ACCCF / Applied Knowledge Library

05

VOLUME

**Device, application, account, and provider**

Spanish edition · 2026

# Cell Phone and Instant Messaging Forensics Manual

## Receipt, isolation, acquisition, analysis, context, and responsible attribution

Examine mobile communications without confusing a screenshot with the source, an extraction with a full acquisition, or an account with the person who used it.

For forensic examiners, first responders, lawyers, investigators, and custodians. The procedure depends on the device, operating system, application, version, encryption, and authority; it does not provide methods for bypassing locks or accessing other people's accounts.

**Editorial coordination: Jocsan Laguna · American Council on Cybersecurity and Forensic Computing**

*General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.*

# Contents

*The visible pagination corresponds to the PDF edition. Word may update this table of contents when the document is opened; headings retain internal navigation.*

**Introduction: the phone does not speak for itself** ..... 3

**Chapter 1. Device receipt and condition** ..... 3

- **1.1 A record another person can reconstruct** ..... 3
- **1.2 Risks of loss and alteration** ..... 4

**Chapter 2. Sources by layer** ..... 4

- **2.1 Device, application, and associated data** ..... 4
- **2.2 Accounts, sessions, and linked devices** ..... 4
- **2.3 Providers and other participants** ..... 5

**Chapter 3. Isolation, power supply, and transport** ..... 5

- **3.1 Effective, verified isolation** ..... 5
- **3.2 Packaging, transport, and custody** ..... 6

**Chapter 4. Acquisition methods** ..... 6

- **4.1 Manual documentation and screenshots** ..... 6
- **4.2 Application exports and backups** ..... 6
- **4.3 Logical, advanced, and provider-based extraction** ..... 7
- **4.4 Tool and output validation** ..... 7

**Chapter 5. Examination of conversations and content** ..... 8

- **5.1 Reconstruct the thread, not just the phrase** ..... 8
- **5.2 Edited, deleted, and forwarded messages** ..... 8
- **5.3 Attachments, thumbnails, and metadata** ..... 9

**Chapter 6. Attribution and communication** ..... 9

- **6.1 Account, device, and person** ..... 9
- **6.2 Timeline and corroboration** ..... 9
- **6.3 Report with explicit scope** ..... 10

**Appendix A. Operational templates** ..... 10

- **A.1 Device receipt** ..... 10
- **A.2 Inventory of accounts and sources** ..... 11
- **A.3 Acquisition log** ..... 11
- **A.4 Attribution matrix** ..... 11

**Appendix B. Legal framework and final checks** ..... 11

# Introduction: the phone does not speak for itself

A cell phone contains conversations, files, sensors, accounts, and traces of activity, but it may also be only a window into a cloud service or other participants. The first question is not which program will open it, but what allegation needs to be tested and which sources can answer it. If the goal is to determine who wrote a message, a photograph of the screen is insufficient: sessions, devices, authentication factors, content, and context are needed.

Mobile analysis varies with the operating system, application, version, encryption, and device state. One extraction may obtain accessible databases; another may be limited to visible files or an export. The word “forensic” does not change the actual coverage. The report must state what was done, what was obtained, and what was excluded, without promising recovery of deleted messages or universal access.

NIST SP 800-101 Rev. 1 organizes the preservation, acquisition, examination, analysis, and reporting of mobile devices, with attention to validation and documentation. It is a methodological guide, not an up-to-date list of each tool's capabilities. Those capabilities must be tested on the specific model and version, using test data and verifiable results.[1]

> **First principle**
> Do not power on, explore, reset, or connect anything out of curiosity. Record the device state and your authority, preserve accessories, and decide what information could disappear before changing anything.

# Chapter 1. Device receipt and condition

## 1.1 A record another person can reconstruct

The record describes the device type, brand, model, visible identifiers, physical condition, power state, lock state, battery level, visible network, date and time zone, people involved, accessories, and prior actions. Do not write a password in the general record. If unlocking is authorized, record the authorization and the secure mechanism for making the credential available. Preserve previous labels and link them to the new identifier.

