ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

05

BAND

Gerät, Anwendung, Konto und Anbieter

Spanische Ausgabe · 2026

Handbuch zur forensischen Untersuchung von Mobiltelefonen und Instant-Messaging

Entgegennahme, Isolierung, Erfassung, Analyse, Kontext und verantwortungsvolle Zurechnung

Mobile Kommunikation untersuchen, ohne ein Bildschirmfoto mit der Quelle, eine Extraktion mit einer vollständigen Erfassung oder ein Konto mit der Person zu verwechseln, die es verwendet hat.

Für Sachverständige, Ersthelfer, Rechtsanwälte, Ermittler und Verantwortliche für die Verwahrung. Das Verfahren hängt von Gerät, System, Anwendung, Version, Verschlüsselung und rechtlicher Befugnis ab; es enthält keine Methoden zum Umgehen von Sperren oder zum Zugriff auf fremde Konten.

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 Seitenzählung entspricht der PDF-Ausgabe. Word kann dieses Inhaltsverzeichnis beim Öffnen des Dokuments aktualisieren; die interne Navigation der Überschriften bleibt erhalten.

Einleitung: Das Telefon spricht nicht für sich selbst 3

Kapitel 1. Entgegennahme und Zustand des Geräts 3

- **1.1 Ein Protokoll, das eine andere Person nachvollziehen kann** 3
- **1.2 Risiken von Verlust und Veränderung** 4

Kapitel 2. Quellen nach Ebenen 4

- **2.1 Gerät, Anwendung und damit verbundene Daten** 4
- **2.2 Konto, Sitzungen und verknüpfte Geräte** 5
- **2.3 Anbieter und andere Beteiligte** 5

Kapitel 3. Isolierung, Stromversorgung und Transport 6

- **3.1 Tatsächliche und überprüfte Isolierung** 6
- **3.2 Verpackung, Transport und Verwahrung** 7

Kapitel 4. Methoden der Erfassung 7

- **4.1 Manuelle Dokumentation und Bildschirmfotos** 7
- **4.2 Anwendungsexport und Sicherungskopie** 7
- **4.3 Logische Extraktion, erweiterte Extraktion und Anbieter** 7
- **4.4 Validierung von Werkzeug und Ausgabe** 8

Kapitel 5. Untersuchung von Gesprächen und Inhalten 9

- **5.1 Gesprächsverlauf rekonstruieren, nicht nur den einzelnen Satz** 9
- **5.2 Bearbeitete, gelöschte und weitergeleitete Nachrichten** 9
- **5.3 Anhänge, Miniaturansichten und Metadaten** 10

Kapitel 6. Zurechnung und Kommunikation 10

- **6.1 Konto, Gerät und Person** 10
- **6.2 Chronologie und unabhängige Bestätigung** 10
- **6.3 Bericht mit ausdrücklich abgegrenztem Umfang** 11

Anhang A. Operative Vorlagen 12

- **A.1 Entgegennahme des Geräts** 12
- **A.2 Inventar von Konten und Quellen** 12
- **A.3 Erfassungsprotokoll** 12
- **A.4 Zurechnungsmatrix** 12

Anhang B. Rechtsrahmen und abschließende Kontrolle 13

Einleitung: Das Telefon spricht nicht für sich selbst

Ein Mobiltelefon enthält Gespräche, Dateien, Sensoren, Konten und Aktivitätsreste, kann aber auch lediglich ein Fenster zu einer Cloud oder zu anderen Teilnehmern sein. Die erste Frage lautet nicht, welches Programm es öffnen wird, sondern welche Behauptung zu beweisen ist und welche Quellen sie beantworten können. Soll festgestellt werden, wer eine Nachricht geschrieben hat, genügt ein Foto des Bildschirms nicht: Erforderlich sind Angaben zu Sitzungen, Geräten, Faktoren, Inhalt und Kontext.

Die mobile forensische Analyse hängt von System, Anwendung, Version, Verschlüsselung und Zustand des Geräts ab. Eine Extraktion kann zugängliche Datenbanken erfassen; eine andere beschränkt sich möglicherweise auf sichtbare Dateien oder einen Export. Das Wort „forensisch“ ändert nichts am tatsächlichen Umfang. Der Bericht muss angeben, was durchgeführt, was erhalten und was nicht erfasst wurde, ohne die Wiederherstellung gelöschter Nachrichten oder universellen Zugriff zu versprechen.

NIST SP 800-101 Rev. 1 behandelt Erhaltung, Erfassung, Untersuchung, Analyse und Berichterstattung bei Mobilgeräten unter besonderer Berücksichtigung von Validierung und Dokumentation. Es ist eine methodische Anleitung, keine aktuelle Liste der Fähigkeiten jedes Werkzeugs. Diese Fähigkeiten werden am konkreten Modell und an der konkreten Version mit Testdaten und überprüfbaren Ergebnissen geprüft.[1]

> **Erste Regel**
> Schalten Sie das Gerät nicht ein, erkunden Sie es nicht, setzen Sie es nicht zurück und verbinden Sie es nicht aus Neugier. Erfassen Sie Zustand und rechtliche Befugnis, bewahren Sie Zubehör auf und klären Sie, welche Informationen verloren gehen könnten, bevor Sie etwas verändern.

