ACCCF / Applied Knowledge Library

04

VOLUME

Sources, contradictions, and alternative hypotheses

Spanish edition · 2026

Technical defense manual for accusations based on digital evidence

Review of screenshots, conversations, files, location data, reports, and expert reasoning

Examine an accusation without accepting its shortcuts or constructing another convenient narrative: locate the object, verify the method, and delimit what can actually be asserted.

For accused persons, defense lawyers, party-appointed and rebuttal experts, independent reviewers, and teams that need to formulate verifiable technical questions. It does not contain procedural strategies or replace legal analysis of the case file.

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: a clear image can tell an incomplete story 3
Chapter 1. The allegation before the file 3
1.1 Breaking down the allegation 3
1.2 The case file and its coverage 4
Chapter 2. Review of receipt and custody 4
2.1 Identity of the item before its content 4
2.2 Transfers missing from the record 5
2.3 Authority and proportionality 5
Chapter 3. Contradiction matrix 6
3.1 Detect without selecting only what supports your position 6
3.2 Types of contradiction and their effects 6
Chapter 4. Screenshots, conversations, and files 7
4.1 The screenshot as a fragment 7
4.2 Messaging exports and context 7
4.3 Metadata and versions 7
Chapter 5. Reasoning and independent review 8
5.1 Premises and false consequences 8
5.2 Alternative hypotheses and falsification testing 8
5.3 A review that tries to break the report 9
Chapter 6. Reviewing the expert report 9
6.1 Traceability of each conclusion 9
6.2 Useful questions for rebuttal 10
Chapter 7. Integrated case: from allegation to limited conclusion 10
7.1 Available material 10
7.2 Checks and findings 10
7.3 Brief findings report 11
Appendix A. Review template and questions 11
A.1 Claims matrix 11
A.2 List of technical questions 11
A.3 Record of sources requested and received 12
Appendix B. Legal functions for review 12

Introduction: a clear image can tell an incomplete story

A screenshot can seem conclusive because it contains a name, a statement, and a time. A video can seem sufficient because it shows a familiar face. A cell tower can seem like an address when it is drawn as a dot on a map. Technical defense begins by interrupting that automatic inference: what exactly is the item, who produced it, what part of the story does it preserve, what method was applied, and what other explanations remain compatible with it?

Challenging evidence does not mean denying everything. If the hash matches, acknowledge the match; if a source is reliable, explain its scope; if a conclusion is correct, do not attack it for sport. The task is to separate what has been proven from what has been inferred. Sometimes the prosecution's conclusion stands. At other times, a mistaken identification, a date without a time zone, or an incomplete export is enough to show that the reasoning does not hold as presented.

An accused person does not need to invent an alternative story to show that the first one is weak. The reviewer may conclude that the source does not establish the allegation, that coverage is insufficient to rule out other explanations, or that the method cannot identify a person. Precision prevents a defense from becoming a second unsupported accusation.

> **Guiding question**
> What allegation disappears if I remove an unproven premise? That question guides the review of every screenshot, report, record, and conclusion.

Chapter 1. The allegation before the file

1.1 Breaking down the allegation

Write the complete allegation without adjectives: a person, an action, an object, a date, a place, and a consequence. Then separate its components. “The accused sent the message from his home at 21:00” contains at least four questions: does the message exist, was the account associated with him, was the device at that location, and did he use it at that time? A single screenshot may not fully answer any of them.

Record each version separately without treating it as fact. The accusation asserts a sequence; the defense may deny it, acknowledge part of it, or state that it is unknown. The goal is not to blend them into an intermediate version, but to identify sources that can confirm or weaken each element. The first working document is a map of claims and required sources.

Component	Review question	Source that can distinguish
Existence	Is there a message, file, post or record?	Native file, provider, recipient, verified copy.
Integrity	What representation was received, and how did it change?	Original, export, EML, manifest and hash.
Attribution	Account, device, or person? With what evidence?	Sessions, authentication factors, enrollment, context, and use.
Time	What clock, time zone, and event does the date represent?	Literal record, synchronization, and independent sources.

Component	Review question	Source that can distinguish
Location	Is it a coordinate, cell, inference, or testimony?	Precision, azimuth, map, sensors, and corroboration.
Meaning	Does the content prove the narrative or only what is visible?	Thread, sequence, original and alternative explanation.

