren. Die hierbei vorliegende Problematik beschreibt *Lynch* mit:

»This distrust of the immaterial world of digital information has forced us to closely and rigorously examine definitions of authenticity and integrity - definitions that we have historically been rather glib about – using the requirements for verifiable proofs as a benchmark. [...] It is much easier to devise abstract definitions than testable ones.«[1]

Laut Duden wird der Begriff *Authentizität* für Gegenstände, Menschen oder Handlungen synonym zu den Worten *Echtheit* und *Original* verwendet. Hingegen bezeichnet die *Integrität* von Gegenständen deren Unverändertheit bzw. deren Unversehrtheit. Bezogen auf Menschen bedeutet Integrität, dass die Person glaubwürdig, vertrauenswürdig und unbestechlich ist. In verschiedenen Fachwissenschaften, auch der Informatik, haben sich spezielle Verständnisse der Begriffe entwickelt. Bei der Verwendung dieser Termini – insbesondere dem der *Authentizität* – vermischt sich das technologie-basierte Feld der IT mit den klassischen Konstrukten der Philosophie, Psychologie und Soziologie.

Im vorliegenden Beitrag werden wir uns mit der Frage beschäftigen, was Authentizität und Integrität für *digitale* Beweismittel bedeuten, wie diese Begriffe im Zusammenhang stehen und welche Unterschiede und Gemeinsamkeiten es gibt zu denselben Begriffen bei klassischen physischen Beweismitteln. Als Methode nutzen wir die Formalisierung und Modellierung zentraler Begriffe, um strukturelle Zusammenhänge zu identifizieren und zu analysieren. Wir entwickeln ein formales Modell, das die verschiedenen Phasen der Verwendung von (digitalen) Beweismitteln nachbildet und diese allgemein als eine fortgesetzte Transformation des Beweismittels darstellt. Das Modell erlaubt es uns schließlich, verständliche Definitionen für *Authentizität* und *Integrität* sowohl für physische wie auch für digitale Beweismittel abzuleiten und dadurch das Verständnis dieser Begriffe anhand des Modells zu schärfen. Am Ende dieses Beitrags werden schließlich die folgenden Fragen, die unterschiedliche Aspekte in Bezug

1 Lynch, C. A. (2000). Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust. In Council on Library and Information Resources, *Authenticity in a Digital Environment.*

auf *Authentizität* und *Integrität* von Beweismitteln problematisieren, konkret beantwortet:

- Wann ist ein Beweismittel authentisch?
- Wann ist ein Beweismittel integer?
- Wie authentisch sind digitale Beweismittel, beispielsweise ein exaktes Duplikat eines Datenträgers?
- Inwiefern beeinflussen Veränderungen an Beweismitteln ihre Authentizität und Integrität?

II. Begriffe aus der Literatur

1. Beweismittel und Spur

Der Begriff des Beweismittels als »Mittel zum Beweis« ist juristischer Natur. Dort sind Beweismittel definiert als »alle beweglichen und unbeweglichen Sachen, die unmittelbar oder mittelbar für die Tat oder die Umstände ihrer Begehung Beweise erbringen«[2]. Für Beweismittel ist es also notwendig, dass sie als Beweise in einem Gerichtsverfahren dienen können.

Der Begriff der *Spur* wird häufig im Kontext von Beweismitteln verwendet und teilweise auch synonym gebraucht. Spuren bilden jedoch nach allgemeiner Auffassung in der kriminalistischen Fachliteratur die »Vorstufe« von Beweismitteln. So schreiben etwa *Frings* und *Rabe*:

»Am Tatort einer Straftat werden oft eine Vielzahl von materiellen Veränderungen (= Spuren) festgestellt, wobei noch nicht klar ist, ob diese einen Bezug zu der zu untersuchenden Straftat haben.«[3]

Nach Frings und Rabe sind *Spuren* »sichtbare oder latente materielle Veränderungen, die im Zusammenhang mit einem kriminalistisch relevanten Ereignis entstanden sind und zu dessen Aufklärung beitragen können«[4]. Diese Auffassung von Spuren ist auch konform mit dem, was *Inman* und *Rudin*[5] auf Englisch als *evidence* bezeichnen.

2 Vgl. NRW. *Justizministerialblatt NRW 79, 226.*

3 Frings, C./Rabe, F. (2011). Grundlagen der Kriminaltechnik I. In H. C. Neidhardt, *Lehr- und Studienbriefe Kriminalistik/Kriminologie.* Verlag Deutsche Polizeiliteratur.

4 Siehe Fn. 3.

5 Vgl. Inman, K., & Rudin, N. (2002). The origin of evidence. *Forensic Science International* (126), S. 11–16.

2. Provenienz

Eine reichhaltige Quelle für Literatur, die sich mit dem Thema Authentizität oder Integrität beschäftigt, bietet der Bereich des Urkundenwesens (*diplomatics*), der seit dem 17. Jahrhundert Methoden entwickelt, um die Zuverlässigkeit und Authentizität schriftlicher Rechtsdokumente (Urkunden) einzuschätzen und zu beweisen.[6] Erste Verwendungen von *Authentizität* und *Integrität* finden sich beispielsweise bei *Thoennissen*[7]. Über die *Authentizität* schreibt er:

»Die inneren Gründe für die Authentizität einer alten Schrift können schlechthin nur aus der Form und dem Inhalte derselben hergenommen werden. Sie sind entweder negativer oder positiver Natur. Die ersteren sind zum Beweise der Echtheit einer Schrift durchaus erforderlich; […].«

Aufbauend hierauf folgen die Überlegungen zur *Integrität*:

»Wenn nun auch der erste Brief des Clemens von Rom als authentisch erwiesen ist; so wäre es doch noch immer möglich, daß Einzelnes darin absichtlich interpolirt oder verfälscht wäre.«[8]

Im Urkundenwesen werden die Begriffe der Authentizität und Integrität vor allem bei der Betrachtungen von Archivierungstechniken verwendet und stehen im Zusammenhang mit dem Begriff der *Provenienz* (*provenance*), der vom lateinischen *provenire* (herkommen) abstammt und allgemein die Herkunft oder den Ursprung einer Person oder Sache bezeichnet. Auch wenn der deutsche Begriff der Provenienz bereits etwas antiquiert erscheint, werden wir ihn im Folgenden als Allgemeinbegriff für alle Aspekte verwenden, die die Herkunft, Historie oder »Karriere« eines Objekts betreffen, um also das auszudrücken, was mit *provenance* bezeichnet wird. Aus diesem allgemeinen Begriff lassen sich aber nicht direkt spezielle Aspekte wie Authentizität und Integrität ableiten.

