ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

04

BAND

Quellen, Widersprüche und alternative Hypothesen

Spanische Ausgabe · 2026

Handbuch zur technischen Verteidigung gegen Anschuldigungen auf der Grundlage digitaler Beweise

Überprüfung von Bildschirmfotos, Gesprächen, Dateien, Standortdaten, Berichten und forensischer Argumentation

Eine Anschuldigung prüfen, ohne ihre Abkürzungen zu akzeptieren oder eine andere bequeme Version zu erzeugen: das Objekt lokalisieren, die Methode überprüfen und abgrenzen, was tatsächlich behauptet werden kann.

Für beschuldigte Personen, Verteidiger, Sachverständige beider Seiten, unabhängige Prüfer und Teams, die überprüfbare technische Fragen formulieren müssen. Enthält keine Verfahrensstrategien und ersetzt nicht die juristische Analyse der Akte.

Redaktionelle Koordination: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

Allgemeine technische Anleitung und offenes Bildungsmaterial. Diese Unterlagen ersetzen keine Rechtsberatung oder forensische Begutachtung und enthalten keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Verzeichnis beim Öffnen des Dokuments aktualisieren; die interne Navigation der Überschriften bleibt erhalten.

Einleitung: Ein scharfes Bild kann eine unvollständige Geschichte erzählen 4
Kapitel 1. Die Behauptung vor der Datei 4
1.1 Die Anschuldigung zerlegen 4
1.2 Akte und Abdeckung 5
Kapitel 2. Überprüfung von Entgegennahme und Verwahrung 6
2.1 Identität des Objekts vor dem Inhalt 6
2.2 Fehlende Übertragungen im Verlauf 6
2.3 Befugnis und Verhältnismäßigkeit 6
Kapitel 3. Matrix der Widersprüche 7
3.1 Erkennen, ohne nur das zu wählen, was nützt 7
3.2 Arten von Widersprüchen und ihre Wirkung 7
Kapitel 4. Bildschirmfotos, Gespräche und Dateien 8
4.1 Das Bildschirmfoto als Fragment 8
4.2 Export und Kontext von Nachrichten 8
4.3 Metadaten und Versionen 9
Kapitel 5. Argumentation und unabhängige Überprüfung 9
5.1 Prämissen und falsche Konsequenz 9
5.2 Alternative Hypothesen und Falsifikationstest 10
5.3 Überprüfung, die den Bericht zu widerlegen versucht 10
Kapitel 6. Überprüfung des forensischen Berichts 11
6.1 Nachverfolgbarkeit jeder Schlussfolgerung 11
6.2 Nützliche Fragen zur Widerlegung 12
Kapitel 7. Integrierter Fall: von der Anschuldigung zur begrenzten Schlussfolgerung 12
7.1 Verfügbares Material 12
7.2 Überprüfungen und Befunde 12
7.3 Kurzer Ergebnisbericht 12
Anhang A. Überprüfungsformat und Fragen 13
A.1 Matrix der Behauptungen 13
A.2 Liste technischer Fragen 13
A.3 Register angeforderter und empfangener Quellen 13
Anhang B. Juristische Funktionen für die Überprüfung 14

Einleitung: Ein scharfes Bild kann eine unvollständige Geschichte erzählen

Ein Bildschirmfoto kann schlüssig erscheinen, weil es einen Namen, einen Satz und eine Uhrzeit enthält. Ein Video kann ausreichend erscheinen, weil es ein bekanntes Gesicht zeigt. Eine Antenne kann wie eine Adresse wirken, wenn sie als Punkt auf einer Karte dargestellt wird. Die technische Verteidigung beginnt damit, diese automatische Übersetzung zu stoppen: Was genau ist das Objekt, wer hat es erzeugt, welchen Teil der Geschichte bewahrt es, welche Methode wurde angewendet und welche anderen Erklärungen bleiben vereinbar?

Widersprechen bedeutet nicht, alles zu leugnen. Stimmt der Hashwert überein, wird diese Übereinstimmung anerkannt; ist eine Quelle zuverlässig, wird ihr Geltungsbereich erläutert; ist eine Schlussfolgerung richtig, wird sie nicht aus Prinzip bekämpft. Die Arbeit trennt das Bewiesene von dem Abgeleiteten. Manchmal bleibt die Anklage bestehen. In anderen Fällen genügen eine falsche Identifizierung, ein Datum ohne Zeitzone oder ein unvollständiger Export, um zu zeigen, dass die Argumentation in ihrer vorliegenden Form nicht trägt.

Die beschuldigte Person muss keine alternative Geschichte erfinden, um die Schwäche der ersten zu zeigen. Der Prüfer kann feststellen, dass die Quelle die Behauptung nicht belegt, dass die Abdeckung andere Erklärungen nicht ausschließt oder dass die Methode keine Identifizierung einer Person ermöglicht. Diese Präzision verhindert, dass aus der Verteidigung eine zweite unbelegte Anschuldigung wird.

> **Leitfrage**
> Welche Behauptung entfällt, wenn eine ungeprüfte Prämisse zurückgezogen wird? Diese Frage leitet die Überprüfung jedes Bildschirmfotos, Berichts, Datensatzes und jeder Schlussfolgerung.