1.2 The case file and its coverage

Inventory the material received and missing: images, native files, disks, official letters, reports, annexes, exports, videos, audio files, call detail records, logs, and statements. Assign each item an identifier without altering its original name. If an expert report cites an unavailable annex, record that absence before evaluating its conclusion. Do not review a report as though its annexes existed merely by reference.

Coverage describes the period, systems, filters, and items not included. “The phone was analyzed” does not indicate whether all memory, a partition, an application, or selected screenshots were examined. “Communications were examined” likewise does not say whether later messages that change the meaning were excluded. The defense needs the query and the universe examined, not merely the result favorable to one party.

> **Working rule**
> Do not begin by attacking the expert's reputation. Check the object, coverage, and method. A critique of credentials cannot repair a source you have not reviewed.

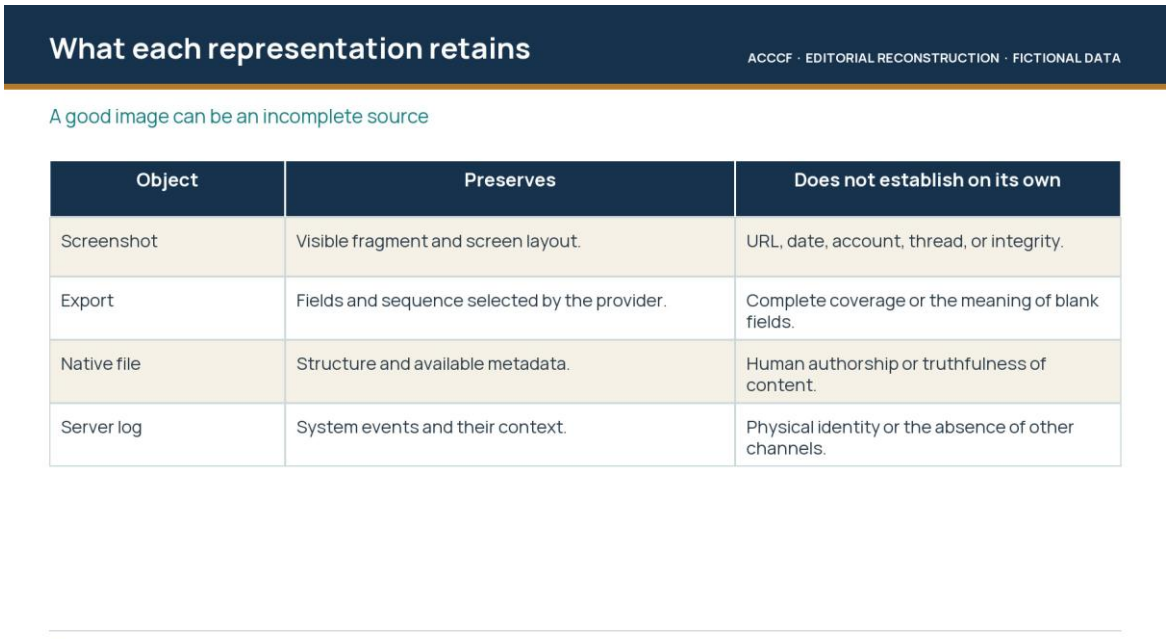


Figure 1. What each representation preserves. A good image can be an incomplete source. Editorial reconstruction; not actual evidence.

Chapter 2. Review of receipt and custody

2.1 Identity of the item before its content

The record must allow the exact item to be identified: type, brand, model, serial number or available identifiers, condition, accessories, packaging, seal, date, and persons involved. A generic disk, an unlabeled memory device, or a phone described differently in two proceedings requires clarification. The

defense asks which item arrived, which was acquired, and which appears in each photograph, without assuming that a difference automatically indicates malicious manipulation.

When an identification inconsistency exists, do not build a conclusion until it is clarified. It may be a transcription error, a different representation, or a genuinely different item. Compare official records, letters, photographs, capacity, format, labels, seals, and center-ring codes on optical discs. Direct the question to the source before the person.

2.2 Transfers missing from the record

The chain of custody must reconstruct access and changes of responsibility: receipt, opening, copying, analysis, transfer, download, and return. If only the final delivery signature exists, there is a period without traceability. This does not prove alteration, but it limits what can be said about who could have changed the item and under what conditions.