Photograph the visible screen without interacting with it whenever possible: time, network icons, battery, notifications, and status. The photograph establishes its appearance at that moment, not all its content. Record whether anyone has already opened applications or attempted an extraction. Document an imperfect receipt; do not rewrite it as though the item had arrived intact.

| Field | Fictitious example | Decision it supports |
|---|---|---|
| Device | DEMO-MBL-003 phone, with visible model and serial number. | Identify and compare with records. |
| Status | Powered on, locked, 43 % battery, mobile network visible. | Prioritize preservation and isolation. |
| Accessories | Cable, charger, SIM and case labelled separately. | Preserve access paths and context. |
| Reported history | The owner attempted to export a conversation before delivery. | Separate prior actions from the analysis. |

[1] NIST SP 800-101 Rev. 1. Guide to forensic analysis of mobile devices: preservation, acquisition, examination, analysis, validation, and reporting. Current technology and specific capabilities must be tested on the specific device and tool being used. Official online source

| Field | Fictitious example | Decision it supports |
|---|---|---|
| Authority | Review of a conversation and specified accounts. | Restrict access to third parties and other applications. |
| Decision | Preserve the device state and contact a specialist. | Avoid unauthorized changes. |

### 1.2 Risks of loss and alteration

A device may receive messages, synchronize, be remotely wiped, lock after inactivity, or lose battery power. It may also contain sessions and keys that are lost when powered off. Identify which risk is most urgent and what technical expertise is available to address it. Powering off does not always preserve evidence; keeping a device on does not always constitute analysis. The record must explain the option chosen.

If the priority conversation is available from another participant or the provider, requesting that source may be less intrusive than examining the device. If volatile activity or an encryption key is the priority, authorized live acquisition may be necessary. Occam's razor selects the source with the greatest discriminatory power and the least alteration, not the most sophisticated tool.

> **When to stop**
> Lack of authority, risk of deletion, an unvalidated tool, encryption that is not understood, or danger to a person require pausing and escalating. Exploring to see what appears can alter evidence and expand the scope without permission.

## Chapter 2. Sources by layer

### 2.1 Device, application, and associated data

Device memory may contain application databases, files, thumbnails, logs, protected credentials, caches, and sensor data. Availability depends on the device state and access. An image folder is not equivalent to the entire photo library if synchronization is enabled. A locally deleted message may still exist on another participant's device or in a backup, but it may also be unrecoverable. The analysis cannot guarantee either outcome.

Accessories matter: SIM or eSIM, memory cards, chargers, cables, adapters, cases, documentation, and other synchronized devices. A watch, tablet, or computer may contain notifications or sessions with different information. Inventory them without automatically expanding authority: a connected item does not mean all its content falls within the engagement.

### 2.2 Accounts, sessions, and linked devices

The application may allow multiple sessions, desktop clients, backups, and recovery by email or mobile operator. When available, request the list of linked devices, additions and removals, authentication factors, dates, recovery changes, and session activity. The account name describes a logical association; physical identity requires additional evidence.

An IP address may provide a network lead, but not an address or a person. A phone number may have been recycled or associated with another person during the period. An IMEI identifies a device or configuration in context, not necessarily the person carrying it. Attribution requires convergence and consideration of alternatives: lending, shared use, remote access, session theft, or administration by another person.

## 2.3 Providers and other participants

A provider may retain metadata, connection logs, or account information without retaining encrypted content. Other participants may hold the message in a different representation and have original attachments. The request identifies the account, period, fields, native format, time zone, and process. Do not promise that a platform will deliver content merely because it was requested; record its capabilities and response.