3. Authentizität

Ein guter Ausgangspunkt für unsere Betrachtungen zum Begriff der Authentizität ist die Definition von *Lynch*:

»Validating authenticity entails verifying claims that are associated with an object – in effect, verifying that an object is indeed what it claims to be, or what it is claimed to be (by external metadata).«[9]

In den englischsprachigen *Federal Rules of Evidence* findet sich juristisch verankert eine Definition, wie sie bereits von *Lynch* gegeben wurde:

6 Vgl. Duranti, L. (1998). Diplomatics: New Uses for an Old Science. *Scarecrow Press*.
7 Thoennissen, C. (1841). Zwei historisch-theologische Abhandlungen.
8 Siehe Fn. 7.
9 Siehe Fn. 1.

»*In General.* To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.«[10]

In der IT-Sicherheit finden sich für die Authentizität von Objekten verschiedene Definitionen. So schreibt etwa *Eckert*, man verstehe unter »Authentizität eines Objekts bzw. Subjekts (*authenticity*) [...] die Echtheit und Glaubwürdigkeit des Objektes bzw. Subjektes, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.«[11] In der Kryptographie gibt es ebenfalls verschiedene etablierte Definitionen von Authentizität, insbesondere für Systeme, die Nachrichten austauschen. Unter einer authentischen Nachricht wird dort verstanden, dass man ihre Quelle überprüfen kann. Authentifikation wird laut dem Standardwerk von *Menezes et al.* definiert als ein

»[...] service related to identification. This function applies to both entities and information itself. [...] Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc.«[12]

4. Integrität

Es gibt in der klassischen Forensik erstaunlich wenig Literatur zu einer Definition der Integrität. Hilfreich ist die Begriffsdefinition aus dem Bereich des Urkundenwesens von *Lynch*:

»When we say that a digital object has ›integrity‹, we mean that it has not been corrupted over time or in transit; in other words, that we have in hand the same set of sequences of bits that came into existence when the object was created.«[13]

Eine ähnliche Definition von Integrität findet sich bei *Casey*:

»The purpose of integrity checks is to show that evidence has not been altered from the time it was collected, thus supporting the authentication process.«[14]

In der Kryptographie wird wieder im Kontext von Systemen argumentiert, die Nachrichten austauschen. *Daten-Integrität* wird dort definiert als:

»[...] a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.«[15]

10 Vgl. Federal Evidence Review. *Federal Rules of Evidence* (2015).
11 Eckert, C. (2008). *IT-Sicherheit.* Oldenbourg Verlag.
12 Menezes, A./Vanstone, S./Van Oorschot, P. (1996). *Handbook of Applied Cryptography.* CRC Press, Inc.
13 Siehe Fn. 1.
14 Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press.
15 Siehe Fn. 12.

Auch wenn hier die Abgrenzung zwischen Beweismitteln, Daten und Informationen noch nicht erfolgt ist, so wollen wir doch eine interessante Beobachtung von *Menezes et al.* festhalten, die einen Zusammenhang zwischen Authentizität und Integrität in der Kryptographie beschreibt:

»Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).«[16]

III. Exkurs: Daten und Information

Daten sind physische Phänomene, die an sich keine direkte Bedeutung haben. Wenn ein Mensch die Daten wahrnimmt und interpretiert, entstehen Informationen. Dabei helfen ihm Interpretationsvereinbarungen. Dieselben Interpretationsvereinbarungen benötigt man, wenn man Informationen an eine materielle Form binden möchte. In einem solchen Fall repräsentiert man die Informationen in Form von Daten. Abbildung 1 stellt diesen Zusammenhang grafisch dar.

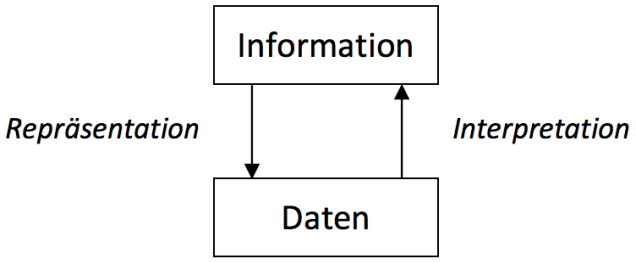


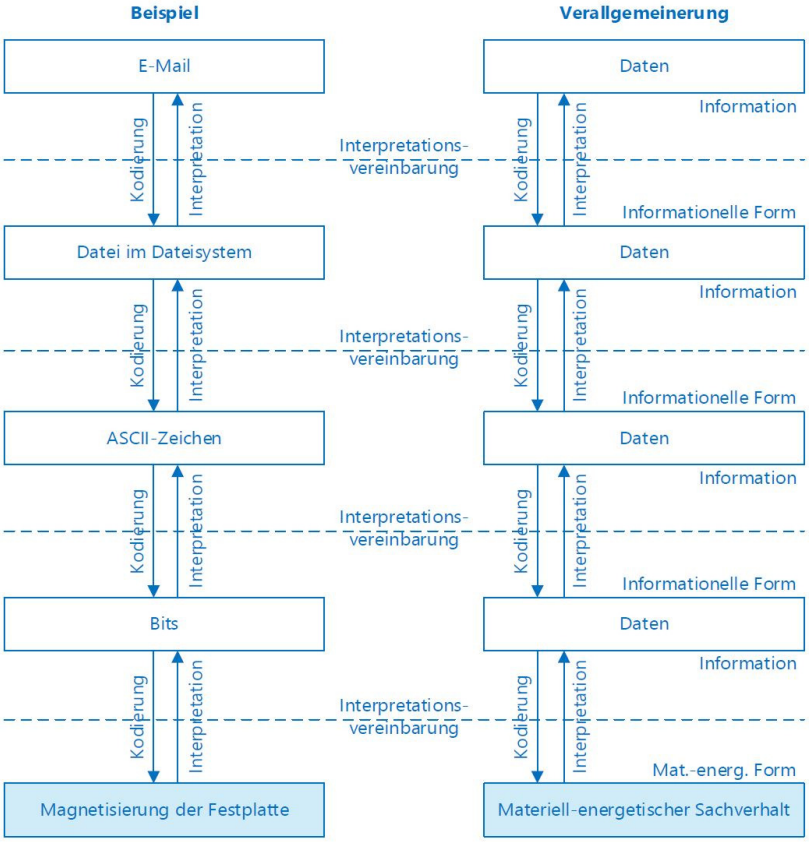
Abb. 1: Daten und Information

Wesentlich ist die Tatsache, dass Informationen immer nur im Kopf eines Menschen entstehen. Sie sind also immer subjektiv. Diese Subjektivität kann man natürlich durch klare und eindeutige Interpretationsvereinbarungen (Standardkodierungen) reduzieren, sie bleibt aber in einem minimalen Grad immer erhalten. Beispiele für solche Interpretationsvereinbarungen sind standardisierte Kodierungen wie z. B. ASCII.