For digital files, preserve the complete channel: EML, headers, body, attachments, link, permissions, version, and download. A hash calculated on receipt controls integrity from that point onward, not retroactively to creation. If the provider writes the hash in the body, verify and preserve the relationship. If a report merely copies a value without an item, algorithm, or date, its meaning is limited.

Custody question	Expected evidence	Conclusion not to draw prematurely
Is it the same object?	Identifiers, photographs, seals, and matching official records.	“The record says the same thing, so everything is valid.”
Who could access it?	Events, roles, location, purpose, and date.	“Only the expert had contact.”
What copy was analyzed?	Relationship to the original, image, export, and working copy.	“The copy is bit-for-bit because the report says so.”
What changed during export?	Filters, time zone, format, fields, and limitations.	“The PDF is equivalent to the complete database.”
What is unknown?	Missing periods, actions, and sources.	“The absence of a record proves forgery.”

2.3 Authority and proportionality

The defense reviews who authorized access, what actions it permitted, and whether any exclusions applied. A voluntarily provided password may authorize a specific query, not indiscriminate copying of an entire digital life. A company device may contain personal or third-party information. The ability to open a file does not by itself establish permission to use it for any purpose.

The review does not invite a repeat intrusion. If the case file does not provide access to a source, request it through the appropriate channel. Defense personnel must not log into third-party accounts to “verify” them or install tools on third-party devices. Technical defense also protects against further harm to privacy.

> **Outcome of this stage**
> A table listing item, status, identity, authority, transfers, representations, and gaps. The next stage analyzes contradictions on that basis, not from memory.

Chapter 3. Contradiction matrix

3.1 Detect without selecting only what supports your position

The matrix includes facts compatible with the accusation and with other explanations. Each row contains the allegation, item, literal value, method, contradiction, possible explanation, and outstanding test. Do not label a contradiction “false” before reviewing clocks, formats, fields, coverage, representations, and transcription. Some differences are explainable; others prevent a conclusion.

A result may confirm one part of an allegation and weaken another. An EML can establish that the received attachment matches the one declared by the provider, but not that the attachment's content is true. A video can be technically original and show a staged scene. A date can be consistent and still not correspond to the alleged event. The review preserves these distinctions.

Allegation	Check	Possible outcome
“The file never changed”	Hash, algorithm, time, and relationship to the source.	Matches from receipt onward; earlier history unknown.
“The conversation is complete”	Export, thread, participants and filters.	Visible fragment; coverage not established.
“The photo was taken at 20:42”	Metadata, clock, time zone, and sequence.	Internal date compatible with another time, or uncertain.
“The cell tower locates the accused”	Cell, technology, coverage, and device.	Network association; not a person or address.
“The expert analysis proves authorship”	Sources, method, alternatives and premises.	Associated account; physical identity unestablished.

3.2 Types of contradiction and their effects

An identity contradiction asks whether the same item is involved; a source contradiction asks whether the representation supports the allegation; a method contradiction asks whether the query can produce that result; a time contradiction asks whether clocks and time zones are compatible; and an inference contradiction asks whether the conclusion follows from the premises. They do not all carry the same weight or invalidate the case file. The report explains the specific effect on each allegation.

Absence of evidence must also be distinguished from evidence of absence. A record missing from an export may be significant if the source is complete for the period and filters, but it does not prove that the event did not occur through other channels. This distinction prevents a provider limitation from becoming absolute proof for either the defense or the accusation.

> **Review test**
> Does the contradiction change the item's identity, coverage, timeline, or conclusion? If it changes none of these, it may be a difference in presentation. If it changes one, formulate the technical question needed to resolve it.