In Mexico, the 2025 Telecommunications and Broadcasting Law contains data retention and disclosure rules for covered entities and authorities. The analysis must establish whether the request falls within that regime and whether the record belongs to a telecommunications provider, an application, or another provider. Do not treat a messaging platform as though all its information were telephone call detail records.[2]

> **Independent source**
> A screenshot and a printout of that screenshot are not two independent pieces of evidence. A message received by another person, an application export, and a session log may have different origins and errors.

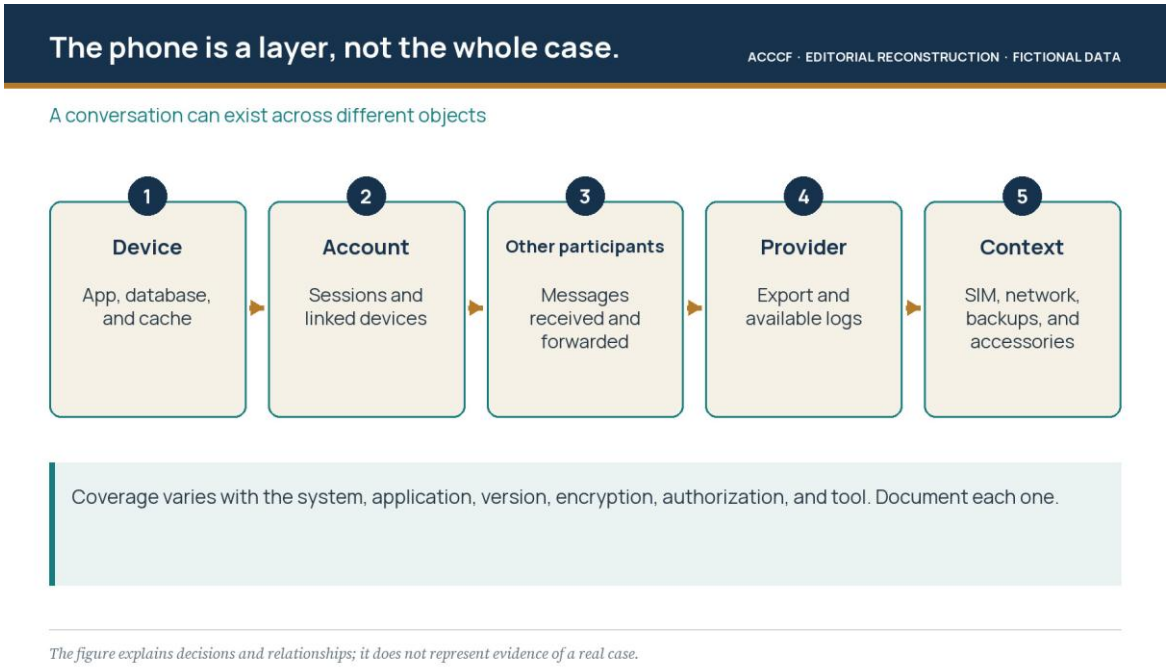



*Figure 1. The phone is one layer, not the entire case. A conversation may exist on different items. Editorial reconstruction; not actual evidence.*

# Chapter 3. Isolation, power supply, and transport

## 3.1 Effective, verified isolation

Isolation seeks to control remote changes and new communications. Assess cellular, Wi-Fi, Bluetooth, NFC, cables, and synchronization. Enabling airplane mode requires interacting with the device and may modify logs; powering off may destroy sessions; an isolation container may be ineffective if it is not validated or if the device attempts to reconnect. Document what was done and its effect.

