COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

The Missing Evidence Problem

Proving What Should Exist, Finding Where It Went, and Litigating the Gap

Every litigator meets the gap: the email chain that stops the week the dispute began, the phone "lost" before imaging, the CCTV overwritten days after the incident, the folder that is simply not in the production. Missing evidence is not the absence of a forensic question; it is the forensic question: whether the material ever existed, whether its absence is innocent (retention policies, device refreshes, routine rotation) or engineered (deletion, wiping, convenient loss), where surviving copies and traces may still be found, and what a court can be asked to infer. This guide gives UK lawyers the method: the evidence-of-absence toolkit that distinguishes gap from destruction, the recovery map across duplicates, backups, counterparties and logs, the preservation-duty framework that turns destruction into consequences, and the practical litigation of spoliation: from disclosure applications to adverse inference.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. A substantial share of its instructions begin with a gap: material a party says is gone, material an opponent's production conspicuously lacks, or material a client fears was destroyed. The laboratory's examiners reconstruct what happened to it: existence evidence, deletion artefacts, recovery routes and the honest statement of what cannot be known: and report under CPR Part 35 when the gap itself goes to trial.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | DELETION & WIPING ANALYSIS | RECOVERY ROUTE MAPPING | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: MISSING EVIDENCE IS INVESTIGATED IN THREE MOVES: PROVE IT EXISTED, EXPLAIN ITS ABSENCE, AND PURSUE IT WHERE IT STILL SURVIVES: WITH THE LITIGATION CONSEQUENCES FLOWING FROM WHAT THOSE MOVES ESTABLISH

Existence first: before anything can be "missing", its prior existence is evidenced: from references in surviving material (replies quoting the vanished email, thread structures with absent hops per guide 83), from system records (file tables, sync logs, message counters per guides 51-66), from counterpart copies, and from the metadata lattice of guide 87 that dates and places what is no longer there. **Cause second:** absence has a spectrum: retention policies that ran as designed, device refreshes and departures (guide 87's created-date cliffs), platform rotation (CCTV loops, log retention): through negligence after a preservation duty arose: to engineered destruction, which leaves its own artefacts: deletion timestamps clustered after the letter of claim, wiping-tool signatures, empty-but-recently-full containers, accounts purged in patterns no policy explains. The distinction is forensic work with legal consequences at every point on the spectrum. **Recovery third:** this series' whole architecture is a recovery map: duplicates in other custodians (guide 82), thread instances (guide 83), backups and archives, cloud versions and recycle mechanisms (guides 51-58, 75), counterparty and third-party holdings, and the logs that survive the content they describe. What the map yields is pursued through disclosure machinery; what it cannot yield becomes the gap the court is asked to weigh: with adverse inference, specific disclosure, costs and (in the gravest cases) strike-out or contempt on the menu, driven by the quality of the existence-and-cause evidence assembled here.

- **Existence is provable without the document:** references, records and residue: the vanished item's outline drawn from what survives.
- **Absence has a forensic signature:** innocent loss and engineered destruction leave different artefacts: read before alleging either.
- **The estate is redundant by design:** most "missing" material survives somewhere on the guide 82-83 and backup maps: pursued before mourned.
- **Duties date the analysis:** when preservation obligations arose (letter of claim, contemplation, hold notices) decides what a gap means legally.
- **Inference follows evidence:** courts punish proven destruction, not suspected gaps: the application built on the §3-§4 file, not indignation.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: gaps have causes, and causes leave evidence

Digital estates forget constantly and remember redundantly: both at once. Retention policies delete on schedule; devices are refreshed and reissued; CCTV loops overwrite; chat platforms expire messages by design (guide 66's ephemerality); departing employees' accounts are purged by routine IT hygiene. Against that, everything of consequence tends to exist in several places: sent and received copies, quoted threads, backups, sync caches, counterparty hands. So a gap is never just a gap: it is a claim about what happened, testable against how the estate actually behaves.