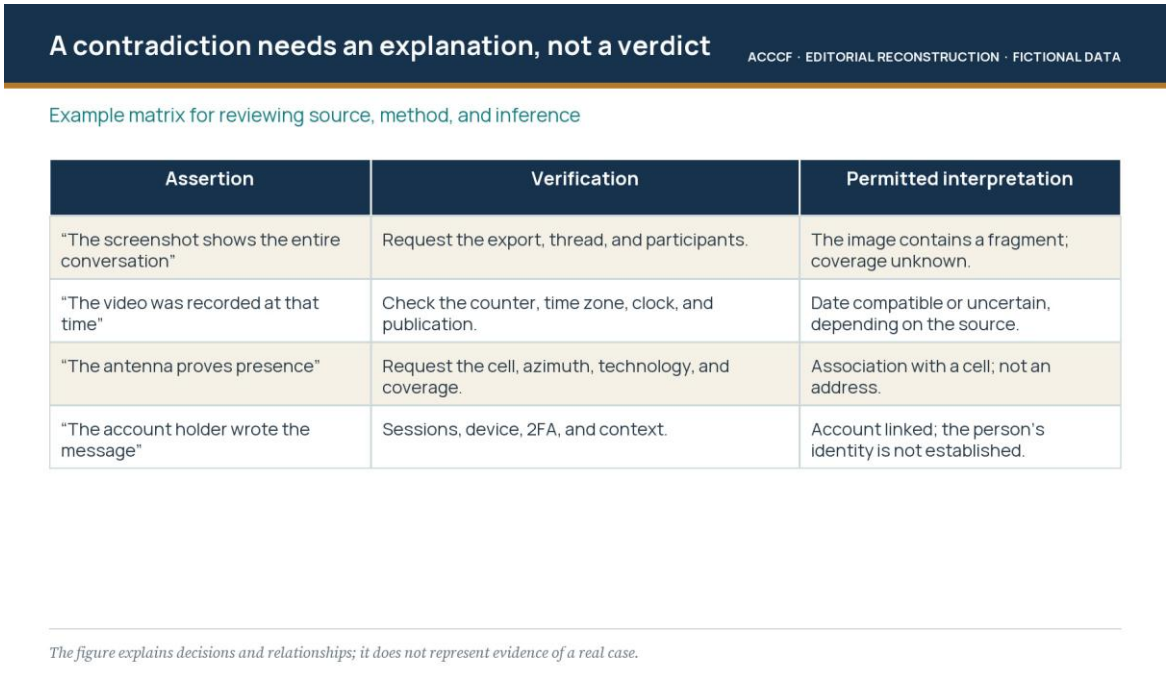


Figure 2. A contradiction requires an explanation, not a verdict. Example matrix for reviewing source, method, and inference. Editorial reconstruction; not actual evidence.

Chapter 4. Screenshots, conversations, and files

4.1 The screenshot as a fragment

Describe exactly what is visible and what is absent: URL, application, version, account, date, time zone, device, participants, earlier and later messages, attachments, and reactions. A screenshot may usefully show a fragment, but does not by itself prove completeness, creation date, or authorship. Request the native file, the application export, the message from another participant, or the provider's records.

When only a screenshot exists, limit the conclusion. Do not claim it was fabricated because of differences in alignment, compression, or format: those artifacts may originate in the application or the screenshot process. Seek an earlier source and document who produced it, when, and with what tool. If no access is available, the uncertainty remains.

4.2 Messaging exports and context

An export may contain text and files selected by the user or by the application's export function. It is not necessarily equivalent to the database or to every event: edits, deletions, reactions, blocks, and linked devices may have different coverage. Request the data dictionary, version, date, and filters. If messages rely on end-to-end encryption, the provider may not retain their content; this does not prevent review of other layers.

Compare the sequence with messages received by other participants and with records from linked devices. A reaction or later message may change the meaning of a statement without proving the earlier one false. The defense must not crop the conversation to produce the opposite effect: request sufficient context and explain what remains ambiguous.

4.3 Metadata and versions

Date, author, application, and device fields have different producers and meanings. The file system creation date may be the copy date; the author may come from a configuration setting; the device model may come from an application that rewrote the file. Compare internal metadata, file system properties,

thumbnails, version history, cloud copies, and filename sequences. A metadata field is a verifiable lead, not infallible testimony.

Data	Initial hypothesis	Alternative to be tested
Document author	The named person wrote it.	Shared account, template, another editor, or configuration.
Creation date	The file was created at that time.	Copying, downloading, conversion, or a different clock.
IMG_0042	It belongs to a continuous sequence.	Importing, renaming, sequence restart, or missing files.
Email account	The account holder wrote the text.	Session, delegation, theft or drafting by a third party.
EXIF location	The person was at the exact spot.	Precision, editing, inheritance, or synchronization.