An antistatic bag protects against electrostatic discharge, not necessarily radio frequency. Calling it Faraday does not change its function. The isolation solution must be tested using safe methods under

[2] Law on Telecommunications and Broadcasting, published on 16-07-2025. Articles 182 and 183: data requests and retention, real-time access, and delivery within 48 hours according to the applicable category. Official online source

similar conditions: signal types, closure, materials, distance, and device state. Testing does not mean calling a person's number without authorization; use test equipment.

| Option | Primary risk | Required record |
|---|---|---|
| Airplane mode | Interaction, log changes, and remaining connections. | Screen, actions, time and verified connections. |
| Power off | Loss of memory, sessions, or access due to encryption. | Justification, state, and acquisition capability. |
| RF container | Insufficient or unvalidated isolation. | Testing, seal, materials, and conditions. |
| Keep connected | Synchronization, messages, or remote wiping. | Need, control and observation. |
| Power supply | Heat, activity, or state alteration. | Charger, cable and purpose documented. |

### 3.2 Packaging, transport, and custody

Packaging is selected for physical and logical functions: protect against impacts, static electricity, moisture, and access, and maintain the chosen isolation state. Package accessories and link them to the device. The seal includes an identifier, date, and responsible party; every opening or change is documented. Do not transport an active device without battery and connectivity controls when these could change data.

The chain records who delivers, who receives, for what purpose, where, in what condition, and with what verification. For an electronic transfer, record permissions, channel, version, download, and the hash of the corresponding item. If an extraction is shared with a reviewer, provide a controlled copy and restrict third-party data outside the scope.

> **Practical rule**
> Packaging cannot repair a poor decision, but it can prevent further alteration. Nor does a seal prove that the content is true: it establishes a closure condition within a documented sequence.

## Chapter 4. Acquisition methods

### 4.1 Manual documentation and screenshots

Manual review can be useful when the question is limited to one conversation or other sources are unavailable. Record the application, version, device, date and time zone, operator, navigation path, and displayed content. Screen recording provides visual continuity but remains a selection of what the interface displays. It does not establish the completeness of the database or events that are not visible.

Before capturing, define the scope and avoid exposing other chats, photos, or notifications. If the application produces an export, preserve the format, filters, attachments, original filename, and date. Hash the file as a new object and link it to the device. Do not rename the source before preserving it.

### 4.2 Application exports and backups

A chat export may include text and attachments in a structure chosen by the application. Check whether it includes edited or deleted messages, reactions, quotes, replies, or references, and how it represents dates and participants. A backup may contain a different snapshot and be encrypted with a separate key. Record the available capability without claiming equivalence to a physical extraction.

When the goal is to preserve the conversation, supplement the export with contextual screenshots and sources from other participants. When the goal is to analyze excluded events, evaluate an authorized extraction. Differences between exports may result from filters or versions, not automatically manipulation. Preserve both objects with related identifiers.

## 4.3 Logical, advanced, and provider-based extraction

Logical extraction obtains accessible files or databases using a compatible tool. Advanced acquisition may provide broader coverage when the device and method permit, but requires training, authority, and validation. The report should avoid the generic label “full extraction” if only certain partitions or applications were covered. Preserve errors, undecrypted objects, and exclusions.

Provider acquisition may provide account information or records not present on the phone. Request fields, time zone, native format, process, and data dictionary. Link the received file to the EML and integrity statement when available. The provider may not hold encrypted content or may apply a different retention policy; do not present its response as universal telephone call detail records.[34]

## 4.4 Tool and output validation

Use a fictitious device or dataset with known data to verify that the tool produces the expected objects, interprets dates, participants, and attachments, and does not modify the source beyond what is documented. Record the name, version, environment, license, configuration, and result. An update may change behavior and requires new validation.

Open the output and compare it with a selected visible source: a control conversation, file, date, or sequence. Mark undecoded objects; do not hide them. If a second tool produces another representation, document the difference and evaluate which better answers the question. The tool does not become a witness; it is a component of the method.

> **Acceptance criterion**
> An acquisition is complete when the output can be opened, linked to the device, described in terms of coverage, retain issues, and allow review with a compatible tool. It is not complete merely because the program displays “100 %”.