The error on both sides is to argue the gap before investigating it. The party facing a hole in its own disclosure asserts "routine deletion" without the policy records that would prove it: and looks worse than the truth may be. The party confronting an opponent's gap alleges destruction without the existence evidence or deletion artefacts: and the application fails, spending credibility the good version would have banked. This guide's order of operations: existence, cause, recovery, then consequences: is the discipline that keeps both chairs on the right side of that error.

§ 0 3 · THE OUTLINE OF THE VANISHED

Proving existence: the traces that show what was once there

- **References in survivors:** replies quoting the missing email; the thread tree with an absent hop (guide 83's structures naming what the quotation preserves); "as per my message this morning"; attachments referenced but not attached: the corpus testifying about its own gaps.
- **System bookkeeping:** file-system tables recording names, sizes and dates of deleted files; mailbox counters and folder statistics; sync and version logs (guides 51-58, 75) listing operations on items no longer present; the guide 87 lattice applied to absence.
- **Counterpart and third-party copies:** the other end of every communication: the recipient's copy proving the sender's deletion, the counterparty's executed agreement proving the vanished draft chain: the single strongest existence evidence there is.
- **Platform and provider records:** message counts, storage metrics, audit logs and billing artefacts that enumerate what accounts contained: obtainable through the guide 55-58 routes and third-party disclosure where proportionate.
- **Shape from negative space:** volume analysis: the custodian whose mailbox holds 40 messages a day for years, and nine for the critical fortnight: statistical outlines a court can see, presented per guide 96's timeline disciplines.

§ 0 4 · READING THE CAUSE

Innocent or engineered: distinguishing routine loss from destruction

- **The innocent baseline:** retention schedules, auto-delete settings, device lifecycle and departure processes documented and matched against the gap: a loss the policy explains, on the policy's timetable, is a loss the policy explains: established, not assumed.
- **Timing against the duty:** the deletion clock read against the preservation clock (§6): material expiring before any duty arose is retention; the same expiry ignored after a hold notice is breach; deletion clustered in the days after the letter of claim is its own exhibit.
- **Destruction's artefacts:** wiping-tool installation and execution traces; mass-deletion patterns (hundreds of items, one session, one account); emptied deleted-items and purged recoverable stores; factory resets dated to the dispute; the guide 110-adjacent anti-forensics catalogue, read by examiners.
- **Selectivity as signature:** routine processes are indiscriminate; engineered deletion is curated: the mailbox intact except the counterparty's threads, the phone backed up nightly except the missing fortnight: selectivity is the pattern policies cannot produce.
- **The honest middle:** negligence, panic deletion by individuals, and IT hygiene run after duties arose but without instruction: commoner than conspiracy, distinguishable by scope and instruction evidence, and pleaded differently: the examiner's report keeping the client on the supportable version.

§ 0 5 · THE RECOVERY MAP

The recovery map: where missing material survives

- **Duplicates and threads:** guide 82's custodian tables and guide 83's quoting hops: the deleted original's content surviving verbatim in other hands and later messages: the first and cheapest sweep.
- **Recycle and version mechanisms:** deleted-item stores, recoverable-items retention, version histories and recycle bins across M365, Google and DMS platforms (guides 51-58, 75): windows measured in days to months: checked immediately, because they close.
- **Backups and archives:** the estate's memory: nightly images, journaling archives, legacy systems: the guide 103-adjacent restoration question scoped for the specific gap, proportionality argued on the §3 existence evidence.
- **Device-level recovery:** unallocated space, database freelists and local caches (the mobile and computer guides' territory): deletion at the interface is often not deletion on the medium: imaged and carved where the device survives.
- **Third parties:** counterparties, providers, professional advisers, regulators: holders of copies outside the destroyer's reach: pursued by request, then CPR 31.17 where the tests are met: the route destruction cannot close.