Kapitel 1. Entgegennahme und Zustand des Geräts

1.1 Ein Protokoll, das eine andere Person nachvollziehen kann

Das Protokoll beschreibt Art, Marke, Modell, sichtbare Identifikatoren, physischen Zustand, Ein-/Ausschaltzustand, Sperrung, Akkuladung, sichtbares Netz, Datum und Zeitzone, anwesende Personen, Zubehör und frühere Handlungen. Ein Passwort wird nicht im allgemeinen Protokoll vermerkt. Liegt eine Autorisierung zum Entsperren vor, werden ihr Vorhandensein und der sichere Mechanismus für ihre Verwendung dokumentiert. Frühere Kennzeichnungen bleiben erhalten und werden dem neuen Identifikator zugeordnet.

Der sichtbare Bildschirm wird nach Möglichkeit ohne Interaktion fotografiert: Uhrzeit, Netzsymbole, Akkuladung, Benachrichtigungen und Zustand. Das Foto belegt den Zustand in diesem Augenblick, nicht den gesamten Inhalt. Hat bereits jemand Anwendungen geöffnet oder eine Extraktion versucht, wird dies vermerkt. Eine nicht ideale Entgegennahme wird dokumentiert und nicht so umgeschrieben, als wäre das Objekt unversehrt eingegangen.

Feld	Fiktives Beispiel	Ermöglichte Entscheidung
Gerät	Telefon DEMO-MBL-003, Modell und Serie sichtbar.	Identifizieren und mit Protokollen abgleichen.

[1] NIST SP 800-101 Rev. 1. Leitfaden zur forensischen Analyse mobiler Geräte: Erhaltung, Erfassung, Untersuchung, Analyse, Validierung und Berichterstattung. Die Technologie und die konkreten Fähigkeiten müssen am aktuellen Gerät und Werkzeug geprüft werden. Offizielle Online-Quelle

Feld	Fiktives Beispiel	Ermöglichte Entscheidung
Zustand	Eingeschaltet, gesperrt, 43 %, sichtbares Mobilfunknetz.	Erhaltung und Isolierung priorisieren.
Zubehör	Kabel, Ladegerät, SIM und Hülle sind separat gekennzeichnet.	Zugriffswege und Kontext erhalten.
Angegebener Hergang	Der Inhaber versuchte vor der Übergabe, ein Gespräch zu exportieren.	Frühere Handlungen von der Analyse trennen.
Rechtliche Befugnis	Prüfung eines Gesprächs und bestimmter Konten.	Zugriff auf Dritte und andere Anwendungen beschränken.
Entscheidung	Zustand erhalten und Fachkraft hinzuziehen.	Nicht autorisierte Änderungen vermeiden.

1.2 Risiken von Verlust und Veränderung

Ein Gerät kann Nachrichten empfangen, synchronisieren, aus der Ferne gelöscht oder wegen Inaktivität gesperrt werden und Akkuladung verlieren. Es kann auch Sitzungen und Schlüssel enthalten, die beim Ausschalten verloren gehen. Zu bestimmen ist, welches Risiko am dringendsten ist und welches technische Wissen für den Umgang damit zur Verfügung steht. Ausschalten bedeutet nicht immer Erhaltung; eingeschaltet lassen bedeutet nicht immer Analyse. Das Protokoll muss die gewählte Vorgehensweise begründen.

Hat ein Gespräch Priorität, das bei einem anderen Teilnehmer oder beim Anbieter verfügbar ist, kann es weniger eingriffsintensiv sein, zunächst diese Quelle anzufordern, statt am Gerät zu arbeiten. Stehen flüchtige Aktivitäten oder ein Verschlüsselungsschlüssel im Vordergrund, kann eine autorisierte Live-Erfassung erforderlich sein. Das Ockhamsche Sparsamkeitsprinzip wählt die Quelle mit der größten Unterscheidungskraft und der geringsten Veränderung, nicht das ausgefeilteste Werkzeug.

> **Wann pausiert werden muss**
> Fehlende rechtliche Befugnis, Löschgefahr, ein nicht validiertes Werkzeug, unverstandene Verschlüsselung oder Gefahr für eine Person erfordern eine Pause und eine Eskalation. Das bloße Erkunden, um zu sehen, was erscheint, kann Beweise verändern und den Umfang ohne Genehmigung erweitern.

Kapitel 2. Quellen nach Ebenen

2.1 Gerät, Anwendung und damit verbundene Daten

Der Gerätespeicher kann Anwendungsdatenbanken, Dateien, Miniaturansichten, Protokolle, geschützte Zugangsdaten, Caches und Sensordaten enthalten. Ihre Verfügbarkeit hängt vom Zustand und vom Zugriff ab. Bei vorhandener Synchronisierung entspricht ein Bildordner nicht der gesamten Fotobibliothek. Eine lokal gelöschte Nachricht kann bei einem anderen Teilnehmer oder in einer Kopie weiterhin vorhanden sein, aber auch unwiederbringlich verloren sein. Die Analyse garantiert keines dieser beiden Extreme.