Fictitious scenario

A screenshot shows a threat at 21:03. The native file and the message received by another participant show 20:03 UTC, which corresponds to a different local time. The difference does not prove fabrication: it reveals a conversion omitted from the accusation. The review corrects the timeline and preserves the content for analysis in context.

Chapter 5. Reasoning and independent review

5.1 Premises and false consequences

A syllogism helps reveal what is missing. Major premise: a cell record establishes a network association under certain conditions. Minor premise: the record associates an event with cell A. Valid conclusion: that documented association exists. It does not follow that the subscriber was at an address or was carrying the phone. That requires additional premises about location, device, and use.

A false consequence arises when a small truth is used as a passport to a larger one: the signature verifies, therefore all content is true; the account belongs to a person, therefore that person wrote it; the file is intact, therefore it has been original since creation; the expert is renowned, therefore the conclusion is scientific. Each leap requires an additional premise and a test.

5.2 Alternative hypotheses and falsification testing

Formulate at least two plausible explanations and a test capable of weakening them. If a file is alleged to be newly created, review version history and backups; if the account holder is alleged to have used it, review sessions and the second factor; if manipulation is alleged, compare the original and references. Do not adopt an alternative because it is convenient: evaluate it by the same standard as the accusation.

Hypothesis A	Hypothesis B	Test that distinguishes them
Document created on the day of departure	Earlier document copied or edited later.	Version history, backup and activity.
Account used by its holder	Account used by another person or a persistent session.	Factors, device, concurrent access and control.
Edited video	Original video of a staged scene.	Structure, references and recording circumstances.

Hypothesis A	Hypothesis B	Test that distinguishes them
Conflicting location	Sources with different precision or time zones.	Metadata, cell, clock and independent sensors.

5.3 A review that tries to break the report

The independent reviewer does more than correct style. They locate each item, repeat queries, compare values, seek missing annexes, and look for explanations the analyst did not consider. They also review material favorable to the accusation to avoid creating a biased defense. Observations are answered with sources and changes, not personal authority.

NIST SP 800-86 and ISO/IEC 27037 provide frameworks for collection, preservation, examination, analysis, and reporting. They do not guarantee that a conclusion is true: they make it possible to ask whether the process was documented and whether another person can reproduce it. Prestige is no substitute for reviewability.[12]

> **Independence principle**
> The best time to identify a weak premise is before delivery. If a report must hide a source or an alternative to hold up, it needs further analysis, not better rhetoric.