Interpretationsvereinbarungen sind in Informatik-Systemen aufgrund ihres Aufbaus häufig hierarchisch geschichtet, so dass Kodierungen auf unteren Ebenen benutzt werden, um Kodierungen auf höheren Ebenen zu realisieren. Ein bekanntes Beispiel ist das ISO/OSI-Referenzmodell für Kommunikationssysteme, aber auch andernorts ist das Konzept anzutreffen. Abb. 2 zeigt auf der linken Seite, welche Abstraktionsschichten durchlaufen werden, wenn man eine

16 Siehe Fn. 12.

E-Mail-Datei auf einem Datenträger zusammensetzt. Auf der rechten Seite der Abbildung wird vom konkreten Beispiel abstrahiert: Auf Basis physischer Phänomene (ganz unten: Daten in materiell-energetischer Form) entstehen so auf immer höheren Ebenen immer komplexere Daten. Dort, wo ein Mensch die Daten »ausliest« und interpretiert, entstehen Informationen.



In Anlehnung an: *Dewald/Freiling* 2011, S. 36; *Tabeling* 2006, S. 15, Abb. 2.11.
Abbildung 2.1-1: Mehrstufige Interpretation

Abb. 2: Mehrstufige Interpretation (Siegert, 2016)[17]

17 Siegert, M. (2016). *Forensisches Reverse Engineering.* Masterarbeit. Hochschule Albstadt-Sigmaringen.

IV. Ein Modell für (digitale) Beweismittel

Je nach Rechtskontext können verschiedene Objekte Beweismittel werden. Wir betrachten zunächst Beweismittel, die im Rahmen einer Sicherstellung oder Beschlagnahme aufgenommen werden, weil sie einen potentiellen Bezug zum untersuchten Fall aufweisen. Man erhofft sich durch die Untersuchung des Objekts Hinweise, die für die Aufklärung des Falls relevant sind.

Werden am Tatort Spuren gesichert, werden die gesicherten Objekte in Beweismitteltüten aufbewahrt. Abb. 3 zeigt eine sichergestellte Festplatte mit entsprechendem deutschen Sicherstellungs-/Asservatenaufkleber. Auf diesen werden wichtige Fallinformationen notiert, die eine spätere Zuordnung und Identifizierung des Beweismittels erlauben.

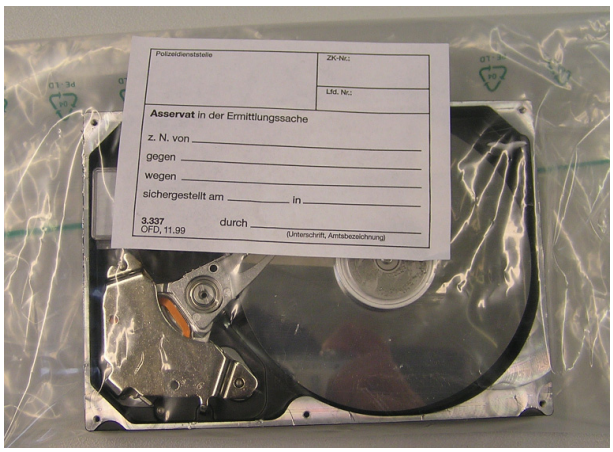


Abb. 3: Festplatte in Beweismitteltüte

Mit Abb. 3 vor Augen definieren wir das Modell eines Beweismittels wie folgt: Ein Beweismittel besteht aus drei Teilen:

1. dem physischen Objekt, das sich *in* der Tüte befindet,
2. der Aufschrift *auf* der Tüte und
3. der Bedeutung des Objekts für den Fall, also das, was man aus dem Objekt für den Fall lernen kann.

Wir präzisieren dies zu einer Definition, deren Teile wir im Folgenden ausführen.

Definition 1 (Beweismittel): Ein Beweismittel besteht aus drei Teilen:

1. einer Behauptung (claim),

2. einem Spurenträger (support) und
3. der eigentlichen Spureninformation (information).

Unter Verwendung der Anfangsbuchstaben der englischen Begriffe entsteht die Abkürzung »CSI«, die als Eselsbrücke für die Bestandteile des Modells verwendet werden kann. Im Folgenden erläutern wir die drei Bestandteile und deren Zusammenhänge etwas genauer.

1. Behauptung (claim)

Die *Behauptung* (*claim*) ist eine Beschreibung dessen, was das Beweismittel zu sein vorgibt. Man kann sich die Behauptung als einen Freitexteintrag vorstellen, der relevante Informationen zum Beweismittel enthält, etwa eine Asservatennummer, den Auffindeort und die Auffindezeit. Hierbei erstreckt sich die Behauptung grundsätzlich auf die Kombination von Spurenträger und Spureninformation. In einem gewissen Sinn spricht man bei der Behauptung auch von den *Metadaten* des Beweismittels.

Beispiel 1 (Behauptung bei einem physischen Beweismittel): Für ein Messer, auf dem sich ein blutiger Fingerabdruck befindet, könnte der *claim* wie folgt lauten: »Das am Tatort (genauer: im Wohnzimmer links neben dem Opfer) aufgefundene blutige Messer, das durch Kriminalkommissar Ehrlich am 3.12.2004 sichergestellt wurde.«

Ein Beweismittel und auch die dazugehörige Behauptung ist immer eingebettet in andere Beweismittel, die ebenfalls am Tatort aufgefunden wurden oder bei der Spurensicherung angefertigt werden, beispielsweise die Tatort-Fotografie oder -Videografie, Sicherungsberichte etc. Es gibt zahlreiche vorgegebene Handlungsalgorithmen, etwa in den deutschsprachigen Polizeidienstvorschriften (PDV) oder im englischsprachigen »Crime Scene Investigation: A Guide for Law Enforcement«[18] [19]. Für digitale Beweismittel gelten die Beobachtungen analog. Eine korrespondierende Handlungsanweisung liefert das U. S. Department of Justice im »Electronic Crime Scene Investigation: A Guide for First Responders«[20].

Beispiel 2 (Behauptung bei einem digitalen Beweismittel): Für eine am Tatort sichergestellte Festplatte könnte der *claim* lauten: »Festplatte Marke X mit Seriennummer Y, die am 25.05.2014 am Tatort von Kommissar Ehrlich sichergestellt wurde.«

18 Technical Working Group on Crime Scene Investigation. (2000). *Crime Scene Investigations: A Guide for Law Enforcement.* U.S. Department of Justice.

19 Vgl. Williams, J. (2012). *Good Practice Guide for Computer-Based Electronic Evidence.* Metropolitan Police Service.

20 Technical Working Group on Crime Scene Investigation. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders.* U.S. Department of Justice.