Zubehör ist wichtig: SIM oder eSIM, Speicherkarten, Ladegerät, Kabel, Adapter, Hülle, Dokumentation und andere synchronisierte Geräte. Eine Uhr, ein Tablet oder ein Computer kann Benachrichtigungen oder Sitzungen mit anderen Informationen enthalten. Diese Objekte werden inventarisiert, ohne die Befugnis automatisch zu erweitern: Eine Verbindung mit einem Objekt bedeutet nicht, dass sein gesamter Inhalt vom Auftrag umfasst ist.

2.2 Konto, Sitzungen und verknüpfte Geräte

Die Anwendung kann mehrere Sitzungen, Desktop-Clients, Sicherungskopien sowie Wiederherstellung per E-Mail oder über den Netzbetreiber ermöglichen. Sofern verfügbar, werden Listen verknüpfter Geräte, Hinzufügungen und Entfernungen, Faktoren, Daten, Änderungen an den Wiederherstellungsoptionen und Sitzungsaktivitäten angefordert. Der Kontoname beschreibt eine logische Verknüpfung; die Identität der natürlichen Person erfordert weitere Elemente.

Eine IP-Adresse kann einen Hinweis auf eine Netzverbindung liefern, aber weder einen Wohnsitz noch eine Person beweisen. Eine Telefonnummer kann neu vergeben worden sein oder im untersuchten Zeitraum einer anderen Person zugeordnet gewesen sein. Eine IMEI identifiziert in ihrem Kontext ein Gerät oder eine Konfiguration, nicht notwendigerweise den Gerätenutzer. Die Zurechnung stützt sich auf übereinstimmende unabhängige Elemente und alternative Erklärungen: Ausleihe, gemeinsame Nutzung, Fernzugriff, Übernahme einer Sitzung oder Verwaltung durch eine andere Person.

2.3 Anbieter und andere Beteiligte

Der Anbieter kann Metadaten, Verbindungsprotokolle oder Kontoinformationen aufbewahren, ohne verschlüsselte Inhalte zu speichern. Andere Teilnehmer können die Nachricht in einer anderen Darstellung und die ursprünglichen Anhänge besitzen. Die Anforderung bezeichnet Konto, Zeitraum, Felder, natives Format, Zeitzone und Verfahren. Es wird nicht zugesichert, dass eine Plattform Inhalte allein aufgrund einer Anforderung herausgibt; ihre technische Möglichkeit und ihre Antwort werden dokumentiert.

In Mexiko enthält die Ley en Materia de Telecomunicaciones y Radiodifusión von 2025 Regeln zur Aufbewahrung und Herausgabe von Daten für ihre Adressaten und Behörden. Bei der Analyse ist zu prüfen, ob die Anforderung unter dieses Regime fällt und ob es sich um Daten eines Telekommunikationsanbieters, einer Anwendung oder eines anderen Anbieters handelt. Eine Messaging-Plattform wird nicht so behandelt, als seien alle ihre Informationen Telefonie-Verkehrsdaten.[2]

> **Unabhängige Quelle**
> Ein Bildschirmfoto und ein Ausdruck dieses Bildschirmfotos sind keine zwei unabhängigen Beweise. Eine von einer anderen Person empfangene Nachricht, ein Anwendungsexport und ein Sitzungsprotokoll können unterschiedliche Ursprünge und Fehler haben.

[2] Ley en Materia de Telecomunicaciones y Radiodifusión, veröffentlicht am 16-07-2025. Artikel 182 und 183: Anforderungen und Aufbewahrung von Daten, Abfrage in Echtzeit und Übermittlung innerhalb von 48 Stunden je nach Abschnitt. Offizielle Online-Quelle



Abbildung 1. Das Telefon ist eine Ebene, nicht der gesamte Fall. Ein Gespräch kann auf verschiedenen Objekten vorhanden sein. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 3. Isolierung, Stromversorgung und Transport

3.1 Tatsächliche und überprüfte Isolierung

Die Isolierung soll Fernveränderungen und neue Kommunikation kontrollieren. Mobilfunk, WLAN, Bluetooth, NFC, Kabel und Synchronisierung werden geprüft. Das Aktivieren des Flugmodus erfordert eine Interaktion mit dem Gerät und kann Protokolle verändern; Ausschalten kann Sitzungen verlieren; ein Isolationsbehälter kann unwirksam sein, wenn er nicht validiert wurde oder das Gerät versucht, sich erneut zu verbinden. Dokumentiert werden die durchgeführten Maßnahmen und ihre Wirkung.

Ein antistatischer Beutel schützt vor elektrostatischen Entladungen, nicht notwendigerweise vor Hochfrequenzsignalen. Die Bezeichnung Faraday ändert seine Funktion nicht. Die Isolationslösung muss mit sicheren Methoden und unter ähnlichen Bedingungen geprüft werden: Signalarten, Verschluss, Materialien, Entfernung und Zustand des Geräts. Die Prüfung besteht nicht darin, ohne Autorisierung die Nummer einer Person anzurufen; es wird Testequipment verwendet.

Option	Hauptrisiko	Erforderliches Protokoll
Flugmodus	Interaktion, Änderungen an Protokolldaten und verbleibende Verbindungen.	Bildschirm, Handlungen, Uhrzeit und überprüfte Verbindungen.
Ausschalten	Verlust von Speicherinhalten, Sitzung oder Zugriff durch Verschlüsselung.	Begründung, Zustand und Erfassungsmöglichkeiten.
RF-Behälter	Unzureichende oder nicht validierte Isolierung.	Prüfung, Verschluss, Materialien und Bedingungen.
Verbunden lassen	Synchronisierung, Nachrichten oder Fernlöschung.	Notwendigkeit, Kontrolle und Beobachtung.
Stromversorgung	Wärme, Aktivität oder Veränderung des Zustands.	Ladegerät, Kabel und Zweck dokumentiert.