Kapitel 1. Die Behauptung vor der Datei

1.1 Die Anschuldigung zerlegen

Die vollständige Behauptung wird ohne Adjektive formuliert: eine Person, eine Handlung, ein Objekt, ein Datum, ein Ort und eine Folge. Anschließend werden ihre Bestandteile getrennt. „Der Beschuldigte hat die Nachricht um 21:00 Uhr von zu Hause gesendet“ enthält mindestens vier Fragen: Existiert die Nachricht, wurde das Konto zugeordnet, befand sich das Gerät an einem Ort und hat die Person es zu diesem Zeitpunkt verwendet? Ein einzelnes Bildschirmfoto kann keine dieser Fragen vollständig beantworten.

Die Versionen werden getrennt dokumentiert, ohne sie zu Tatsachen zu erklären. Die Anklage behauptet eine Abfolge; die Verteidigung kann sie bestreiten, teilweise anerkennen oder nicht kennen. Ziel ist nicht, sie zu einer Zwischenversion zu vermischen, sondern zu bestimmen, welche Quellen jedes Element bestätigen oder schwächen können. Das erste Arbeitsdokument ist eine Übersicht der Behauptungen und der benötigten Quellen.

Komponente	Überprüfungsfrage	Quelle, die unterscheiden kann
Vorhandensein	Liegt die Nachricht, Datei, Veröffentlichung oder Aufzeichnung vor?	Native Datei, Anbieter, Empfänger, verifizierte Kopie.

Komponente	Überprüfungsfrage	Quelle, die unterscheiden kann
Integrität	Welche Darstellung wurde empfangen und wie hat sie sich verändert?	Original, Export, EML-Datei, Manifest und Hashwert.
Zurechnung	Konto, Gerät oder Person: Mit welchen Beweisen?	Sitzungen, Faktoren, Registrierung, Kontext und Nutzung.
Zeit	Welche Uhr, Zeitzone und welches Ereignis stellt das Datum dar?	Wörtlicher Datensatz, Synchronisation und unabhängige Quellen.
Ort	Handelt es sich um Koordinaten, eine Funkzelle, eine Ableitung oder eine Aussage?	Genauigkeit, Azimut, Karte, Sensoren und Bestätigung.
Bedeutung	Beweist der Inhalt das Geschilderte oder nur das Sichtbare?	Gesprächsverlauf, Abfolge, Original und alternative Erklärung.

1.2 Akte und Abdeckung

Das empfangene und das fehlende Material werden inventarisiert: Bilder, native Dateien, Datenträger, Schreiben, Berichte, Anhänge, Exporte, Videos, Audios, Gesprächsdatenlisten, Aufzeichnungen und Aussagen. Jedes Objekt erhält eine Kennung, ohne seinen ursprünglichen Namen zu verändern. Zitiert ein Gutachten einen nicht verfügbaren Anhang, wird dessen Fehlen dokumentiert, bevor die Schlussfolgerung bewertet wird. Ein Bericht wird nicht so geprüft, als existierten seine Anhänge lediglich durch Verweis.

Die Abdeckung beschreibt Zeitraum, Systeme, Filter und nicht einbezogene Objekte. „Das Telefon wurde analysiert“ sagt nicht, ob der gesamte Speicher, eine Partition, eine Anwendung oder einige Bildschirmfotos geprüft wurden. Auch „die Kommunikation wurde untersucht“ sagt nicht, ob spätere Nachrichten ausgeschlossen wurden, die den Sinn verändern. Die Verteidigung benötigt die Abfrage und den untersuchten Bestand, nicht nur das für eine Seite günstige Ergebnis.

> **Arbeitsregel**
> Prüfen Sie zuerst nicht die Reputation des Sachverständigen. Prüfen Sie Objekt, Abdeckung und Methode. Eine Kritik an den Referenzen repariert keine Quelle, die Sie selbst nicht geprüft haben.

Was jede Darstellung bewahrt — ACCCF · REDAKTIONELLE REKONSTRUKTION · FIKTIVE DATEN

Ein gutes Bild kann eine unvollständige Quelle sein.

Objekt	Bewahrt	Bewährt nicht allein
Bildschirmfoto	Sichtbares Fragment und Bildschirmdesign.	URL, Datum, Konto, Gesprächsverlauf oder Integrität.
Export	Felder und Abfolge nach Wahl des Anbieters.	Vollständige Abdeckung oder Bedeutung von Leerstellen.
Native Datei	Struktur und verfügbare Metadaten.	Menschliche Urheberschaft oder Wahrheitsgehalt des Inhalts.
Serverprotokoll	Systemereignisse und ihr Kontext.	Physische Identität oder Nichtvorhandensein anderer Kanäle.

Die Abbildung erläutert Entscheidungen und Zusammenhänge; sie stellt keine Beweise aus einem echten Fall dar.

Abbildung 1. Was jede Darstellung bewahrt. Ein gutes Bild kann eine unvollständige Quelle sein. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 2. Überprüfung von Entgegennahme und Verwahrung

2.1 Identität des Objekts vor dem Inhalt

Das Protokoll muss das genaue Objekt identifizieren: Typ, Marke, Modell, Serie oder verfügbare Kennungen, Zustand, Zubehör, Verpackung, Siegel, Datum und Personen. Ein generischer Datenträger, ein Speicher ohne Kennzeichnung oder ein in zwei Vorgängen unterschiedlich beschriebenes Telefon erfordert eine Klärung. Die Verteidigung fragt, welches Objekt eingegangen, welches erfasst und welches auf jeder Fotografie erscheint, ohne eine Abweichung automatisch als böswillige Manipulation zu werten.