Im Fall digitaler Beweismittel wird durch die Dokumentation – oder im Optimalfall durch die zusätzliche Sicherung – möglichst eindeutiger Metadaten die Behauptung untermauert.

Beispiel 3 (Behauptung bei einem digitalen Beweismittel): Für ein digitales Beweismittel, z. B. eine Bild-Datei, könnte der *claim* wie folgt lauten: »Die Bild-Datei *kinderporno.jpg* mit dem Hashwert *XYZ*, die sich auf der Festplatte mit der Seriennummer 123 im Pfad C:\Users\Taeter\Bilder befunden hat.«

Wie wir später sehen werden, ist der claim ein wichtiger Faktor bei der Bestimmung der Integrität und Authentizität. *Lynch* schreibt hierzu:

»Typically, claims are linked to an object in such a way that they include, at least implicitly, a verification of integrity of the object about which claims are made.«[21]

2. *Spurenträger (support)*

Der *Spurenträger* (*support*) ist, grob gesprochen, das, was in der Beweismitteltüte »drin ist«. Dazu gehört sowohl die Materie als auch die Energie, die mit ihr zusammenhängt. Der Spurenträger ist also dasjenige, was die eigentliche Spur »speichert«. Der Begriff ist auch im Fachgebrauch verankert. So definiert das *BKA* Spurenträger als »Subjekte oder Objekte, an denen sich eine Spur befindet«[22]. Mit Subjekten meint das BKA Personen. Der Fachgebrauch unterscheidet jedoch zwischen Spur und Spurenträger. So schreibt *Bär*:

»[so sind] die Ermittlungsbehörden hier an sich nicht an dem Trägermedium in verkörperter Form interessiert, sondern an den unkörperlichen Daten, doch bildet beides eine technische Einheit. Vergleichbar dem Blutfleck an einem Mantel muss sich hier die Beweisbedeutung auch auf das eigentliche Trägermedium erstrecken.«[23]

Im Falle eines Fingerabdrucks auf einer Glasplatte wäre die Glasplatte der Spurenträger und der Fingerabdruck (auch wenn er aus besonders angeordneter Materie besteht) die Spur.

Im Gegensatz zur vorgenannten Definition enthält unsere Auffassung von Spurenträger die komplette Materie (also Trägermedium *und* Spur). Wir betrachten zudem die Materie mitsamt ihrer Energie; die Temperatur eines Gegenstands ist somit Teil des Spurenträgers. Das macht deutlich, dass sich der Spurenträger (zumindest theoretisch) permanent ändert. Wie wir später sehen werden, mag das für die Praxis nur in besonderen Situationen relevant sein (Temperaturen, Verwesung, entleerte Batterien), ist aber trotzdem Teil unseres Modells.

Wir führen die beiden Beispiele von oben weiter fort. In Beispiel 1 ist der Spurenträger das blutige Messer (also Messer mitsamt Blut). In Beispiel 2 ist der Spurenträger die Festplatte. In Beispiel 3 handelt es sich beim Spurenträger

21 Siehe Fn. 1.
22 BKA. *Anleitung Tatortarbeit - Spuren, Ziff. 1.0.1.* BKA.
23 Bär, W. (2007). *Handbuch der EDV-Beweissicherung.* Boorberg.

um den entsprechenden physischen Datenträger, auf dem sich das zu untersuchende Datenobjekt befindet.

3. Spureninformation (information)

Die *Spureninformation* (*information*) bildet die eigentliche Spur ab, die für die weitere Untersuchung relevant ist. Die Spureninformation ist vermutlich das abstrakteste Element unserer Definition eines Beweismittels, sie ist aber notwendig, um Beziehungen zwischen Beweismitteln zu beschreiben. Wir betrachten erneut die Beispiele von oben.

In Beispiel 1 wurde das blutige Messer vermutlich deshalb sichergestellt, weil es sich um ein Tötungsdelikt handelt. Man erhofft sich von dem Messer beispielsweise Aufschlüsse über den Tathergang oder auch den Täter. Die Spureninformation des Beweismittels könnte also beispielsweise sein:

- die Länge und Breite des Messers, um es mit den Einstichstellen des Opfers zu vergleichen,
- DNA-Informationen des anhaftenden Blutes, um es einer Person zuordnen zu können,
- die Zuordnung des Messers zu einer Person, die man aus einem ggf. vorhandenen Fingerabdruck ableiten kann, oder
- der Auffindeort des Messers.

Abstrakt gesehen könnte man die Spureninformationen eines physischen Objekts betrachten als die Menge aller Merkmale, die das Objekt hat. Im Sinne der Abgrenzung zwischen Daten und Informationen unter III. kann man hierbei von den auf dem Spurenträger »gespeicherten« Daten sprechen. Unter dem Begriff der Spureninformation sind aber keineswegs ausschließlich diese Daten zu verstehen. Gemeint ist vielmehr die Interpretation der Daten im Kopf eines Beobachters. Die Daten eignen sich jedoch gut als erste Approximation der Spureninformation.

Da es sicherlich viele Merkmale des Objekts (und somit viele Informationen) gibt, die gar keine Relevanz für das Tatgeschehen haben, wird durch die Definition der Spureninformationsbegriff überapproximiert. Problematisch ist jedoch, dass man – wie eingangs erwähnt – oft noch gar nicht weiß, welche Merkmale (und damit welche Informationen) für das Tatgeschehen relevant sind und welche nicht. Einige der Merkmale des Objekts sind sicherlich auch ausschließlich dazu geeignet, um die Korrektheit des claim zu prüfen. Dies sind den Spurenträger selbst beschreibende Informationen, die »charakteristischen Eigenschaften«[24] oder eine »physical manifestation«[25] des Objekts.

24 Siehe Fn. 11.

25 Smith, A. (2000). Authenticity in Perspective. In *Authenticity in a Digital Environment.* Council on Library and Information Resources.

Problematisch ist zudem, dass selbst die Menge der relevanten Merkmale unendlich groß sein kann, da ein (vor allem zeitlich) vollkommen uneingeschränkter Ermittler die vorgefundene Szene und damit einhergehend die entsprechenden Spurenträger theoretisch aus »potentiell unendlich vielen Perspektiven«[26] betrachten kann. Die Spureninformationen, auf die wir unsere Definition einschränken wollen, können somit lediglich einen Bruchteil der möglicherweise im Objekt vorhandenen Informationen abbilden. Wir differenzieren daher zwischen (allgemeinen) Spureninformationen und relevanten Spureninformationen. Analog dazu kann man die materielle Repräsentation dieser Spureninformationen auf dem Spurenträger als die (relevanten) Daten bezeichnen.