3.2 Verpackung, Transport und Verwahrung

Die Verpackung wird nach ihrer physischen und logischen Funktion ausgewählt: Sie schützt vor Stößen, statischer Elektrizität, Feuchtigkeit und Zugriff und erhält die getroffene Isolierungsentscheidung. Zubehör wird verpackt und zugeordnet. Die Versiegelung enthält Identifikator, Datum und Verantwortlichen; jede Öffnung oder Änderung wird dokumentiert. Ein aktives Gerät wird nicht ohne Kontrolle von Akku und Konnektivität transportiert, wenn dadurch Daten verändert werden können.

Die Beweismittelkette erfasst, wer was zu welchem Zweck, wo, in welchem Zustand und mit welcher Prüfung übergibt und empfängt. Bei einer elektronischen Übertragung werden Berechtigungen, Kanal, Version, Download und Hashwert des entsprechenden Objekts erfasst. Wird die Extraktion einer prüfenden Person übermittelt, wird eine kontrollierte Kopie bereitgestellt und der Zugriff auf Daten Dritter außerhalb des Umfangs beschränkt.

> **Praktische Regel**
> Die Verpackung korrigiert keine schlechte Entscheidung, verhindert aber neue Veränderungen. Auch die Versiegelung beweist nicht die Wahrheit des Inhalts: Sie belegt einen Verschlusszustand innerhalb einer dokumentierten Abfolge.

Kapitel 4. Methoden der Erfassung

4.1 Manuelle Dokumentation und Bildschirmfotos

Die manuelle Prüfung kann nützlich sein, wenn sich die Frage auf ein Gespräch beschränkt oder andere Quellen nicht verfügbar sind. Erfasst werden Anwendung, Version, Gerät, Datum und Zeitzone, Bedienperson, Navigationsweg und angezeigter Inhalt. Eine Bildschirmaufzeichnung schafft visuelle Kontinuität, bleibt jedoch eine Auswahl dessen, was die Oberfläche anzeigt. Sie beweist weder die gesamte Datenbank noch nicht sichtbare Ereignisse.

Vor der Erfassung wird der Umfang festgelegt; andere Chats, Fotos oder Benachrichtigungen sollen nicht unnötig offengelegt werden. Bei einem Export aus der Anwendung bleiben Format, Filter, Anhänge, ursprünglicher Name und Datum erhalten. Die Datei wird als neues Objekt behandelt und dem Gerät zugeordnet. Die Quelle wird nicht umbenannt, bevor sie gesichert wurde.

4.2 Anwendungsexport und Sicherungskopie

Ein Chat-Export kann Text und Anhänge in einer von der Anwendung festgelegten Struktur enthalten. Zu prüfen ist, ob bearbeitete oder gelöschte Nachrichten, Reaktionen, Zitate, Antworten oder Verweise enthalten sind und wie Daten und Teilnehmer dargestellt werden. Eine Sicherungskopie kann einen anderen Zeitpunkt abbilden und mit einem separaten Schlüssel verschlüsselt sein. Die verfügbare Funktion wird dokumentiert, ohne Gleichwertigkeit mit einer physischen Extraktion zu behaupten.

Zur Erhaltung des Gesprächs wird der Export durch Bildschirmfotos des Kontexts und Quellen anderer Teilnehmer ergänzt. Sollen nicht enthaltene Ereignisse analysiert werden, wird eine autorisierte Extraktion erwogen. Ein Unterschied zwischen Exporten kann auf Filtern oder Versionen beruhen und nicht automatisch auf Manipulation. Beide Objekte werden mit miteinander verknüpften Identifikatoren aufbewahrt.

4.3 Logische Extraktion, erweiterte Extraktion und Anbieter

Die logische Extraktion erhält zugängliche Dateien oder Datenbanken mithilfe eines kompatiblen Werkzeugs. Eine erweiterte Erfassung kann einen größeren Umfang haben, wenn Gerät und Methode

dies zulassen, erfordert jedoch Schulung, rechtliche Befugnis und Validierung. Der Bericht vermeidet die allgemeine Bezeichnung „vollständige Extraktion“, wenn lediglich bestimmte Partitionen oder Anwendungen erfasst wurden. Fehler, nicht entschlüsselte Objekte und Ausschlüsse bleiben dokumentiert.