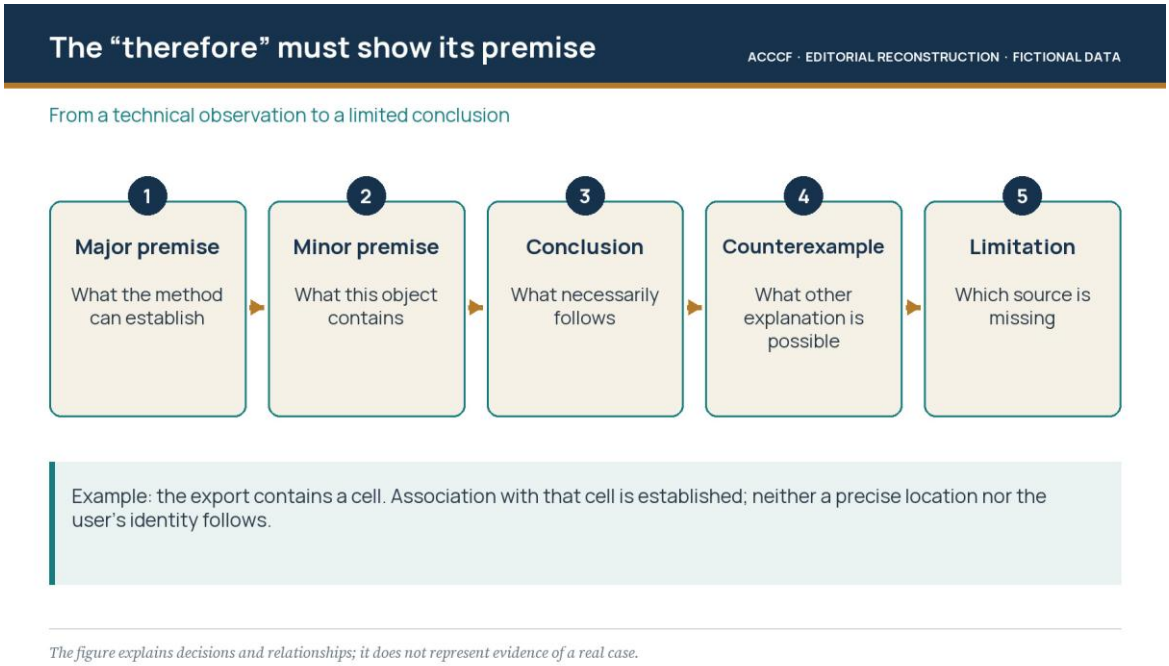


Figure 3. "Therefore" must reveal its premise. From a technical observation to a limited conclusion. Editorial reconstruction; not actual evidence.

Chapter 6. Reviewing the expert report

6.1 Traceability of each conclusion

Trace each conclusion backward: conclusion → finding → query → item → acquisition → source → authority. If a link is missing, identify which allegation must be limited. Bibliography pages cannot

[1]NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodological guidance, not legislation or a guarantee of admissibility. Official online source

[2]ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed as current by ISO. Official online source

replace that path. A technical standard may be valid without proving that it was applied to the correct item.

Distinguish documentary facts, technical results, inferences, and legal opinions. The expert can explain what they did and observed; they do not need to declare guilt or the outcome of the proceedings. Separate legal opinions from findings so that their evaluation does not contaminate the technical review.

Text level	Review example	Pending question
Receipt	The EML arrived with two attachments.	Is it preserved in full with its identifiers?
Result	The attachment matches the declared hash.	What does that prove about content and origin?
Inference	The delivery retains verification of integrity.	From what point in time, and with what limitations?
Conclusion	The record is consistent with a verifiable delivery.	Can identity or truthfulness be asserted?
Legal opinion	The party is responsible.	Is this within the expert's role, and what premises does it rely on?

6.2 Useful questions for rebuttal

Questions should elicit a verifiable answer, not deliver a speech: which item produced the data, what tool version was used, what filters were applied, which fields are empty, what time zone was used, which source ruled out a hypothesis, and which limitations prevent attributing an action to a person. If the answer is “the expert's experience,” request the specific record.

Also ask what would change the conclusion. If no source could change it, the method may not be falsifiable. A robust report states which data support its conclusion and which could weaken it. This does not make it less firm; it makes it testable.

> **Central question**
> Can someone who does not share the initial account locate the item, repeat the method, and reach a compatible result? If not, the conclusion depends on an explanation that the case file does not allow others to review.

Chapter 7. Integrated case: from allegation to limited conclusion

7.1 Available material

A fictitious case contains a conversation screenshot, a video downloaded from a platform, call detail records in PDF, and a report asserting presence and authorship. The accused acknowledges the account but denies writing the message and identifies another location. Neither the native video file nor the EML for the call detail records is yet available. The first deliverable is not an extensive rebuttal expert report: it is an inventory of missing sources.

7.2 Checks and findings

The conversation export shows later messages that change the meaning of the fragment without deleting the initial message. The video has undergone platform conversion, so the camera original is requested to

assess continuity. The EML for the call detail records allows the attachment to be verified, but the data dictionary indicates that the cell represents a network association, not a user coordinate. The accusation report had combined three distinct allegations into one.

The review does not conclude that everything is false. It concludes that the message exists, the initial context was incomplete, the video does not yet support a conclusion of originality, and the call detail records do not establish an address or who was carrying the device. These conclusions are useful because they delimit what can be challenged on a sound basis and what requires another source.

7.3 Brief findings report

Example of technical conclusion

```
1. Screenshot EV-01 contains the visible fragment of the message but does not establish its completeness, physical authorship, or generation date. Subsequent export EV-04 provides adjacent messages that must be considered when interpreting the content.

2. File EV-02 is a platform download. Its structure may be consistent with legitimate conversion; without the camera original and a comparable reference, no conclusion on originality is issued.

3. Call detail record EV-03 associates the event with cell DEMO-A17. The data dictionary contains no measurements that permit a precise location. The source does not establish an address or who was carrying the device.

4. The assertion of physical authorship requires additional evidence of the session, device, authentication factors, and context. The result does not establish general falsity or the absence of other events outside the reviewed coverage.
```

Lesson

Technical defense can be precise without promising acquittal. Its strength lies in showing exactly which part of an accusation does not follow from the source.