[3]RFC Editor. RFC 5322, Internet Message Format: message structure, headers, and body. It is a technical reference for preserving and understanding email, not automatic proof of a person's identity. Official online source

[4]NIST SP 800-101 Rev. 1. Guide to forensic analysis of mobile devices: preservation, acquisition, examination, analysis, validation, and reporting. Current technology and specific capabilities must be tested on the specific device and tool being used. Official online source

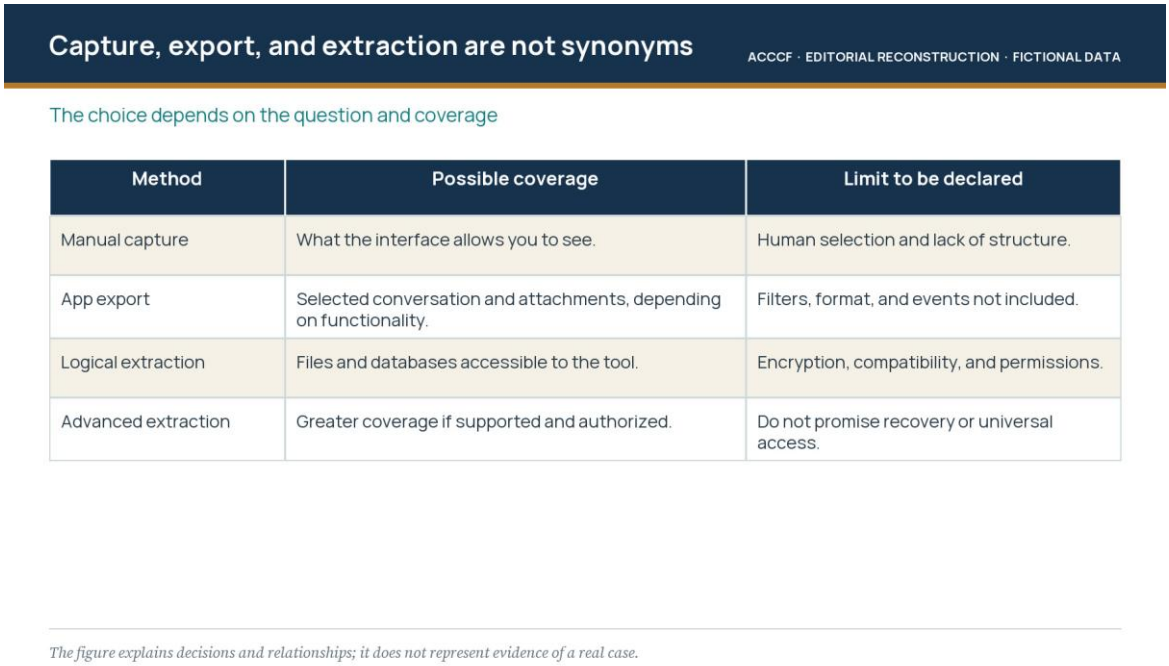



*Figure 2. Screenshots, exports, and extractions are not synonyms. The choice depends on the question and the coverage. Editorial reconstruction; not actual evidence.*

# Chapter 5. Examination of conversations and content

## 5.1 Reconstruct the thread, not just the phrase

Analyze participants, identifiers, quoted messages, replies, attachments, reactions, edits, deletions, and sent, received, and read timestamps when the source contains them. A screenshot can hide the message to which someone replied. Document the sequence using source identifiers, not invented numbering that suggests unproven continuity.

Compare the conversation with its context: calls, files, contacts, application activity, approximate location, email, and testimony. Interpreting a phrase requires language, relationship, events, and sequence. A “yes” may answer a different question if the quoted message is missing. The analysis must not fill in meaning through imagination.