Die Erfassung beim Anbieter kann Kontoinformationen oder Protokolle liefern, die nicht auf dem Telefon vorhanden sind. Anzufordern sind Felder, Zeitzone, natives Format, Verfahren und Feldverzeichnis. Die empfangene Datei wird der EML-Datei und gegebenenfalls der Integritätserklärung zugeordnet. Der Anbieter besitzt möglicherweise keine verschlüsselten Inhalte oder wendet andere Aufbewahrungsfristen an; seine Antwort wird nicht als universeller Telefonie-Verkehrsdatensatz dargestellt.[34]

4.4 Validierung von Werkzeug und Ausgabe

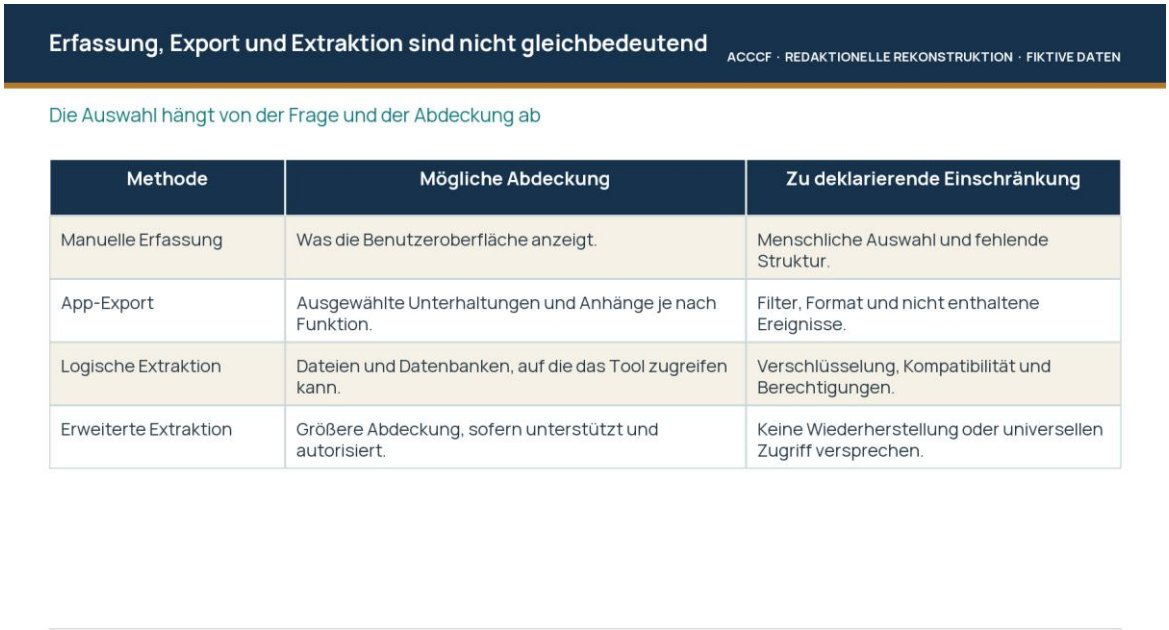
Ein Gerät oder Datensatz mit bekannten fiktiven Daten wird verwendet, um zu prüfen, ob das Werkzeug die erwarteten Objekte erzeugt, Datumsangaben, Teilnehmer und Anhänge richtig interpretiert und die Quelle nur im dokumentierten Umfang verändert. Name, Version, Umgebung, Lizenz, Konfiguration und Ergebnis werden erfasst. Eine Aktualisierung kann das Verhalten ändern und erfordert eine erneute Validierung.

Die Ausgabe wird geöffnet und mit einer ausgewählten sichtbaren Quelle verglichen: einem Kontrollgespräch, einer Datei, einem Datum oder einer Sequenz. Nicht dekodierte Objekte werden gekennzeichnet und nicht ausgeblendet. Erzeugt ein zweites Werkzeug eine andere Darstellung, wird der Unterschied dokumentiert und bewertet, welche Darstellung die Frage besser beantwortet. Das Werkzeug wird nicht zum Zeugen; es ist Bestandteil der Methode.

> **Abnahmekriterium**
> Eine Erfassung ist abgeschlossen, wenn die Ausgabe geöffnet und dem Gerät zugeordnet werden kann, ihr Umfang beschrieben ist, Vorkommnisse erhalten bleiben und eine nachvollziehbare Überprüfung möglich ist. Sie ist nicht abgeschlossen, nur weil das Programm „100 %“ anzeigt.

[3]RFC Editor. RFC 5322, Internet Message Format: Struktur der Nachricht, Kopfzeilen und Nachrichtentext. Diese technische Referenz dient der Aufbewahrung und dem Verständnis von E-Mails; sie ist kein automatischer Beweis für die Identität eines Menschen. Offizielle Online-Quelle

[4]NIST SP 800-101 Rev. 1. Leitfaden zur forensischen Analyse mobiler Geräte: Erhaltung, Erfassung, Untersuchung, Analyse, Validierung und Berichterstattung. Die Technologie und die konkreten Fähigkeiten müssen am aktuellen Gerät und Werkzeug geprüft werden. Offizielle Online-Quelle



Erfassung, Export und Extraktion sind nicht gleichbedeutend

ACCCF · REDAKTIONELLE REKONSTRUKTION · FIKTIVE DATEN

Die Auswahl hängt von der Frage und der Abdeckung ab

Methode	Mögliche Abdeckung	Zu deklarierende Einschränkung
Manuelle Erfassung	Was die Benutzeroberfläche anzeigt.	Menschliche Auswahl und fehlende Struktur.
App-Export	Ausgewählte Unterhaltungen und Anhänge je nach Funktion.	Filter, Format und nicht enthaltene Ereignisse.
Logische Extraktion	Dateien und Datenbanken, auf die das Tool zugreifen kann.	Verschlüsselung, Kompatibilität und Berechtigungen.
Erweiterte Extraktion	Größere Abdeckung, sofern unterstützt und autorisiert.	Keine Wiederherstellung oder universellen Zugriff versprechen.