Bei einer Inkonsistenz in der Identifizierung wird die Schlussfolgerung bis zur Klärung ausgesetzt. Möglich sind ein Transkriptionsfehler, eine andere Darstellung oder tatsächlich ein anderes Objekt. Protokolle, Schreiben, Fotografien, Kapazität, Format, Kennzeichnungen, Siegel und Codes des Zentralrings optischer Datenträger werden verglichen. Die Unsicherheit richtet sich auf die Quelle, nicht auf die Person.

2.2 Fehlende Übertragungen im Verlauf

Die Beweismittelkette muss Zugriffe und Verantwortungswechsel rekonstruieren: Entgegennahme, Öffnen, Kopie, Analyse, Transport, Download und Rückgabe. Liegt nur die Unterschrift der abschließenden Übergabe vor, bleibt ein Zeitraum ohne Nachverfolgbarkeit. Das beweist keine Veränderung, begrenzt jedoch, wer das Objekt unter welchen Bedingungen verändert haben könnte.

Bei digitalen Dateien wird der gesamte Kanal aufbewahrt: EML-Datei, Kopfzeilen, Nachrichtentext, Anhänge, Link, Berechtigungen, Version und Download. Ein bei Empfang berechneter Hashwert kontrolliert die Integrität ab diesem Zeitpunkt, nicht rückwirkend seit der Erstellung. Schreibt der Anbieter den Hashwert in den Nachrichtentext, wird dieser überprüft und die Beziehung aufbewahrt. Kopiert der Bericht nur einen Wert ohne Objekt, Algorithmus und Datum, ist seine Aussage begrenzt.

Frage zur Verwahrung	Erwarteter Nachweis	Schlussfolgerung, die nicht vorgezogen werden darf
Handelt es sich um dasselbe Objekt?	Kennungen, Fotografien, Siegel und Protokolle stimmen überein.	„Das Protokoll sagt dasselbe, also ist alles gültig.“
Wer konnte zugreifen?	Ereignisse, Rollen, Standort, Zweck und Datum.	„Nur der Sachverständige hatte Kontakt.“
Welche Kopie wurde analysiert?	Beziehung zwischen Original, Image, Export und Arbeitskopie.	„Die Kopie ist bitweise, weil der Bericht dies behauptet.“
Was hat sich beim Export geändert?	Filter, Zeitzone, Format, Felder und Einschränkungen.	„Die PDF-Datei entspricht der vollständigen Datenbank.“
Was ist unbekannt?	Fehlende Zeiträume, Handlungen und Quellen.	„Das Fehlen eines Datensatzes beweist eine Fälschung.“

2.3 Befugnis und Verhältnismäßigkeit

Die Verteidigung prüft, wer den Zugriff autorisiert hat, welche Handlungen erlaubt waren und welche Ausschlüsse bestanden. Ein freiwillig übergebenes Passwort kann eine konkrete Abfrage autorisieren, aber keine undifferenzierte Kopie des gesamten digitalen Lebens. Ein Unternehmensgerät kann

persönliche Daten oder Daten Dritter enthalten. Die Fähigkeit, eine Datei zu öffnen, beweist für sich allein nicht die Erlaubnis, sie für jeden Zweck zu verwenden.

Die Überprüfung lädt nicht dazu ein, einen Eingriff zu wiederholen. Erlaubt die Akte keinen Zugriff auf eine Quelle, wird diese über den entsprechenden Weg angefordert. Die verteidigende Person darf nicht auf fremde Konten zugreifen, um zu „verifizieren“, und darf keine Werkzeuge auf fremden Geräten installieren. Die technische Verteidigung schützt auch vor einer zweiten Verletzung der Privatsphäre.

> **Ergebnis dieser Etappe**
> Eine Tabelle mit Objekt, Zustand, Identität, Befugnis, Übertragungen, Darstellungen und Lücken. Die nächste Etappe analysiert Widersprüche auf dieser Grundlage, nicht auf Grundlage einer erinnerten Geschichte.

Kapitel 3. Matrix der Widersprüche

3.1 Erkennen, ohne nur das zu wählen, was nützt

Die Matrix enthält Tatsachen, die mit der Anklage und mit anderen Erklärungen vereinbar sind. Jede Zeile enthält Behauptung, Objekt, wörtlichen Wert, Methode, Widerspruch, mögliche Erklärung und ausstehenden Beweis. Ein Widerspruch wird nicht als „falsch“ markiert, bevor Uhren, Formate, Felder, Abdeckung, Darstellungen und Transkription geprüft wurden. Einige Unterschiede sind erklärbar; andere verhindern die Schlussfolgerung.

Ein Ergebnis kann einen Teil bestätigen und einen anderen schwächen. Eine EML-Datei kann beweisen, dass der empfangene Anhang mit der Erklärung des Anbieters übereinstimmt, aber nicht, dass sein Inhalt wahr ist. Ein Video kann technisch original sein und eine inszenierte Szene zeigen. Ein Datum kann kohärent sein und dennoch nicht zum behaupteten Ereignis gehören. Die Überprüfung bewahrt diese Unterschiede.