## 5.2 Edited, deleted, and forwarded messages

An “edited” label indicates a visible condition, not the previous content. A “deleted” label does not prove that every trace has disappeared or that the motive was concealment. A forwarded message may add a different layer of provenance. Review available logs, copies, other participants, and backups without promising recovery of the earlier text.

| Observation | What it may mean | What is needed to draw further conclusions |
|---|---|---|
| Edited | Later change in the application. | Versions, logs, or participants with earlier content. |
| Deleted for everyone | Deletion displayed in the client. | Scope of the deletion and available copies. |
| Forwarded | Content forwarded from another message. | Original source and date, if available. |
| No attachment | Attachment not downloaded, expired, or not included. | Log, link, another participant, or copy. |

| Observation | What it may mean | What is needed to draw further conclusions |
|---|---|---|
| Different time | Time zone, clock, conversion, or editing. | Literal value and source configuration. |

### 5.3 Attachments, thumbnails, and metadata

Preserve the attachment separately and link it to the message. Its thumbnail may correspond to a different version; its filename may change when downloaded. Review internal metadata, content, size, format, and file system dates without treating those fields as automatic proof of origin. A copy from another participant may retain better quality or additional information.

A document, image, or audio file may require specific analysis of originality and content. Mobile forensics can establish that a file was associated with a message or folder, not that its scene is truthful or that its author is the sender. This separation prevents a sound acquisition from being used to justify an excessive conclusion about the content.

> **Fictitious scenario**
> A conversation contains a threat followed by a deleted message. Another participant retains the later message, which was a clarification sent by the same author. Both the defense and the prosecution must analyze both messages. Recovering context proves neither innocence nor guilt; it prevents an isolated phrase from being interpreted as the entire communication.

## Chapter 6. Attribution and communication

### 6.1 Account, device, and person

Attribution is organized around questions: which account sent or received the message, which device held the session, who could unlock it, who controlled the authentication factors, who else had access, and what activity the sequence shows. Contractual ownership of the line may provide context, but does not by itself prove use at the relevant time.

Consider lending, shared use, delegation, credential theft, persistent sessions, remote access, and administration by third parties. The defense does not need to prove one of these alternatives to show that attribution is insufficient; the accusation needs evidence to rule them out. If strong convergence exists, describe its scope without jumping to absolute certainty.

### 6.2 Timeline and corroboration

Preserve each literal date, its time zone, and its precision. Sending, receipt, reading, editing, and capture are distinct events. The export date is not the message date. A notification time may depend on another layer. Analyze differences using the data dictionary and clock before presenting them as fabrication.

Corroboration may come from another participant, a session log, a backup, a receipt, a camera, or a sequence of sensor data. Do not count multiple screenshots as though they were independent sources. The question is what error each source could contain and whether their convergence rules out alternative explanations.

## 6.3 Report with explicit scope

| Level | Defensible wording | Do not assert |
|---|---|---|
| Item | The device was received with these identifiers and accessories. | “It was the accused's phone” based solely on appearance. |
| Acquisition | The tool obtained these files and databases within the described scope. | “Everything that existed was extracted.” |
| Content | The message appears with this date and participants in the source. | “The account holder wrote it” without evidence of use. |
| Analysis | The sources are consistent with this sequence and have these limitations. | “There is no other explanation.” |
| Absence | The event was not observed within the coverage and filters. | “It never existed.” |

**Analysis closeout**

A person cannot be inferred from a single label. Attribution grows stronger when independent sources could have contradicted it but did not; it weakens when one source establishes another possibility.