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

Abbildung 2. Bildschirmfoto, Export und Extraktion sind keine Synonyme. Die Auswahl hängt von der Fragestellung und dem Erfassungsumfang ab. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 5. Untersuchung von Gesprächen und Inhalten

5.1 Gesprächsverlauf rekonstruieren, nicht nur den einzelnen Satz

Sofern in der Quelle vorhanden, werden Teilnehmer, Identifikatoren, zitierte Nachrichten, Antworten, Anhänge, Reaktionen, Bearbeitung, Löschung sowie Sende-, Empfangs- und Lesezeitpunkte analysiert. Ein Bildschirmfoto kann die Nachricht verbergen, auf die geantwortet wurde. Die Abfolge wird mit den Identifikatoren der Quelle dokumentiert, nicht mit einer erfundenen Nummerierung, die eine unbewiesene Kontinuität suggeriert.

Das Gespräch wird mit dem Kontext abgeglichen: Anrufe, Dateien, Kontakte, Anwendungsaktivität, ungefährer Standort, E-Mail und Zeugenaussagen. Die Interpretation eines Satzes erfordert Kenntnisse über Sprache, Beziehung, Ereignisse und Abfolge. Ein „Ja“ kann sich auf eine andere Frage beziehen, wenn die zitierte Nachricht fehlt. Die Analyse ergänzt den Sinn nicht durch Vermutungen.

5.2 Bearbeitete, gelöschte und weitergeleitete Nachrichten

Die Kennzeichnung „bearbeitet“ weist einen sichtbaren Zustand aus, nicht den früheren Inhalt. Die Kennzeichnung „gelöscht“ beweist weder, dass alle Spuren verschwunden sind, noch dass der Grund das Verbergen war. Eine Weiterleitung kann eine zusätzliche Herkunftsebene einführen. Verfügbare Protokolle, Kopien, andere Teilnehmer und Sicherungskopien werden geprüft, ohne die Wiederherstellung des früheren Texts zu versprechen.

Beobachtung	Mögliche Bedeutung	Erforderliche Elemente für weitergehende Schlussfolgerungen
Bearbeitet	Nachträgliche Änderung in der Anwendung.	Versionen, Protokolle oder Teilnehmer mit dem früheren Inhalt.
Für alle gelöscht	Anzeige der Löschung im Client.	Umfang der Löschung und verfügbare Kopien.

Beobachtung	Mögliche Bedeutung	Erforderliche Elemente für weitergehende Schlussfolgerungen
Weitergeleitet	Inhalte, die von einer anderen Nachricht übertragen wurden.	Ursprung und ursprüngliches Datum, sofern verfügbar.
Kein Dateianhang	Anhang nicht heruntergeladen, abgelaufen oder nicht enthalten.	Protokoll, Link, anderer Teilnehmer oder Kopie.
Abweichende Uhrzeit	Zeitzone, Uhr, Umrechnung oder Bearbeitung.	Ursprünglicher Wert und Konfiguration der Quelle.

5.3 Anhänge, Miniaturansichten und Metadaten

Der Dateianhang wird separat aufbewahrt und der Nachricht zugeordnet. Seine Miniaturansicht kann zu einer anderen Version gehören; sein Name kann sich beim Herunterladen ändern. Interne Metadaten, Inhalt, Größe, Format und Systemdatum werden geprüft, ohne diese Felder als automatischen Herkunftsnachweis zu behandeln. Die Kopie bei einem anderen Teilnehmer kann eine bessere Qualität oder zusätzliche Informationen enthalten.

Ein Dokument, ein Bild oder eine Audiodatei kann eine gesonderte Prüfung von Originalität und Inhalt erfordern. Die mobile forensische Untersuchung belegt, dass die Datei mit einer Nachricht oder einem Ordner verknüpft gefunden wurde, nicht dass die dargestellte Szene wahr oder der Absender ihr Urheber ist. Diese Trennung verhindert, dass eine ordnungsgemäße Erfassung für eine übertriebene Schlussfolgerung über den Inhalt verwendet wird.

> **Fiktiver Fall**
> Ein Gespräch enthält eine Drohung und anschließend eine gelöschte Nachricht. Ein anderer Teilnehmer besitzt die spätere Nachricht, eine Klarstellung desselben Autors. Verteidigung und Anklage müssen beide Nachrichten untersuchen. Die Wiederherstellung des Kontexts beweist weder Unschuld noch Schuld; sie verhindert, dass ein einzelner Satz als gesamte Kommunikation interpretiert wird.

Kapitel 6. Zurechnung und Kommunikation

6.1 Konto, Gerät und Person

Die Zurechnung wird anhand von Fragen strukturiert: Welches Konto hat die Nachricht erzeugt oder empfangen, auf welchem Gerät bestand die Sitzung, wer konnte es entsperren, wer kontrollierte die Faktoren, wer sonst hatte Zugriff und welche Aktivität zeigt die Abfolge? Die vertragliche Inhaberschaft eines Anschlusses kann Kontext liefern, beweist aber allein nicht die Nutzung zum fraglichen Zeitpunkt.