§ 0 6 · THE DUTY CLOCK

Preservation duties and their breach: the legal framework

- **When duties arise:** in Business and Property Courts matters, PD 57AD's express duty to preserve documents once proceedings are contemplated: including suspending relevant deletion processes and notifying employees and former employees: with parallel obligations flowing from the CPR generally, regulatory holds, and criminal-context CPIA duties.
- **What compliance looks like:** hold notices issued, documented and refreshed (guide 2's disciplines); auto-deletion suspended for relevant sources; departures and device refreshes gated; the preservation record that §4's analysis reads as the innocent explanation.
- **Breach and its shades:** from inadequate holds through negligent loss to deliberate destruction: with solicitors' own obligations (advising on preservation, confirming compliance in the disclosure certificate) making the record professionally load-bearing.
- **Criminal and regulatory overlays:** destruction in contemplation of proceedings can engage perverting-the-course offences; regulated firms face record-keeping and integrity consequences; insolvency and fraud contexts carry their own preservation statutes: flagged for specialist advice where they bite.
- **The certificate's weight:** the disclosure certificate's statements about preservation are signed into the record: a gap later shown to contradict them is a problem of a different order: which is why the preservation file is built as if it will be read aloud.

§ 0 7 · THE CONSEQUENCES

Litigating the gap: applications, inferences and remedies

- **Specific disclosure first:** the gap particularised (the §3 existence file), the recovery routes identified (§5's map), and the order sought for searches, restorations and third-party routes: the constructive application that often ends the problem.
- **Interrogating the loss:** orders for evidence about the circumstances of loss: who deleted what, when, under what instruction, on what systems: the §4 questions given procedural teeth, answered on statement.
- **Adverse inference:** the court invited to infer that destroyed material was unhelpful to its destroyer: available where destruction and its timing are proven, calibrated to the evidence: the remedy the §3-§4 file exists to earn.
- **Costs, strike-out and contempt:** the escalation for grave cases: costs orders for preservation failures; strike-out where destruction makes fair trial impossible; contempt and criminal referral for the worst: rare, fact-heavy, and built entirely on the forensic record.
- **Defending the gap:** the same machinery in reverse: the documented retention explanation, the recovery efforts evidenced, the honest witness statement about what was lost and why: the innocent version, proven rather than asserted, defusing the inference.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a missing-evidence investigation runs on sources that describe the vanished item, sources that may still contain it, and sources that explain its absence: three overlapping maps. The description lives in surviving references (quoting threads, replies, mentions), system bookkeeping (file tables, sync logs, counters), and the metadata lattice of adjacent items. The content may survive in duplicates and counterpart copies, recycle and version stores, backups and archives, device-level residue, and third-party hands. The explanation lives in retention policies and their execution logs, hold notices and the preservation file, deletion and wiping artefacts, account and device lifecycle records, and the instruction evidence (or its absence) around the loss. The three maps are worked in that order: describe, recover, explain: because recovery often moots the fight, and because the explanation's credibility is judged against how hard the first two maps were worked.

EVIDENCE	SURVIVING REFERENCES	SYSTEM BOOKKEEPING	DUPLICATES / COUNTERPARTS	BACKUPS / RECYCLE STORES	DEVICE RESIDUE	POLICY / PRESERVATION FILE
That it existed	Y: quotes + replies	Y: tables + logs	Y: the strongest form	Listings survive content	Names + dates carved	n/a
What it said	Quoted fragments	n/a	Y: verbatim	Y where restorable	Sometimes: carving	n/a
When it vanished	Last quoting date	Y: operation logs	n/a	Last backup containing it	Deletion timestamps	Policy schedule dates
Why it vanished	n/a	Session + account context	n/a	Rotation records	Y: wiping artefacts	Y: the innocent case
Who is responsible	n/a	Y: account attribution	n/a	Admin action logs	User-context artefacts	Instruction evidence

Fallback strategy in one line: describe from survivors, recover from the redundant estate, and only then litigate the residue: the gap that remains after a worked map is the gap worth a court's time.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE FORTNIGHT THAT FELL SILENT

In a shareholder dispute, a director's disclosed mailbox averaged sixty messages a day: and nine a day for the two weeks around the contested board decision. The §3 negative-space analysis put the gap beyond argument; the §5 map then filled most of it: the co-directors' mailboxes held their halves of forty-one deleted threads, the M365 recoverable-items store (checked inside its window) yielded ninety more, and purge audit logs dated the deletions to the evening after the letter of claim, from the director's own account. The specific disclosure application became an adverse-inference application with a schedule of recovered material attached; it settled at the next mediation. The sequence is the guide's whole method: outline, recover, and let the deletion logs argue the cause.