Behauptung	Überprüfung	Mögliches Ergebnis
„Die Datei hat sich nie verändert“	Hashwert, Algorithmus, Zeitpunkt und Beziehung zur Quelle.	Übereinstimmung seit Empfang; frühere Geschichte unbekannt.
„Die Konversation ist vollständig“	Export, Gesprächsverlauf, Teilnehmer und Filter.	Sichtbares Fragment; Abdeckung noch zu belegen.
„Das Foto wurde um 20:42 Uhr aufgenommen“	Metadaten, Uhr, Zeitzone und Abfolge.	Internes Datum mit anderer Uhrzeit vereinbar oder unsicher.
„Die Antenne lokalisiert den Beschuldigten“	Funkzelle, Technologie, Abdeckung und Endgerät.	Netzwerkbeziehung; weder Person noch Wohnadresse.
„Das Gutachten beweist die Urheberschaft“	Quellen, Methode, Alternativen und Prämissen.	Zugeordnetes Konto; physische Identität noch offen.

3.2 Arten von Widersprüchen und ihre Wirkung

Ein Identitätswiderspruch fragt, ob es sich um dasselbe Objekt handelt; ein Quellenwiderspruch, ob die Darstellung die Behauptung erlaubt; ein Methodenwiderspruch, ob die Abfrage dieses Ergebnis erzeugen kann; ein Zeitwiderspruch, ob Uhren und Zonen vereinbar sind; ein Ableitungswiderspruch, ob die Schlussfolgerung den Prämissen folgt. Nicht alle haben dasselbe Gewicht und nicht alle machen die Akte unbrauchbar. Der Bericht erläutert die konkrete Wirkung auf jede Behauptung.

Auch wird zwischen dem Fehlen von Beweisen und dem Beweis des Nichtvorhandenseins unterschieden. Das Fehlen eines Datensatzes in einem Export kann bedeutsam sein, wenn die Quelle für Zeitraum und Filter vollständig ist, beweist jedoch nicht, dass das Ereignis in anderen Kanälen nicht stattfand. Diese Unterscheidung verhindert, dass eine Einschränkung des Anbieters zu einem absoluten Beweis für Verteidigung oder Anklage wird.

> **Prüfung der Überprüfung**
> Verändert der Widerspruch die Identität des Objekts, die Abdeckung, die Chronologie oder die Schlussfolgerung? Wenn nichts davon, handelt es sich vielleicht um einen Unterschied in der Darstellung. Wenn ja, wird die technische Frage formuliert, die ihn auflöst.

Ein Widerspruch erfordert eine Erklärung, kein Urteil ACCCF · REDAKTIONELLE REKONSTRUKTION · FIKTIVE DATEN

Beispiel einer Matrix zur Prüfung von Quelle, Methode und Ableitung

Behauptung	Prüfung	Zulässige Interpretation
„Die Bildschirmaufnahme zeigt die gesamte Konversation“	Export, Gesprächsverlauf und Teilnehmer anfordern.	Das Bild enthält ein Fragment; die Abdeckung ist unbekannt.
„Das Video wurde zu dieser Zeit aufgenommen“	Zähler, Zeitzone, Uhr und Veröffentlichung prüfen.	Datum je nach Quelle vereinbar oder unsicher.
„Die Antenne beweist die Anwesenheit“	Funkzelle, Azimut, Technologie und Abdeckung anfordern.	Beziehung zu einer Funkzelle, keine Wohnadresse.
„Der Inhaber schrieb die Nachricht“	Sitzungen, Gerät, 2FA und Kontext.	Zugeordnetes Konto; Person nicht belegt.

Die Abbildung erläutert Entscheidungen und Zusammenhänge; sie stellt keine Beweise aus einem echten Fall dar.

Abbildung 2. Ein Widerspruch erfordert eine Erklärung, kein Urteil. Beispiel einer Matrix zur Prüfung von Quelle, Methode und Ableitung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 4. Bildschirmfotos, Gespräche und Dateien

4.1 Das Bildschirmfoto als Fragment

Sichtbares und Fehlendes werden genau beschrieben: URL, Anwendung, Version, Konto, Datum, Zeitzone, Gerät, Teilnehmer, frühere und spätere Nachrichten, Anhänge und Reaktionen. Ein Bildschirmfoto kann ein Fragment zeigen, beweist für sich allein jedoch weder Vollständigkeit noch Erstellungsdatum oder Urheberschaft. Die Anfrage richtet sich an die native Datei, den Anwendungsexport, die Nachricht bei einem anderen Teilnehmer oder den Anbieterdatensatz.

Liegt nur das Bildschirmfoto vor, wird die Schlussfolgerung begrenzt. Eine Abweichung in Ausrichtung, Komprimierung oder Format wird nicht automatisch als Herstellung bezeichnet: Diese Hinweise können von der Anwendung oder der Aufnahme stammen. Eine frühere Quelle wird gesucht und dokumentiert, wer sie wann mit welchem Werkzeug erzeugt hat. Fehlt der Zugriff, bleibt die Unsicherheit bestehen.

4.2 Export und Kontext von Nachrichten

Ein Export kann Text und Dateien enthalten, die der Benutzer oder die Anwendungsfunktion ausgewählt hat. Er entspricht nicht notwendigerweise der Datenbank oder allen Ereignissen: Bearbeitung, Löschung, Reaktionen, Sperrungen und verknüpfte Geräte können unterschiedliche Abdeckung haben.

Feldverzeichnis, Version, Datum und Filter werden angefordert. Bei Ende-zu-Ende-Verschlüsselung kann der Anbieter den Inhalt nicht aufbewahren; andere Ebenen können dennoch geprüft werden.

Die Abfolge wird mit Nachrichten anderer Teilnehmer und mit Protokollen verknüpfter Geräte verglichen. Eine Reaktion oder eine spätere Nachricht kann den Sinn eines Satzes verändern, ohne die frühere zu widerlegen. Die Verteidigung kürzt die Konversation nicht, um den gegenteiligen Effekt zu erzeugen: Sie fordert ausreichenden Kontext und erklärt, welcher Teil weiterhin mehrdeutig ist.