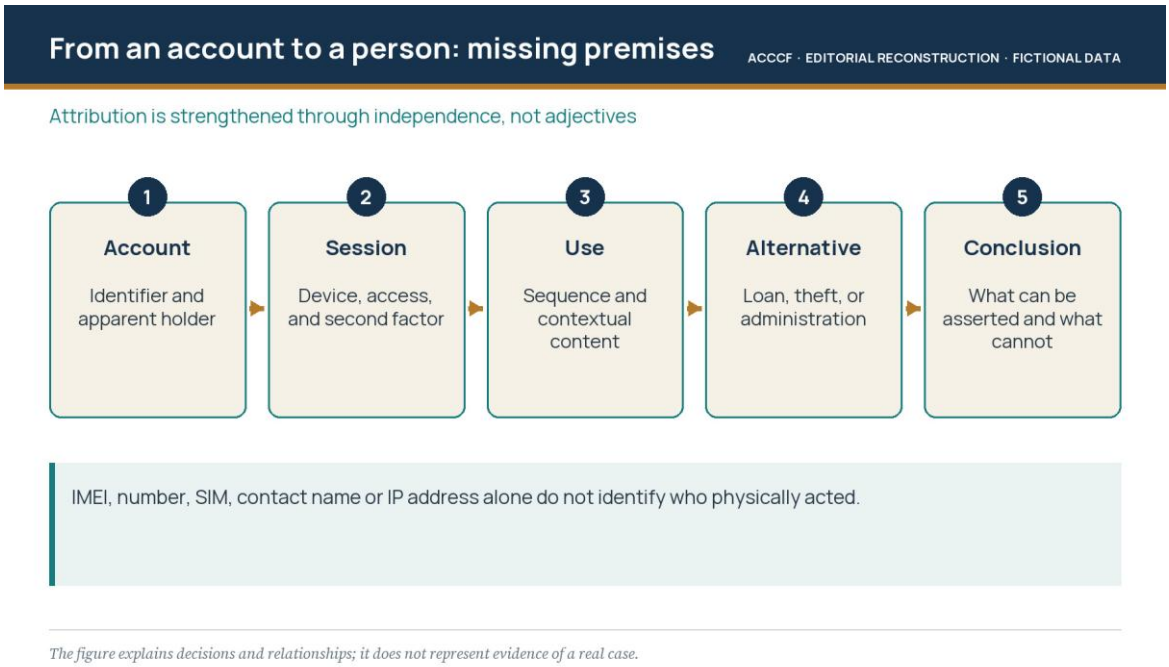



*Figure 3. From an account to a person: premises are missing. Attribution is strengthened by independence, not adjectives. Editorial reconstruction; not actual evidence.*

# Appendix A. Operational templates

## A.1 Device receipt

**Fictitious record**

```
Case: EXP-DEMO-2026-005
Device / ID: DEMO-MBL-003
Brand, model, and visible identifiers: [record]
Condition: [power state, lock state, battery, network, damage]
Accessories: [cable, SIM, memory, case, others]
Delivery / receipt: [roles, date, time zone, location]
Prior actions: [observed and reported separately]
Authority: [applications, accounts, period, exclusions]
Risks: [volatility, deletion, battery, privacy]
Initial decision: [isolation, power supply, escalation]
```

```
Photographs and seals: [identifiers and relationship]
Observations: [no keys or unnecessary data]
```

## A.2 Inventory of accounts and sources

| Layer | Account / source | Availability and authority | Limit |
|---|---|---|---|
| Device | [Application and version] | [Condition, access, and scope] | [Encryption, coverage] |
| Account | [Identifier] | [Sessions, authentication factors, and permission] | [Use by third parties] |
| Participants | [Authorized contact] | [Available source] | [Different representation] |
| Provider | [Service and custodian] | [Request and reply] | [Content or retention] |
| Backup | [Date and location] | [Key and access] | [Snapshot and coverage] |

## A.3 Acquisition log

**Output log**

```
Source and authority: DEMO-MBL-003 / [scope]
Method: [manual, export, logical, advanced, provider]
Device, operating system, and application: [versions]
Tool, version, and validation: [fictitious test]
Start / end date and time zone: [literal values]
Actions on the device: [interactions and changes]
Items obtained: [files, databases, exports]
Filters and coverage: [period, accounts, exclusions]
Hash and manifest: [per item]
Issues: [errors, undecoded items, missing items]
Verification: [opening, sampling and review]
Subsequent custody: [working copy and access]
```