Es ist wichtig zu betonen, dass die Spureninformationen unabhängig vom Spurenträger existieren können. Das ist bei physischen Spuren schwer einzusehen, da die physische Materie oft implizit die Spureninformation enthält (wie etwa die DNA). Der Unterschied wird aber deutlicher, wenn man digitale Spuren betrachtet. Bei dem digitalen Beweismittel aus Beispiel 3 sind die auf dem Datenträger gespeicherten Bits mitsamt ihrer Interpretation als Bild die Spureninformation.

V. Phasen der forensischen Analyse

Ein Beweismittel, wie es oben in Definition 1 beschrieben wurde, durchläuft von seiner Sicherung am Tatort bis zur Präsentation vor Gericht verschiedene Phasen:

1. Die *Sicherungsphase* markiert den Anfang der Karriere eines Beweismittels. In dieser Phase entstehen Beweismittel gemäß Definition 1 »aus dem Nichts«. Es ist der Anfang der Provenienz des Beweismittels, seiner Karriere.
2. In der *Präsentationsphase* erfolgt die Vorlage eines Beweismittels gemäß Definition 1 vor Gericht in der Hoffnung, dass die relevanten Informationen, die es enthält, bei der Beantwortung der diskutierten Rechtsfragen hilfreich sind. In dieser Phase verändert sich ein Beweismittel nicht mehr weiter. Es ist das Ende der Karriere des Beweismittels.
3. In der *Analysephase* erfolgt die Verarbeitung und Veredelung des Beweismittels im Labor. Es wird auf relevante Informationen abgeklopft und kann in Zusammenhang gebracht werden mit anderen Beweismitteln. Daraus entstehen neue Beweismittel nach Definition 1. In dieser Phase wird das Beweismittel so lange transformiert, bis es »reif« für die Präsentationsphase ist.

26 Böhme, R./Freiling, F./Gloe, T./Kirchner, M. (2009). Multimedia Forensics is not Computer Forensics. *Third International Workshop on Computational Forensics*, (S. 90–103).

Wir werden im Folgenden diese drei Phasen nacheinander behandeln und in unser Modell einbeziehen. Über allen Phasen dieser Provenienz steht die Verwahrungskette (*chain of custody*), die lückenlos dokumentiert, wie sich das Beweismittel auf seinem Weg durch die Phasen entwickelt. Dazu zählen auch Angaben darüber, welche Personen zu welchen Zeitpunkten mit ihm befasst waren. Das Ziel der Verwahrungskette ist »accountability and appropriate handling and storage of the evidence«[27]. Die schriftliche Beschreibung der Verwahrungskette kann als Teil der Behauptung (*claim*) aus Definition 1 angesehen werden. In Abb. 4 werden vereinfacht die oben beschriebenen drei Phasen und die damit verbundenen Handlungsorte einer forensischen Analyse schematisch dargestellt.

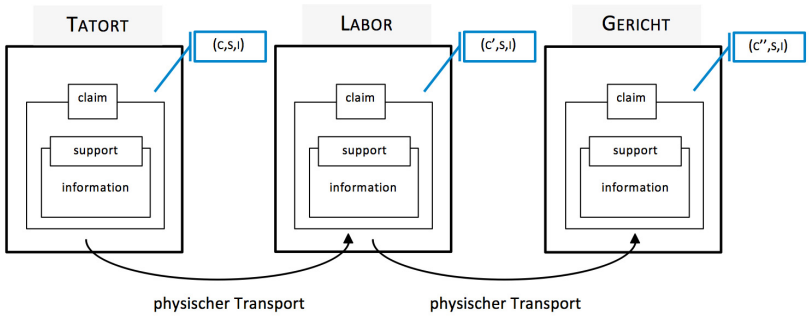


Abb. 4: Phasen und Handlungsorte der forensischen Analyse

1. Sicherungsphase

Am Tatort werden potentielle Beweismittel gesichert, in Beweismitteltüten verpackt und beschriftet. Hierdurch ist ein Beweismittel gemäß Definition 1 entstanden. Vom Tatort wird das Beweismittel dann gewöhnlich ins Labor und später von dort vor Gericht transportiert. Wir werden jedoch sehen, dass sich das Beweismittel im Verlauf seiner Karriere ständig verändert. Mit der Terminologie unseres Modells kann differenziert über diesen Verlauf gesprochen und die Provenienz eines Beweismittels von der Sicherung bis vor Gericht nachgezeichnet werden.

27 SANS Institute. *SANS – SCORE: Law Enforcement FAQ*. Abgerufen am 29.07.2016 von SANS – SCORE: Law Enforcement FAQ: https://www.sans.org/score/law-enforcement-faq/chainofcustody.php.

2. Präsentationsphase

Die Präsentationsphase findet verkürzt gesprochen »vor Gericht« statt. Gericht steht hierbei als Sammelbegriff für den Ort, an dem das Beweismittel wirksam und nicht mehr weiter bearbeitet wird. Dies kann durch die Präsentation des Beweismittels durch einen Sachverständigen im Gerichtssaal erfolgen oder durch die Übergabe von Bericht und Beweismitteln (im polizeilichen Umfeld) an die Staatsanwaltschaft.

In unserem Modell beschreibt die Präsentationsphase das Ende der Karriere des Beweismittels, den Schlusspunkt seiner Provenienz. Spätestens hier muss die Menge der relevanten Informationen klar bestimmt sein.

3. Analysephase

Die Analysephase erfolgt, grob gesprochen, im Labor. Das Labor ist der Ort, an dem Analysen und Untersuchungen (physikalisch wie digital) an den Beweismitteln durchgeführt werden. In bestimmten Fällen können Untersuchungen bereits am Tatort erfolgen. Im Bereich der IT-Forensik unterscheidet man etwa zwischen einer Untersuchung vor Ort (Live-Analyse) und der Sicherung der Spuren zur späteren kriminaltechnischen Analyse im Labor (Post-mortem-Analyse).

Im Rahmen der kriminaltechnischen Untersuchung werden die in der Sicherungsphase gesicherten Spuren durch Experten, in der Regel durch Wissenschaftler wie z. B. Biologen, Chemiker oder Informatiker, unter entsprechenden Bedingungen, die die Spur selbst so gering wie möglich beeinflussen, analysiert. Biologen oder Chemiker arbeiten in klassischen Laboren, während bei den Experten der IT-Forensik der eigene Arbeitsplatz mithilfe technischer Geräte zum Labor wird. Wichtigste Hilfsmittel für den IT-Forensiker sind Schreibschutz-Geräte, die dafür sorgen sollen, dass Datenträger nicht unbemerkt verändert werden.