4.3 Metadaten und Versionen

Felder für Datum, Autor, Anwendung oder Gerät haben unterschiedliche Erzeuger und Bedeutungen. Das Erstellungsdatum des Systems kann das Datum der Kopie sein; der Autor kann eine Konfiguration sein; das Modell kann von einer Anwendung stammen, die die Datei neu geschrieben hat. Interne Metadaten, Systemeigenschaften, Miniaturansichten, Versionsverlauf, Cloud-Kopie und Namensabfolge werden verglichen. Ein Metadatum ist ein überprüfbarer Hinweis, kein unfehlbares Zeugnis.

Datenelement	Ausgangshypothese	Zu prüfende Alternative
Autor des Dokuments	Die genannte Person hat es geschrieben.	Gemeinsam genutztes Konto, Vorlage, anderer Bearbeiter oder Konfiguration.
Erstellungsdatum	Die Datei entstand zu diesem Zeitpunkt.	Kopie, Download, Konvertierung oder andere Uhr.
IMG_0042	Gehört zu einer durchgehenden Abfolge.	Import, Umbenennung, Neunummerierung oder fehlende Dateien.
E-Mail-Konto	Der Inhaber hat den Text geschrieben.	Sitzung, Delegation, Diebstahl oder Verfassen durch Dritte.
EXIF-Standort	Die Person befand sich am exakten Punkt.	Genauigkeit, Bearbeitung, Vererbung oder Synchronisierung.

Fiktiver Fall

Ein Bildschirmfoto zeigt eine Drohung um 21:03 Uhr. Die native Datei und die von einem anderen Teilnehmer empfangene Nachricht zeigen 20:03 UTC, was einer anderen Ortszeit entspricht. Die Abweichung beweist keine Fälschung: Sie zeigt eine in der Anklage ausgelassene Umrechnung. Die Überprüfung korrigiert die Chronologie und bewahrt den Inhalt zur Analyse in seinem Kontext.

Kapitel 5. Argumentation und unabhängige Überprüfung

5.1 Prämissen und falsche Konsequenz

Der Syllogismus hilft zu zeigen, was fehlt. Obersatz: Ein Funkzellendatensatz belegt unter bestimmten Bedingungen eine Netzwerkbeziehung. Untersatz: Der Datensatz verknüpft ein Ereignis mit Funkzelle A. Zulässige Schlussfolgerung: Diese dokumentierte Beziehung besteht. Daraus folgt weder, dass sich der Inhaber an einer Adresse befand noch, dass er das Telefon bei sich trug. Dafür werden Prämissen über Standort, Endgerät und Nutzung benötigt.

Eine falsche Konsequenz entsteht, wenn eine kleine Wahrheit als Freibrief für eine größere verwendet wird: Die Signatur wird überprüft, also ist der gesamte Inhalt wahr; das Konto gehört einer Person, also hat sie geschrieben; die Datei ist integer, also ist sie seit ihrer Entstehung original; der Sachverständige ist anerkannt, also ist seine Schlussfolgerung wissenschaftlich. Jeder Sprung erfordert eine zusätzliche Prämisse und eine Überprüfung.

5.2 Alternative Hypothesen und Falsifikationstest

Mindestens zwei plausible Erklärungen und eine Prüfung zu ihrer Schwächung werden formuliert. Wird die Neuerstellung einer Datei behauptet, werden Verlauf und Sicherungskopien geprüft; wird die Nutzung durch den Inhaber behauptet, werden Sitzungen und zweiter Faktor geprüft; wird Manipulation behauptet, werden Original und Referenzen verglichen. Die Alternative wird nicht gewählt, weil sie nützlich ist: Sie wird mit demselben Standard wie die Anklage bewertet.

Hypothese A	Hypothese B	Unterscheidende Prüfung
Am Austrittstag erstelltes Dokument	Früheres Dokument, das nachträglich kopiert oder bearbeitet wurde.	Versionsverlauf, Sicherungskopie und Aktivität.
Vom Inhaber verwendetes Konto	Von einer anderen Person verwendetes Konto oder eine dauerhafte Sitzung.	Faktoren, Gerät, gleichzeitiger Zugriff und Kontrolle.
Bearbeitetes Video	Originalvideo einer inszenierten Szene.	Struktur, Referenzen und Umstände der Aufzeichnung.
Widersprüchlicher Standort	Quellen mit unterschiedlicher Genauigkeit oder Zeitzone.	Metadaten, Funkzelle, Uhr und unabhängige Sensoren.

5.3 Überprüfung, die den Bericht zu widerlegen versucht

Der unabhängige Prüfer korrigiert nicht nur den Stil. Er lokalisiert jedes Objekt, wiederholt Abfragen, vergleicht Werte, sucht fehlende Anhänge und versucht, eine Erklärung zu finden, die der Analyst nicht berücksichtigt hatte. Auch günstige Beweise für die Anklage werden geprüft, damit keine voreingenommene Verteidigung entsteht. Anmerkungen werden mit Quelle und Änderung beantwortet, nicht mit persönlicher Autorität.