Zu berücksichtigen sind Ausleihe, gemeinsame Nutzung, Übertragung, Diebstahl von Zugangsdaten, dauerhafte Sitzungen, Fernzugriff und Verwaltung durch Dritte. Die Verteidigung muss keine dieser Alternativen beweisen, um eine unzureichende Zurechnung aufzuzeigen; die Anklage benötigt eine Grundlage, um sie durch Beweise auszuschließen. Liegt eine starke Übereinstimmung unabhängiger Elemente vor, wird ihr Umfang beschrieben, ohne absolute Gewissheit zu behaupten.

6.2 Chronologie und unabhängige Bestätigung

Der ursprüngliche Wert jeder Datumsangabe, ihre Zeitzone und Genauigkeit bleiben erhalten. Senden, Empfangen, Lesen, Bearbeiten und Erfassen sind unterschiedliche Ereignisse. Das Datum eines Exports ist nicht das Datum der Nachricht. Die Uhrzeit einer Benachrichtigung kann von einer anderen Ebene abhängen. Abweichungen werden anhand des Feldverzeichnisses und der Uhr geprüft, bevor sie als Fälschung dargestellt werden.

Die Bestätigung kann von einem anderen Teilnehmer, einem Sitzungsprotokoll, einer Kopie, einem Beleg, einer Kamera oder einer Sensorsequenz stammen. Die Zahl der Bildschirmfotos wird nicht als Zahl unabhängiger Quellen behandelt. Entscheidend ist, welche Fehler jede Quelle enthalten kann und ob ihre Übereinstimmung alternative Erklärungen ausschließen lässt.

6.3 Bericht mit ausdrücklich abgegrenztem Umfang

Niveau	Belastbare Formulierung	Nicht behaupten
Gegenstand	Das Gerät wurde mit diesen Identifikatoren und diesem Zubehör entgegengenommen.	„Es war das Telefon des Angeklagten“, allein aufgrund des äußeren Erscheinungsbilds.
Erfassung	Das Werkzeug hat diese Dateien und Datenbanken im beschriebenen Umfang erhalten.	„Es wurde alles extrahiert, was vorhanden war.“
Inhalt	Die Nachricht erscheint in der Quelle mit diesem Datum und diesen Teilnehmern.	„Der Inhaber hat sie geschrieben“, ohne Nachweis der Nutzung.
Analyse	Die Quellen sind mit dieser Sequenz kompatibel und haben diese Grenzen.	„Es gibt keine andere Erklärung.“
Fehlende Daten	Das Ereignis wurde im erfassten Bereich und mit den verwendeten Filtern nicht beobachtet.	„Es hat nie existiert.“

Abschluss der Analyse

Eine Person wird nicht aus einer einzigen Kennzeichnung abgeleitet. Die Zurechnung wird gestärkt, wenn unabhängige Quellen ihr hätten widersprechen können und dies nicht tun; sie wird geschwächt, wenn eine dieser Quellen eine andere Möglichkeit belegt.



Abbildung 3. Von einem Konto zu einer Person: Es fehlen Prämissen. Die Zurechnung gewinnt durch unabhängige Quellen an Stärke, nicht durch Adjektive. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Anhang A. Operative Vorlagen

A.1 Entgegennahme des Geräts

Fiktives Protokoll

```
Fall: EXP-DEMO-2026-005
Gerät / ID: DEMO-MBL-003
Marke, Modell und sichtbare Identifikatoren: [Eintrag]
Zustand: [eingeschaltet, Sperrung, Akku, Netz, Schaden]
Zubehör: [Kabel, SIM, Speicher, Hülle, andere]
Übergabe / Entgegennahme: [Rollen, Datum, Zeitzone, Ort]
Frühere Handlungen: [beobachtete und angegebene getrennt]
Rechtliche Befugnis: [Anwendungen, Konten, Zeitraum, Ausschlüsse]
Risiken: [Flüchtigkeit, Löschung, Akku, Datenschutz]
Erste Entscheidung: [Isolierung, Stromversorgung, Eskalation]
Fotografien und Versiegelungen: [Identifikatoren und Zuordnung]
Anmerkungen: [ohne Schlüssel und unnötige Daten]
```

A.2 Inventar von Konten und Quellen

Ebene	Konto / Quelle	Verfügbarkeit und rechtliche Befugnis	Einschränkung
Gerät	[Anwendung und Version]	[Zustand, Zugriff und Umfang]	[Verschlüsselung, Abdeckung]
Konto	[Identifikator]	[Sitzungen, Faktoren und Befugnis]	[Nutzung durch Dritte]
Teilnehmer	[Autorisierter Kontakt]	[Verfügbare Quelle]	[Abweichende Darstellung]
Anbieter	[Dienst und zuständige Stelle]	[Anfrage und Antwort]	[Inhalt oder Aufbewahrungsfristen]
Sicherungskopie	[Datum und Speicherort]	[Schlüssel und Zugriff]	[Momentaufnahme und Umfang]