Während der Karriere eines Beweismittels können sich claim, support und information eines Beweismittels ändern. Grob gesprochen, durchläuft jedes Beweismittel bei jeder Form der Analyse eine solche Transformation, beispielsweise wenn von einer Flüssigkeit ein Abstrich gemacht wird oder wenn von einer Faser ein Teil abgetrennt und chemisch analysiert wird. Wie oben erwähnt, verändert sich das Beweismittel aber auch von selbst, wenn es sich beispielsweise abkühlt (und damit Energie verliert). Es folgen später noch Beispiele solcher Veränderungen.

In unserem Modell abstrahieren wir von den Zwischenschritten und modellieren alle Veränderungen eines Beweismittels als einen unteilbaren (atomaren) Zustandsübergang. Zur abstrakten Darstellung der Analysephase verwenden wir das Konzept des Graphen aus der Informatik[28]. Wir modellieren die Analysephase als Beweismittelgraph wie folgt.

28 Vgl. Diestel, R. (2000). *Graphentheorie.* Springer-Verlag.

Definition 2 (Beweismittelgraph): Sei $\boldsymbol{B}$ die Menge aller möglichen durch Definition 1 beschreibbaren Beweismittel. Ein Beweismittelgraph über $\boldsymbol{B}$ ist ein gerichteter azyklischer Graph $\boldsymbol{G} = (\boldsymbol{B}, \boldsymbol{E})$ bestehend aus $\boldsymbol{B}$ als der Menge von Knoten und der Menge $\boldsymbol{E} \subseteq \boldsymbol{B} \times \boldsymbol{B}$ von Kanten.

Die Kanten beschreiben die Zustandsübergänge zwischen den Beweismitteln. Bildlich darstellen lassen sich die Knoten durch Punkte sowie die Kanten durch Pfeile zwischen diesen Punkten. Knoten können deshalb eingehende und ausgehende Kanten haben. Der Graph ist azyklisch, d. h. es gibt keine zyklische Verbindung von Knoten durch Kanten. Das bedeutet aber auch, es existieren Knoten, die keine eingehende Kante haben, sowie Knoten, die keine ausgehende Kante haben. Erstere entstehen im Rahmen der Sicherungsphase, letztere entstehen mit dem Ziel, sie im Rahmen der Präsentationsphase zu verwenden.

Die Zustandsübergänge im Beweismittelgraph stellen im Prinzip beliebige Transformationen von einem Beweismittel ins andere dar. Allerdings ist es sinnvoll, nur bestimmte Arten von Zustandsübergängen zu fordern. Intuitiv sollen nur solche Zustandsübergänge erlaubt sein, die für die Untersuchung zielführend sind. Das wird dadurch formalisiert, dass man beim Übergang keine relevanten Daten (und damit keine relevanten Informationen) verliert. Dies ist in der Praxis aus zwei Gründen schwierig zu erreichen:

1. Wie bereits erwähnt, weiß man während einer Untersuchung oft noch nicht, welche Daten für den Fall relevant sind. Man konzentriert sich dann auf bestimmte Daten und verliert dabei andere, die sich später als relevant herausstellen.
2. Auch Nichtstun kann dazu führen, dass relevante Daten verloren gehen. Wenn beispielsweise die Temperatur eines Gegenstands relevant ist, dann muss man dieses Merkmal etwa durch schriftliche Dokumentation sichern. In unserem Modell würde man also ein neues Beweismittel erzeugen, das die relevanten Daten erhält.

Beobachtung 1 (Fortschreibung des *claim*): Ein *claim* für ein Beweismittel sollte genauen Aufschluss über die Provenienz des Beweismittels geben. Er sollte also Hinweise auf die wesentlichen vorhergehenden Veränderungen (u. a. Analyseschritte) enthalten. Dies kann als Inklusionsbeziehung modelliert werden, d. h. für die Sequenz von Behauptungen eines Beweismittels $\boldsymbol{c_1, c_2, c_2 \ldots, c_n}$ in einem Pfad sollte gelten:

$$\boldsymbol{c_1 \subset c_2 \subset c_2 \subset \cdots \subset c_n}$$

Beispiel 4 (Entwicklung der Behauptung): Betrachten wir die Behauptung aus Beispiel 1 »Das am Tatort (genauer: im Wohnzimmer links neben dem Opfer) aufgefundene blutige Messer, das durch Kriminalkommissar Ehrlich am 03.12.2004 sichergestellt wurde.« Wenn nun ein Abstrich des Blutes mit einem Wattestäbchen genommen wird, dann entwickelt sich die Behauptung wie folgt weiter: »Wattestäbchen mit Abstrich der Flüssigkeit vom am Tatort (genauer:

im Wohnzimmer links neben dem Opfer) aufgefundenen blutigen Messer, das durch Kriminalkommissar Ehrlich am 03.12.2004 sichergestellt wurde.«

4. Transformation von Information

Es wird deutlich, dass sich bei analogen sowie bei digitalen Beweismitteln über die Phasen der forensischen Analyse der *Spurenträger* ändern kann. Die Interpretation von in materiell-energetischen Daten enthaltenen Informationen wurde bereits betrachtet. Können Informationen aus digitalen Daten nicht direkt durch Dekodierung innerhalb eines informationstechnischen Systems in menschenlesbare Form gebracht werden, so wie es z. B. bei Bild-, Video- oder Textdokumenten möglich ist, so dass diese in »Papierform« vor Gericht gesichtet werden können, erfolgt eine schriftliche Dokumentation des informationellen Inhalts in einem sog. Gutachten (Untersuchungsbericht). Analog ist die Vorgehensweise bei physikalischen Beweismitteln, falls diese nicht als Beweismittel für sich selbst sprechen (z. B. ein Messer, welches als solches als Beweismittel vor Gericht gezeigt wird). Gemeint sind hierbei verallgemeinert Spuren, deren Information zunächst gewonnen werden muss: Beispiele hierfür sind Fingerabdruckspuren, Blutspuren zur DNA-Analyse etc.

VI. Authentizität und Integrität

Wir kommen nun zurück auf die Begriffe, auf die wir es eigentlich abgesehen haben: Authentizität und Integrität von Beweismitteln. Wir betrachten zunächst den oft impliziten Zusammenhang zwischen Spurenträger und Spureninformation. Anschließend entwickeln wir aus der Literatur und auf Basis unseres Modells Definitionen von Authentizität und Integrität.