NIST SP 800-86 und ISO/IEC 27037 bieten Rahmen für Sammlung, Sicherung, Untersuchung, Analyse und Bericht. Sie garantieren nicht, dass eine Schlussfolgerung wahr ist: Sie ermöglichen zu prüfen, ob der Weg dokumentiert wurde und ob eine andere Person ihn reproduzieren kann. Ansehen ersetzt keine Überprüfbarkeit.[12]

> **Unabhängigkeitsregel**
> Der beste Zeitpunkt, um eine schwache Prämisse zu finden, ist vor der Übermittlung. Muss der Bericht eine Quelle oder eine Alternative verbergen, um sich zu halten, benötigt er eine weitere Analyse, keine bessere rhetorische Verteidigung.

[1]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die Zulässigkeit. Offizielle Online-Quelle

[2]ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt. Offizielle Online-Quelle

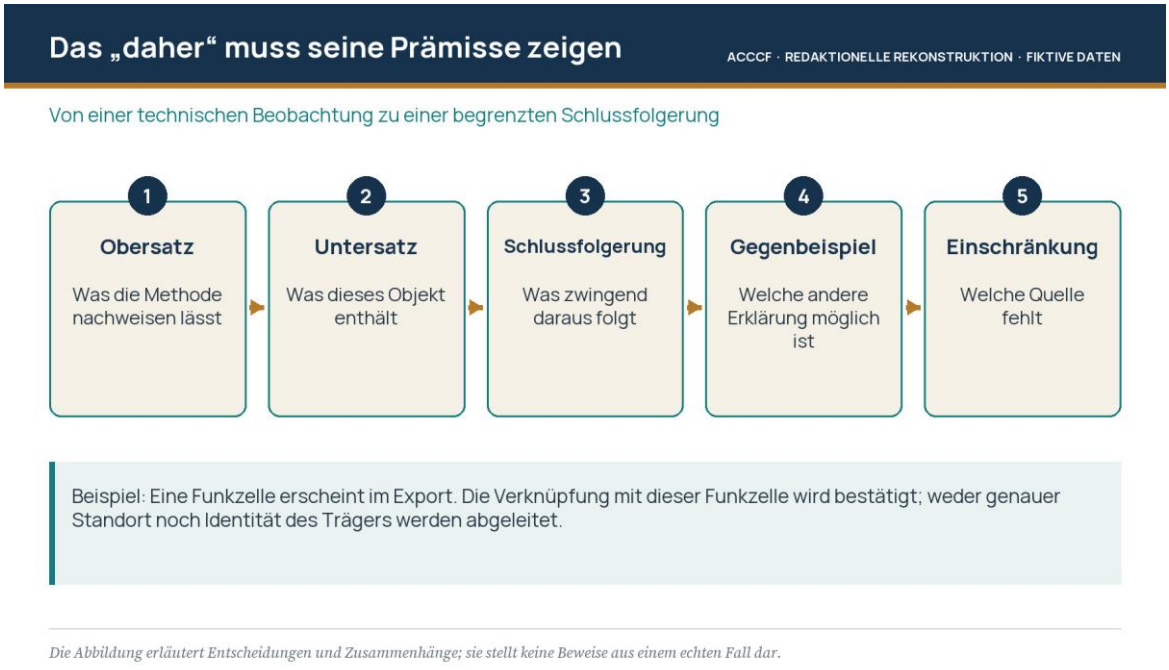


Abbildung 3. Das „daher“ muss seine Prämisse zeigen. Von einer technischen Beobachtung zu einer begrenzten Schlussfolgerung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 6. Überprüfung des forensischen Berichts

6.1 Nachverfolgbarkeit jeder Schlussfolgerung

Jede Schlussfolgerung wird rückwärts verfolgt: Schlussfolgerung → Befund → Abfrage → Objekt → Erfassung → Quelle → Befugnis. Fehlt eine Verbindung, wird bestimmt, welche Behauptung eingeschränkt werden muss. Bibliografische Seiten ersetzen diesen Weg nicht. Eine technische Norm kann wahr sein und beweist nicht, dass sie auf das richtige Objekt angewendet wurde.

Dokumentierte Tatsachen, technische Ergebnisse, Ableitungen und juristische Stellungnahmen werden unterschieden. Der Sachverständige kann erklären, was er getan und beobachtet hat; er muss weder Schuld noch den Ausgang des Verfahrens erklären. Eine Rechtsmeinung wird von den Befunden getrennt, damit ihre Bewertung die technische Überprüfung nicht beeinträchtigt.

Textebene	Beispiel für eine Überprüfung	Offene Frage
Entgegennahme	Die EML-Datei traf mit zwei Anhängen ein.	Ist sie vollständig und mit Kennungen versehen?
Ergebnis	Der Anhang stimmt mit dem angegebenen Hashwert überein.	Was beweist dies über Inhalt und Herkunft?
Ableitung	Die Übermittlung bewahrt eine Integritätsprüfung.	Ab welchem Zeitpunkt und mit welcher Einschränkung?
Schlussfolgerung	Der Datensatz ist mit einer überprüfbaren Übermittlung vereinbar.	Können Identität oder Wahrheit behauptet werden?
Juristische Stellungnahme	Die Partei ist verantwortlich.	Entspricht dies der Aufgabe des Sachverständigen und welche Prämissen werden verwendet?

6.2 Nützliche Fragen zur Widerlegung

Die Fragen werden formuliert, um eine Überprüfung zu erhalten, nicht um eine Rede zu halten: Welches Objekt erzeugte die Daten, welche Werkzeugversion wurde verwendet, welche Filter wurden angewendet, welche leeren Felder bestehen, welche Zeitzone wurde verwendet, welche Quelle schloss eine Hypothese aus und welche Einschränkungen verhindern die Zuordnung einer Handlung zu einer Person? Lautet die Antwort „die Erfahrung des Sachverständigen“, wird der konkrete Datensatz angefordert.