EXAMPLE 2 · THE PHONE IN THE RIVER AND THE CLOUD THAT REMEMBERED

A defendant in a harassment claim reported his phone lost the week before imaging: the messages gone with it, he said. The §5 map disagreed: the iCloud backup predating the "loss" restored the message store; the complainant's handset held the counterpart copies; and the account's own records showed a manual backup deletion attempted two days after the loss report: unsuccessfully, a second sync copy surviving. The recovered content mattered; the recovery story mattered more: the attempted cloud deletion, timed and attributed, converted a credibility contest into a documented destruction attempt, and the §7 consequences followed. Devices are lost every day; estates are redundant every day too: the map is checked before the loss is accepted.

EXAMPLE 3 · THE GAP THE POLICY EXPLAINED

A claimant demanded adverse inference over a defendant's missing 2019 project emails, alleging destruction. The defendant's response was the §7 defence done properly: the retention policy (three-year mailbox expiry, documented and version-controlled), the execution logs showing the 2019 material expiring on schedule in 2022: eighteen months before any dispute: the hold notice issued promptly on contemplation and the suspension records showing nothing relevant expired after it, plus a §5 recovery effort that restored a partial set from an archived PST a former employee's leaver process had preserved. The application failed with costs: the gap was real, the duty analysis was fatal to the inference, and the recovery effort's visible diligence carried the credibility. The innocent version wins exactly when it is proven like a guilty one would be prosecuted.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Arguing before investigating:** destruction alleged on suspicion, or routine loss asserted without the policy file: both chairs' §2 error.
- **Recovery windows missed:** recoverable-items and recycle stores expiring while correspondence was exchanged: §5's clocks run from day one.
- **Counterparts unchecked:** the deleted email mourned while its recipient's copy sits in an unexamined custodian: guide 82's first sweep skipped.
- **The duty clock unread:** gaps condemned or excused without dating them against contemplation and holds: §4's timing analysis, the whole game, omitted.
- **Preservation files never built:** the innocent explanation existing but unprovable: Example 3's defence, unavailable for want of records.
- **Overpleading the middle:** negligence dressed as conspiracy: the supportable case traded for the dramatic one, and lost.
- **Spoliation of the spoliation evidence:** the suspect device used, reimaged or "checked" by IT before examination: the deletion artefacts destroyed by the investigation.
- **Certificates signed over unexamined gaps:** preservation statements made without the file that supports them: §6's professional exposure, self-inflicted.

Technical limitations

- **Absence of evidence has limits:** some material vanishes without existence traces: the honest report states what cannot be shown to have existed.
- **Secure deletion works:** properly wiped media and expired cloud stores are gone: recovery promises calibrated to §5's real mechanics, per the standing honesty rule.
- **Attribution needs the account layer:** deletion logs name accounts, not fingers: the guide 105-107 attribution disciplines apply to destruction too.
- **Volume baselines need care:** negative-space statistics require honest baselines (holidays, role changes): the outline drawn by an examiner, not an advocate.
- **Third-party routes take time:** provider disclosures and CPR 31.17 run on their own clocks: started early or arriving late.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What retention policies, auto-deletion settings and lifecycle processes touch the relevant sources: and where are their execution records?
- When was litigation first contemplated, and what did the hold notice actually suspend, when, evidenced how?
- Is anything already known to be gone: and can we investigate it now, before the certificate speaks to it?

Ask your opponent

- Please state the circumstances in which [the material] ceased to exist, identifying the date, mechanism, responsible account or person, and any policy or instruction under which the deletion occurred, with supporting records.
- Please confirm what steps have been taken to recover [the material], including searches of deleted-item and recoverable stores, backups, version histories and duplicate custodians, with the results.
- Please confirm the date on which your client's preservation obligations were engaged, the date and content of any hold notice, and the deletion processes suspended pursuant to it.