## A.4 Attribution matrix

| Allegation | Supporting source | Alternative | Limited conclusion |
|---|---|---|---|
| The account sent the message. | [Record] | [Another possible session] | [ ] |
| The device was active. | [Screen, logs] | [Different date or session] | [ ] |
| The person used it | [Authentication factors, context] | [Lending, theft, delegation] | [ ] |
| The conversation is complete. | [Export] | [Filters and other layers] | [ ] |
| The file is associated with the event. | [Message, metadata] | [Forwarding or prior editing] | [ ] |

# Appendix B. Legal framework and final checks

Recognition of electronic documents does not imply that every screenshot is authentic or that an account identifies a person. In Mexico, review CCom 89–94 and 1205, the CFPC/CNPCF regime according to the transition, and the LMTR for the relevant domain. Peru separates signature, procedure, and archives; Chile distinguishes signature types and dating; Argentina assesses reliability; Colombia and Ecuador

specify retention; Spain combines eIDAS and the LEC. Apply each source according to its version, subject matter, and jurisdiction.[5][6][7][8][9][10][11][12][13][14]

Data protection applies throughout the procedure: limit applications, period, accounts, and third-party data; separate working and delivery versions; and preserve evidence of authority and access. Reports must not publish passwords, private keys, complete numbers, or information that could facilitate further harm.[15][16][17]

| Final checks | Acceptance question |
|---|---|
| Identity | Do the device, accessories and records match? |
| Status | Was the isolation and power-supply decision documented? |
| Coverage | Does the extraction declare filters, limits and errors? |
| Context | Does the conversation preserve the thread, attachments, and other layers? |
| Attribution | Are the account, device, and person distinguished? |
| Privacy | Were data outside the engagement excluded? |
| Review | Can another person locate and verify the item? |

### Closeout

The phone may hold a decisive part of the facts. The method determines whether that part can be understood without turning a screen into an accusation.

[5] Mexico's Commercial Code, Articles 89–94 and 1205: neutrality, attribution, written form, originality, integrity, accessibility, and admissibility of data messages. Official compilation. Official online source

[6] National Code of Civil and Family Procedure, Articles 348–350. Compilation including the amendment of 15-01-2026. Application is gradual and depends on declarations. Official online source

[7] Law on Telecommunications and Broadcasting, published on 16-07-2025. Articles 182 and 183: data requests and retention, real-time access, and delivery within 48 hours according to the applicable category. Official online source

[8] Peru. IOFE Regulations, DS 052-2008-PCM, Articles 3 and 4: requirement for and admissibility of digitally signed electronic documents. Official online source

[9] Peru. Code of Civil Procedure, Articles 188–197 and 245.5: purpose, legality, means of evidence, burden of proof, evaluation, and dating by technical means. Official online source

[10] Chile. Law 19.799 on electronic documents and electronic signatures, Articles 1–5: equivalence, written form, simple/advanced signatures, dating, and evidentiary value. Official online source

[11] Argentina. Civil and Commercial Code, Articles 318–319: correspondence by any medium and assessment of the reliability of media and technical procedures. Official online source

[12] Colombia. Law 527 of 1999, Articles 5–13, 16–25, and 28: data messages, written form, originals, integrity, admissibility, retention, dispatch, receipt, and digital signatures. Official online source

[13] Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages, Law 67, Articles 2, 6–8, and 10–16: equivalence, written form, originals, retention, provenance, dispatch, receipt, and electronic signatures. Official online source

[14] Spain. Code of Civil Procedure, Articles 326 and 384: private documents, challenges, instruments for storing, accessing, or reproducing data, examination, custody, and sound judicial evaluation. Official online source

[15] Mexico. Federal Law on the Protection of Personal Data in the Possession of Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, data breaches, and the handling of rights requests. The current federal authority is the Secretariat of Anti-Corruption and Good Governance. Official online source

[16] Ecuador. Organic Law on Personal Data Protection, Official Registry Supplement 459 of 26-05-2021. Articles 10 and 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

[17] European Union. Regulation (EU) 2016/679, Articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of personal data breaches. In Spain, applicable national and sector-specific legislation must also be reviewed. Official online source