Es wird auch gefragt, was die Schlussfolgerung ändern würde. Existiert keine Quelle, die sie ändern könnte, kann die Methode für Falsifikation geschlossen sein. Ein belastbarer Bericht gibt an, welche Daten seine Schlussfolgerung stützen und welche sie schwächen könnten. Das macht ihn nicht schwächer, sondern überprüfbar.

> **Zentrale Frage**
> Kann eine andere Person die Ausgangsversion ablehnen, das Objekt finden, die Methode wiederholen und zu einem vereinbaren Ergebnis gelangen? Wenn nicht, hängt die Schlussfolgerung von einer Erklärung ab, die die Akte nicht überprüfen kann.

Kapitel 7. Integrierter Fall: von der Anschuldigung zur begrenzten Schlussfolgerung

7.1 Verfügbares Material

Ein fiktiver Fall enthält eine Gesprächsaufnahme, ein von einer Plattform heruntergeladenes Video, eine PDF-Gesprächsdatenliste und einen Bericht, der Anwesenheit und Urheberschaft behauptet. Die beschuldigte Person erkennt das Konto an, bestreitet jedoch, die Nachricht geschrieben zu haben, und nennt einen anderen Standort. Es gibt noch keine native Videodatei und keine EML-Datei der Gesprächsdatenliste. Das erste Ergebnis ist kein umfangreiches Gegengutachten: Es ist ein Inventar fehlender Quellen.

7.2 Überprüfungen und Befunde

Der Export der Konversation zeigt spätere Nachrichten, die den Sinn des Fragments verändern, ohne die erste Nachricht zu löschen. Das Video weist eine Plattformkonvertierung auf, und das Kameraoriginal wird angefordert, um Kontinuität zu bewerten. Die EML-Datei der Gesprächsdatenliste ermöglicht die Überprüfung des Anhangs; das Feldverzeichnis zeigt jedoch, dass die Funkzelle eine Netzwerkbeziehung und keine Benutzerkoordinate ist. Der Anklagebericht hatte drei unterschiedliche Behauptungen miteinander verbunden.

Die Überprüfung kommt nicht zu dem Ergebnis, dass alles falsch ist. Sie kommt zu dem Ergebnis, dass die Nachricht existiert, der ursprüngliche Kontext unvollständig war, das Video noch keine Aussage zur Originalität zulässt und die Gesprächsdatenliste weder Wohnadresse noch Träger beweist. Diese Schlussfolgerungen sind nützlich, weil sie abgrenzen, was fundiert diskutiert werden kann und was eine andere Quelle erfordert.

7.3 Kurzer Ergebnisbericht

Beispiel einer technischen Schlussfolgerung

```
1. Die Bildschirmaufnahme EV-01 enthält das sichtbare Fragment der Nachricht, belegt jedoch weder
Vollständigkeit, physische Urheberschaft noch Erstellungsdatum. Der spätere Export EV-04 liefert
angrenzende Nachrichten, die für die Interpretation des Inhalts berücksichtigt werden müssen.
```

```
2. Die Datei EV-02 ist ein Plattformdownload. Ihre Struktur kann mit einer legitimen Konvertierung
vereinbar sein; ohne Kameraoriginal und eine vergleichbare Referenz wird keine Aussage zur Originalität
getroffen.

3. Die Gesprächsdatenliste EV-03 verknüpft das Ereignis mit der Funkzelle DEMO-A17. Das Feldverzeichnis
enthält keine Messungen für eine punktgenaue Standortbestimmung. Die Quelle belegt weder Wohnadresse noch
Träger.

4. Die Behauptung physischer Urheberschaft erfordert zusätzliche Beweise zu Sitzung, Gerät, Faktoren und
Kontext. Das Ergebnis beweist weder allgemeine Falschheit noch das Nichtvorhandensein anderer Ereignisse
außerhalb des geprüften Umfangs.
```

Lehre

Die technische Verteidigung kann präzise sein, ohne eine Freisprechung zu versprechen. Ihre Stärke liegt darin, genau zu zeigen, welcher Teil einer Anschuldigung nicht aus der Quelle folgt.

Anhang A. Überprüfungsformat und Fragen

A.1 Matrix der Behauptungen

Feld	Erforderlicher Inhalt	Fiktives Beispiel
Wörtliche Behauptung	Text ohne Interpretation oder Adjektive.	„Die Person schrieb um 21:03 Uhr.“
Objekt und Quelle	Kennung, Darstellung und Herkunft.	Bildschirmaufnahme EV-01; native Datei ausstehend.
Verwendete Prämissen	Was für ihre Aufrechterhaltung wahr sein muss.	Konto = Person; angezeigte Uhrzeit = Ortszeit.
Überprüfung	Methode, Filter, Werkzeug und Abdeckung.	Export, Sitzungen und Feldverzeichnis.
Widerspruch	Wörtlicher Wert, der nicht passt, und mögliche Ursachen.	Nachricht mit einer anderen UTC-Zeitzone.
Begrenzte Schlussfolgerung	Was bewiesen ist und was nicht.	Die Nachricht existiert; physische Urheberschaft nicht belegt.
Ausstehende Quelle	Was das Ergebnis verändern kann und wie es angefordert wird.	Sitzungs- und Teilnehmerprotokolle.