A.3 Erfassungsprotokoll

Ausgabeprotokoll

```
Quelle und rechtliche Befugnis: DEMO-MBL-003 / [Umfang]
Methode: [manuell, Export, logisch, erweitert, Anbieter]
Gerät, System und Anwendung: [Versionen]
Werkzeug, Version und Validierung: [fiktive Prüfung]
Start-/Enddatum und Zeitzone: [ursprüngliche Angaben]
Aktionen auf dem Gerät: [Interaktionen und Änderungen]
Erhaltene Objekte: [Dateien, Datenbanken, Exporte]
Filter und Abdeckung: [Zeitraum, Konten, Ausschlüsse]
Hashwert und Manifest: [je Objekt]
Vorkommnisse: [Fehler, nicht dekodiert, fehlende Daten]
Überprüfung: [Öffnen, Stichprobe und Revision]
Spätere Verwahrung: [Arbeitskopie und Zugriff]
```

A.4 Zurechnungsmatrix

Behauptung	Unterstützende Quelle	Alternative	Eingeschränktes Ergebnis
Das Konto schickte die Nachricht.	[Eintrag]	[Andere mögliche Sitzung]	[ ]
Das Gerät war aktiv.	[Bildschirm, Protokolle]	[Anderes Datum oder andere Sitzung]	[ ]

Behauptung	Unterstützende Quelle	Alternative	Eingeschränktes Ergebnis
Die Person hat es benutzt.	[Faktoren, Kontext]	[Ausleihe, Diebstahl, Übertragung]	[ ]
Das Gespräch ist vollständig.	[Export]	[Filter und andere Ebenen]	[ ]
Die Datei gehört zum Ereignis.	[Nachricht, Metadaten]	[Weiterleitung oder frühere Bearbeitung]	[ ]

Anhang B. Rechtsrahmen und abschließende Kontrolle

Die Anerkennung elektronischer Dokumente bedeutet nicht, dass jedes Bildschirmfoto authentisch ist oder dass ein Konto eine Person identifiziert. In Mexiko sind CCom 89–94 und 1205, je nach Übergangsregelung das Regime CFPC/CNPCF sowie die LMTR für den jeweiligen Bereich zu prüfen. Peru verteilt Signatur, Verfahren und Archivierung auf unterschiedliche Regeln; Chile unterscheidet Signaturen und Datum; Argentinien gewichtet die Zuverlässigkeit; Kolumbien und Ecuador regeln die Aufbewahrung im Einzelnen; Spanien verbindet eIDAS und LEC. Die Anwendung wird anhand von Fassung, Themenbereich und Rechtsordnung geprüft.[5][6][7][8][9][10][11][12][13][14]

Der Datenschutz begleitet das gesamte Verfahren: Anwendungen, Zeitraum, Konten und Daten Dritter werden begrenzt; Arbeits- und Ausgabeversionen werden getrennt; Nachweise über rechtliche Befugnis und Zugriffe werden aufbewahrt. Ein Bericht veröffentlicht keine Passwörter, privaten Schlüssel, vollständigen Nummern oder Informationen, die weiteren Schaden ermöglichen könnten.[15][16][17]

Abschließende Kontrolle	Prüffrage zur Abnahme
Identität	Stimmen Gerät, Zubehör und Protokolle überein?
Zustand	Wurde die Entscheidung zu Isolierung und Stromversorgung dokumentiert?
Abdeckung	Weist die Extraktion Filter, Einschränkungen und Fehler aus?
Kontext	Bleiben Gesprächsverlauf, Anhänge und andere Ebenen erhalten?

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

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

[7] Ley en Materia de Telecomunicaciones y Radiodifusión, veröffentlicht am 16-07-2025. Artikel 182 und 183: Anforderungen und Aufbewahrung von Daten, Abfrage in Echtzeit und Übermittlung innerhalb von 48 Stunden je nach Abschnitt. Offizielle Online-Quelle

[8] Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung und Zulassung elektronischer Dokumente mit digitaler Signatur. Offizielle Online-Quelle

[9] Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Beweismittel, Beweislast, Beweiswürdigung und Datumsangaben durch technische Mittel. Offizielle Online-Quelle

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

[11] Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz mit beliebigen Mitteln und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren. Offizielle Online-Quelle

[12] 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

[13] 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

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

[15] Mexiko. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, veröffentlichter Text vom 20-03-2025 und Reform vom 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Datenschutzverletzungen und Wahrnehmung von Rechten. Die derzeitige Bundesbehörde ist die Secretaría Anticorrupción y Buen Gobierno. Offizielle Online-Quelle

[16] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 vom 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Vorgaben, Risiken und Vorgehen bei Vorfällen. Offizielle Online-Quelle

[17] Europäische Union. Verordnung (EU) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Vorgaben, Auftragsverarbeiter, Sicherheit sowie Meldung/Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten. In Spanien sind außerdem die einschlägigen nationalen und sektoriellen Rechtsvorschriften zu prüfen. Offizielle Online-Quelle

Abschließende Kontrolle	Prüffrage zur Abnahme
Zurechnung	Sind Konto, Gerät und Person getrennt?
Datenschutz	Wurden Daten außerhalb des Auftrags ausgeschlossen?
Überprüfung	Kann eine andere Person das Objekt auffinden und überprüfen?

Fazit

Das Telefon kann einen entscheidenden Teil der Tatsachen speichern. Die Methode entscheidet, ob dieser Teil verstanden werden kann, ohne einen Bildschirm zu einer Anklage zu machen.