1. Bindung von Spurenträger und Spureninformation

In vorhergehenden Abschnitt wurde deutlich, dass bei analogen Beweismitteln eine Gewinnung von Informationen aus einem Spurenträger in der Regel nicht ohne die Manipulation des *support* möglich ist. Bei analogen Beweismitteln existiert also eine enge Beziehung zwischen Spurenträger und Spureninformation, da der *support* in natürlicher Weise Träger der Merkmale ist, aus denen die *information* entsteht. Bei digitalen Beweismitteln ist das nicht notwendigerweise der Fall, wenn man als Merkmale ausschließlich die auf dem Datenträger gespeicherten Bits betrachtet. Vergleichbar ist dies allenfalls mit Dokumenten, bei denen es ausschließlich auf den Inhalt des fixierten Textes ankommt, also etwa Gutachten oder Geschäftskorrespondenz in Wirtschaftsstrafverfahren. Aber

auch dort kommt es manchmal auf zusätzliche Merkmale des Spurenträgers an, etwa die Verfärbung des Papiers, handschriftliche Notizen oder DNA-Spuren.

Trotz der relativ schwachen Bindung von *support* und *information* bei digitalen Beweismitteln betrachtet die Literatur häufig noch »das Trägermedium und die unkörperlichen Daten als eine technische Einheit«[29]. Problematisch für diese beschriebene Einheit ist jedoch, dass es bei digitalen Beweismitteln im Gegensatz zu analogen Beweismitteln leichter möglich ist, bestimmte Merkmale (nämlich die digitalen Daten) exakt auf einen anderen Spurenträger zu übertragen. Hierbei entstehen die aus der Praxis bekannten Bit-für-Bit-Kopien (forensische Duplikate, images). Durch die Verwendung besonderer Schreibschutz-Techniken ist es zudem möglich, diese Merkmale auszulesen, ohne den Träger oder die darauf vorhandenen Merkmale zu verändern. *Bär* beschreibt dies wie folgt:

»Im Gegensatz zu den herkömmlichen Printmedien kann bei Computerdaten von einem Original und einer Kopie nicht gesprochen werden. Da die Dateien beim Kopiervorgang dupliziert werden, entstehen völlig identische Datensätze. Die dabei verwendeten Speichermedien – besser als Quelldatenträger und Kopie zu bezeichnen – unterscheiden sich nur hinsichtlich äußerer Kriterien.«[30]

Festzuhalten bleibt: Im Falle digitaler Beweismittel können bestimmte Merkmale des Spurenträgers, nämlich die gemäß den bekannten Kodierungsvorschriften darauf gespeicherten digitalen Daten, perfekt auf einen anderen Spurenträger kopiert werden. Der ursprüngliche Spurenträger bleibt jedoch das Original, denn seine »äußeren Kriterien« sind unterschiedlich. Perfekt ist die Kopie lediglich bezüglich einer Teilmenge von Merkmalen. Diese Teilmenge kann jedoch präzise umrissen werden und ist ohne Unschärfe auslesbar. Dies ist die neue Qualität digitaler Beweismittel.

2. Definition

Wir betrachten einen Pfad $(\boldsymbol{c_1}, \boldsymbol{s_1}, \boldsymbol{i_1}) \mapsto (\boldsymbol{c_2}, \boldsymbol{s_2}, \boldsymbol{i_2}) \mapsto \cdots \mapsto (\boldsymbol{c_n}, \boldsymbol{s_n}, \boldsymbol{i_n})$ eines Beweismittels durch den Beweismittelgraph. Beweismittel $(\boldsymbol{c_1}, \boldsymbol{s_1}, \boldsymbol{i_1})$ kann man sich beispielsweise vorstellen als das Beweismittel direkt nach der Sicherung (Sicherungsphase) und $(\boldsymbol{c_n}, \boldsymbol{s_n}, \boldsymbol{i_n})$ als das Beweismittel vor Gericht (Präsentationsphase), aber es können auch beliebige Teilpfade aus dem Beweismittelgraph gemeint sein.

Beobachtung 2: Authentizität ist ein Begriff, den man im Wesentlichen auf den Spurenträger bezieht.

Authentizität des Beweismittels ist gegeben, wenn der Spurenträger im Verlauf des Beweismittelpfades gleich bleibt.

29 Siehe Fn. 23.
30 Siehe Fn. 23.

Definition 3 (Authentizität des Beweismittels): Das Beweismittel $(\boldsymbol{c_n}, \boldsymbol{s_n}, \boldsymbol{i_n})$ ist authentisch, falls der Spurenträger aus der Sicherung stammt, d. h. falls $\boldsymbol{s_n} = \boldsymbol{s_1}$ gilt.

Wir kommen nun zum Begriff der Integrität. Im Gegensatz zur Authentizität bezieht sich Integrität eher auf das, was das Beweismittel für das Verfahren bedeutet. Dies kann man über die Unverändertheit der relevanten Spureninformation genauer fassen.

Definition 4 (Integrität des Beweismittels): Das Beweismittel $(\boldsymbol{c_n}, \boldsymbol{s_n}, \boldsymbol{i_n})$ ist integer, falls die relevanten Spureninformationen aus der Sicherung erhalten geblieben sind.

Bleibt der Spurenträger über den Pfad des Beweismittels erhalten, so bleiben natürlich auch die relevanten Merkmale und somit die Spureninformationen erhalten.

Beobachtung 3: Wenn ein Beweismittel authentisch ist, dann ist es auch integer.

Diese Beobachtung erklärt, warum es bei physischen Beweismitteln nicht notwendig ist, zwischen Authentizität und Integrität zu unterscheiden, bei digitalen Beweismitteln hingegen schon.

Eine wichtige Rolle spielt in diesem Zusammenhang die Behauptung (*claim*).

Beispiel 5: An einem Tatort werden in einem PKW jeweils auf dem Fahrersitz und auf dem Rücksitz ein blutiger Handschuh aufgefunden. Der *claim* des Beweismittels lautet: »blutiger Handschuh vom Fahrersitz«; im Laufe der Karriere des Beweismittels stellt sich allerdings heraus, dass es sich um den blutigen Handschuh vom Rücksitz handelt.

Da Authentizität und Integrität auf Basis des Beweismittelpfades definiert sind, kommt der Behauptung, also der Beschreibung der Provenienz des Beweismittels, eine zentrale Bedeutung zu. Erst mittels der Behauptung kann eine Beziehung zwischen dem Beweismittel in der Präsentationsphase und dem Beweismittel aus der Sicherungsphase hergestellt werden. Sind die Angaben in der Behauptung fehlerhaft, so gibt es keine sinnvolle Definition von Authentizität und Integrität mehr.

Beobachtung 4: Authentizität und Integrität eines Beweismittels basieren auf der Annahme, dass der *claim* wahrhaftig ist, also keine fehlerhaften oder irreführenden Angaben enthält.