A.2 Liste technischer Fragen

Leitfaden zur Überprüfung

```
1. Was ist das genaue Objekt und wo liegt seine native Darstellung?
2. Welche Abfrage erzeugte den Befund und welche Abdeckung hatte sie?
3. Welche Felder wurden ausgeschlossen, gefiltert oder blieben leer?
4. Was bedeuten Datum, Zeitzone und Genauigkeit?
5. Welche andere Erklärung ist mit demselben Befund vereinbar?
6. Welche Quelle könnte die Haupthypothese schwächen?
7. Ist die Bestätigung unabhängig oder wiederholt sie dieselbe Datei?
8. Welche Prämisse erlaubt den Schritt vom Konto zur Person?
9. Welcher Teil der Schlussfolgerung ist technisch und welcher juristisch?
10. Welche Einschränkungen verhindern weitergehende Aussagen?
```

A.3 Register angeforderter und empfangener Quellen

Anfrage	Entgegennahme und Kontrolle	Zustand
Native Datei und Export der Konversation	EML-Datei, Anhänge, Hashwert, Filter und Feldverzeichnis.	[ausstehend / empfangen / eingeschränkt]

Anfrage	Entgegennahme und Kontrolle	Zustand
Originaldatei und Videoreferenzen	Objekt, Werkzeug, Version, Datum und Methode.	[ ]
Native Gesprächsdatenliste und Feldverzeichnis	Felder, Zeitzone, Funkzelle, Abdeckung und EML-Datei.	[ ]
Sitzungen und Kontofaktoren	Registrierung, Geräte, Zugriff und Wiederherstellung.	[ ]
Anhänge des bestrittenen Berichts	Beziehung zu Zitaten und reproduzierbaren Abfragen.	[ ]

Anhang B. Juristische Funktionen für die Überprüfung

Die technische Überprüfung verbindet Regeln von Anerkennung, Integrität, Original, Zurechnung und Bewertung. Die Zulassung ist keine vollständige Beweiskraft, und eine Signaturvermutung belegt nicht alle Tatsachen. Die Quelle muss in ihrer Gerichtsbarkeit, Materie und Version analysiert werden; dieser Leitfaden ersetzt die prozessuale Prüfung der Verteidigung nicht.

Jurisdiktion	Relevante dokumentarische Funktion	Anwendung in der Verteidigung
Mexiko	CCom 89–94 und 1205; CFPC 210-A / CNPCF 348–350 je nach Übergang.	Zuverlässigkeit der Methode, Zurechnung, Integrität und Zugänglichkeit; geltendes Regime prüfen.
Peru	IOFE-Verordnung; CPC 188–197 und 245.5; sektorale Archivnormen.	Beweislast, Rechtmäßigkeit, typische und atypische Mittel und Datumsbestimmung durch technische Mittel.
Chile	Ley 19.799, Artikel 1–5.	Signaturklassen, Datum und unterschiedlicher Beweiswert.
Argentinien	Ley 25.506; CCyC 318–319; Decreto 182/2019.	Zuverlässigkeit von Trägern, Korrespondenz und begrenzte Vermutungen.
Kolumbien	Ley 527, Artikel 5–13, 16–25 und 28; CPACA, soweit zutreffend.	Original, Aufbewahrung, Kontext, Zulässigkeit und Bewertung.
Ecuador	Ley 67, Artikel 2, 6–8, 10–16 und Verordnung.	Integrität, Aufbewahrung, Herkunft und Wirkungen der Signatur.
Spanien / EU	eIDAS 25–26 und 46; LEC 326 und 384; Ley 6/2020.	Anfechtung, Verwahrung, Prüfung und Bewertung; das Gesetz 59/2003 nicht als gültig zitieren.

Quellen der Tabelle:[3][4][5][6][7][8][9][10][11][12][13][14]

Abschluss

Überprüfen bedeutet nicht, Zweifel zu erzeugen. Es verlangt, dass eine Behauptung eine Quelle, eine Methode und eine Schlussfolgerung hat, die das Bewiesene nicht überschreitet.

[3] Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung. Offizielle Online-Quelle

[4] Código Federal de Procedimientos Civiles, Artikel 210-A: Zuverlässigkeit der Methode, Zurechnung, Zugänglichkeit und Integrität elektronischer Informationen. Der Code wurde durch Dekret vom 07-06-2023 aufgehoben und unterliegt einem schrittweisen Übergangsregime. Offizielle Online-Quelle

[5] Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab. Offizielle Online-Quelle

[6] Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Mittel, Beweislast, Bewertung und Datumsbestimmung durch technische Mittel. Offizielle Online-Quelle

[7] Chile. Ley 19.799 über elektronische Dokumente und elektronische Signatur, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert. Offizielle Online-Quelle

[8] Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz unabhängig vom Medium und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren. Offizielle Online-Quelle

[9] Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen. Offizielle Online-Quelle

[10] Kolumbien. Ley 527 de 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur. Offizielle Online-Quelle

[11] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[12] Reglamento (UE) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene elektronische Signatur und Rechtswirkungen qualifizierter elektronischer Signaturen. Offizielle Online-Quelle

[13] Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und gesunde Kritik. Offizielle Online-Quelle

[14] Spanien. Ley 6/2020 über elektronische Vertrauensdienste: Aufhebung des Gesetzes 59/2003 und von Artikel 25 der LSSI; das frühere Regime wird nicht als gültig zitiert. Offizielle Online-Quelle