Appendix A. Review template and questions

A.1 Claims matrix

Field	Required content	Fictitious example
Literal allegation	Text without interpretation or adjectives.	“The person wrote at 21:03.”
Item and source	Identifier, representation, and provenance.	Screenshot EV-01; native file pending.
Premises used	What must be true to sustain the allegation.	Account = person; displayed time = local time.
Check	Method, filters, tool and coverage.	Export, sessions and dictionary.
Contradiction	Literal value that does not fit and possible causes.	Message with a different UTC time zone.
Limited conclusion	What is established and what is not.	The message exists; physical authorship is not established.
Outstanding source	What can change the outcome and how it is requested.	Session and participant records.

A.2 List of technical questions

Guide to conducting a review

```
1. What is the exact item, and where is its native representation?
2. Which query produced the finding, and what coverage did it have?
3. Which fields were excluded, filtered out, or left empty?
```

```
4. What do the date, time zone, and precision mean?
5. What other explanation is compatible with the same finding?
6. What source could weaken the main hypothesis?
7. Is the corroboration independent, or does it repeat the same file?
8. What premise supports the inference from account to person?
9. What part of the conclusion is technical and what part is legal?
10. What limitations prevent further assertions?
```

A.3 Record of sources requested and received

Request	Receipt and checks	Status
Native conversation file and export	EML, attachments, hash, filters and dictionary.	[pending / received / limited]
Original file and video references	Item, tool, version, date, and method.	[ ]
Native call detail records and dictionary	Fields, time zone, cell, coverage, and EML.	[ ]
Account sessions and authentication factors	Enrollment, devices, access and recovery.	[ ]
Annexes to the contested report	Relationship to citations and reproducible queries.	[ ]

Appendix B. Legal functions for review

Technical review connects with rules on recognition, integrity, originality, attribution, and evaluation. Admission does not equate to full proof, and a presumption of signature does not establish every fact. Sources must be analyzed in their jurisdiction, subject matter, and version; this guide does not replace the defense's procedural analysis.

Jurisdiction	Relevant documentary function	Application to the defense
Mexico	CCom 89–94 and 1205; CFPC 210-A / CNPCF 348–350, depending on the transition.	Method reliability, attribution, integrity, and accessibility; review the regime currently in force.
Peru	IOFE Regulations; CPC 188–197 and 245.5; sector-specific archival regulations.	Burden of proof, legality, typical/atypical means of evidence, and dating by technical means.
Chile	Law 19.799, Articles 1–5.	Signature types, dating, and distinct evidentiary values.
Argentina	Law 25.506; CCyC 318–319; Decree 182/2019.	Reliability of media, correspondence, and limited presumptions.
Colombia	Law 527, Articles 5–13, 16–25, and 28; CPACA where applicable.	Originality, retention, context, admissibility, and evaluation.
Ecuador	Law 67, Articles 2, 6–8, and 10–16, and its Regulations.	Integrity, retention, provenance, and signature effects.
Spain / EU	eIDAS 25–26 and 46; LEC 326 and 384; Law 6/2020.	Challenges, custody, examination, and evaluation; do not cite Law 59/2003 as being in force.

Sources for the table:[3,4,5,6,7,8,9,10,11,12,13,14]

Closeout

Reviewing does not mean manufacturing doubt. It means requiring every allegation to have a source, a method, and a conclusion that does not exceed what has been proven.

[3]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

[4]Federal Code of Civil Procedure, Article 210-A: method reliability, attribution, accessibility, and integrity of electronic information. Code repealed by decree dated 07-06-2023, subject to a gradual transition regime. Official online source

[5]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

[6]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

[7]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

[8]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

[9]Argentina. Digital Signature Law 25.506, Articles 1 and 5–9: digital documents, the burden on a party invoking an unrecognized electronic signature, and limited presumptions. Official online source

[10]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

[11]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

[12]Regulation (EU) 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination against electronic signatures and documents based on their format, advanced signatures, and the legal effects of qualified signatures. Official online source

[13]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

[14]Spain. Law 6/2020 on electronic trust services: repeal of Law 59/2003 and Article 25 of the LSSI; the previous regime is not cited as being in force. Official online source