Diese Beobachtung wird gestützt durch *Lynch*:

»We examine the provenance of the object (for example, the documentation of the chain of custody) and the extent to which we trust and believe this documentation as well as the extent to which we trust the custodians themselves.«[31]

Beispiel 6: In den Jahren von 2007 und 2009 geisterte das »Heilbronner Phantom« durch die Medienlandschaft. Bei einer großen Menge von Straftaten wurde in DNA-Proben von Tatort immer wieder DNA einer weiblichen Person ge-

31 Siehe Fn. 1.

funden. Bei Untersuchungen wurde jedoch festgestellt, dass die für die Spurensicherung verwendeten Wattestäbchen durch DNA einer Mitarbeiterin in der Fabrik, die die Wattestäbchen herstellte, verunreinigt waren. In diesem Fall war der *claim* nicht wahrhaftig, denn er implizierte die Annahme, dass keine fremde DNA durch die Verwendung der Wattestäbchen in die Probe gelangte.

VII. Zusammenfassung

Dieser Artikel stellt zunächst ein Modell für Beweismittel vor, auf dessen Basis dann die Begriffe *Authentizität* und *Integrität* von Beweismitteln definiert werden können. Ein Beweismittel ist demnach die Kombination aus einer Behauptung (*claim*), dem Spurenträger (*support*) und der Spureninformation (*information*). Im Bereich der analogen/physikalischen Welt besteht ein enger Zusammenhang zwischen *support* und der enthaltenen *information*. Dies steht im Gegensatz zu digitalen Beweismitteln, bei denen bestimmte Merkmalsmengen nahezu beliebig zwischen Spurenträgern ausgetauscht werden können.

Herausgeber und Autoren

Beyerer, Jürgen, Prof. Dr.-Ing. habil., Karlsruher Institut für Technologie (Universität Karlsruhe), geschäftsführender Leiter des Fraunhofer-Instituts für Optronik, Systemtechnik und Bildauswertung (IOSB), Karlsruhe, Ettlingen, Ilmenau, Lemgo und Görlitz

Bliesener, Thomas, Prof. Dr. phil., Direktor des Kriminologischen Forschungsinstituts Niedersachsen e.V., Hannover

Brüggemann, Gert-Peter, Prof. Dr. phil., Deutsche Sporthochschule Köln, Institut für Biomechanik und Orthopädie, Köln

Caspers, Georg, Prof. Dr. iur., Friedrich-Alexander-Universität Erlangen-Nürnberg, Prodekan, Lehrstuhl für Bürgerliches Recht und Arbeitsrecht

Dietz, Florian, Dr. iur., Notar, Bamberg

Freiling, Felix, Prof. Dr.-Ing., Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Informatik 1

Geis, Max-Emanuel, Prof. Dr. iur., Prodekan, Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Deutsches und Bayerisches Staats- und Verwaltungsrecht

Grundmann, *Stefan*, Prof. Dr. iur. Dr. phil., Humboldt-Universität zu Berlin, Lehrstuhl für Bürgerliches Recht, Deutsches, Europäisches und Internationales Wirtschaftsrecht (beurlaubt), Europäisches Hochschulinstitut, Florenz

Hager, Johannes, Prof. Dr. iur., Ludwig-Maximilian-Universität München, Lehrstuhl für Bürgerliches Recht, deutsches, internationales und vergleichendes Zivilverfahrensrecht

Heuberger, Albert, Prof. Dr. Ing., Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Informationstechnik, Leiter des Fraunhofer-Instituts für Integrierte Schaltungen (IIS), Erlangen

Hübner, Horst, Prof. Dr. phil., Bergische Universität Wuppertal, Arbeitsbereich Sportsoziologie, Wuppertal

Koch, Hans-Georg, Privatdozent, Dr. iur., Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg

Kötter, Rudolf, Ltd. Akad. Dir. i. R., Friedrich-Alexander-Universität Erlangen-Nürnberg, Zentralinstitut für Angewandte Ethik und Wissenschaftskommunikation

Lenk, *Hans,* Prof. Dr. phil. Dr. h.c. mult., Karlsruher Institut für Technologie (Universität Karlsruhe), Ehrenpräsident des Institut international de Philosophie, Paris

Lorz, Sigrid, Privatdozentin, Dr. iur., Friedrich-Alexander-Universität Erlangen-Nürnberg, Institut für Recht und Technik

Martinek, Michael, Prof. Dr. iur. Dr. rer. publ. Dr. h.c. mult., M.C.J. (NYU), Universität des Saarlandes, Hon.-Prof. (Johannesburg), Hon.-Prof. (Wuhan)

Paul, Christian, Dr. iur, Dipl.-Chem., Rechtsanwalt, München

Petri, Grischka, Privatdozent, Dr. iur., Dr. phil., Rheinische Friedrich-Wilhelms-Universität Bonn, Kunsthistorisches Institut

Regenfus, *Thomas*, Privatdozent, Dr. iur., Richter am Landgericht, Nürnberg-Fürth

Reinfelder, *Waldemar*, Richter am Bundesarbeitsgericht, Erfurt

Renn, Ortwin, Prof. Dr. rer. pol. Dr. h.c., wissenschaftlicher Direktor am Institut für Transformative Nachhaltigkeitsforschung (IASS), Potsdam und Präsidiumsmitglied der Deutschen Akademie der Technikwissenschaften (acatec)

Röthel, *Anne,* Prof. Dr. iur., Bucerius Law School, Hamburg, Lehrstuhl für Bürgerliches Recht, Europäisches und Internationales Privatrecht

Sack, Konstantin, wiss. Mitarbeiter, Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Informatik 1, und Polizeipräsidium Südhessen, Darmstadt

Salje, *Peter*, Prof. Dr. iur. Dr. rer. pol., Leibniz-Universität Hannover

Schneider (nach Eheschließung: *Settgast), Christine,* Dipl.-Ing., wiss. Mitarbeiterin, Friedrich-Alexander-Universität Erlangen-Nürnberg, Institut für Recht und Technik

Schnieder, Eckehard, Prof. a.D. Dr.-Ing. Dr. h.c. mult., TU Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik

Schrenk, Christoph, Dr. iur., Lehrbeauftragter an der Friedrich-Alexander-Universität Erlangen-Nürnberg, Notar, Nürnberg

Thies, Bernhard, Dr. Ing., Geschäftsführer DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Präsident CENELEC European Committee for Electrotechnical Standardization

Vieweg, Klaus, Prof. Dr. phil., Friedrich-Schiller-Universität Jena, Institut für Philosophie

Vieweg, *Klaus,* Prof. Dr. iur., Friedrich-Alexander-Universität Erlangen-Nürnberg, Institut für Recht und Technik, Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, Technik- und Wirtschaftsrecht

Werner, Almuth, Dr. iur., Rechtsanwältin, Leipzig

Zech, Herbert, Prof. Dr. iur., Dipl-Biol., Professor für Life Sciences-Recht und Immaterialgüterrecht, Juristische Fakultät der Universität Basel