Ask your eDiscovery / forensic provider

- What does the existence file establish: and how strong is each trace against the "never existed" answer?
- Which §5 recovery windows are still open, and which close this month?
- Does the deletion evidence support timing and selectivity findings: and what is the honest ceiling of the attribution?

SUGGESTED WORDING · PRESERVATION AND LOSS-EXPLANATION REQUEST

> "We refer to [the identified gap]. Our client's analysis of the disclosed material, including [thread references / system records / volume analysis], indicates that documents responsive to the agreed scope existed and are absent from your production. Please provide within [14] days: (1) a full account of the circumstances of any deletion or loss, including dates, mechanisms, responsible persons and any applicable policy or instruction, with contemporaneous records; (2) confirmation of the recovery steps taken across deleted-item stores, backups, version histories and duplicate custodians, with results; and (3) the date your client's preservation duty was engaged and the terms and implementation of any litigation hold. Our client reserves the right to rely on this correspondence on any application, including as to specific disclosure, adverse inference and costs."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The missing-evidence checklist

- ☐ Gap particularised: what, whose, when, per the existence file
- ☐ Existence evidence assembled: references, bookkeeping, counterparts
- ☐ Recovery windows checked immediately; the clocks logged
- ☐ Duplicate custodians and thread instances swept first
- ☐ Backups, versions and recycle stores scoped proportionately
- ☐ Duty clock established: contemplation, holds, suspensions
- ☐ Deletion artefacts examined before devices are touched further
- ☐ Cause analysis honest: policy, negligence or engineering, on evidence
- ☐ Preservation file maintained as if read aloud in court
- ☐ Applications built on the file: specific disclosure before inference

Red flags

- Deletion clustered after the letter of claim: Example 1's logs.
- Devices "lost" on the eve of imaging: Example 2's river.
- Selective gaps no policy could produce: the curated mailbox.
- Wiping tools installed mid-dispute.
- Loss explanations that shift between letters.
- Holds issued but nothing suspended: paper compliance.
- Your own side's gap unexamined while the certificate is drafted.

When to involve a digital forensic expert

At first sight of a gap in either direction: to build the existence file before arguing it, to sweep the §5 recovery routes while their windows are open, to read the deletion artefacts before the devices are handled further, and to date the loss against the duty clock: then at the application stage, where the §3-§4 file is the evidence and CPR Part 35 the vehicle, in pursuit or defence alike (Example 3's winning defence was a forensic product). Through **cflab.uk** and **e-discovery.uk**, the gap work runs from same-week recovery sweeps to full spoliation reports: and the earlier the instruction, the more of the map is still warm.

§ 13 · COMMON QUESTIONS

Frequently asked questions

The other side says the documents were deleted under a retention policy. Is that the end of it?

Only if the policy story survives testing: the policy's terms and dates, its execution logs, the duty clock (§6) and the selectivity check (§4) either corroborate the account or contradict it: Example 3 shows the version that holds, Example 1 the version that does not. Ask for the records with §11's request; policies that ran as claimed can always produce them.

Can deleted material really be recovered, or is that television?

Both, honestly: recycle stores, versions, backups, duplicates and counterparts recover a great deal inside their windows (Examples 1-2), while properly wiped media and expired cloud stores are genuinely gone: §5's map with §10's limits. The practical rule is speed: most recovery is a race against rotation clocks that started before you were instructed.

How do we prove something existed if it no longer does?

From the estate's redundancy: quoting replies and thread structures, file-system and sync bookkeeping, counterpart copies, platform counters, and volume analysis (§3): traces that outline the item precisely enough to litigate. Counterpart copies are the gold standard: the deleted email's recipient rarely deleted it too.

When does the duty to preserve actually start?

On contemplation of proceedings, not service: PD 57AD's duty (with its hold-notice and suspension obligations) is engaged when litigation is reasonably in prospect, and the certificate later signs for compliance: which is why the contemplation date is investigated, not conceded, in every gap dispute. Material expiring before that date is retention; after it, the questions begin.

Will a court really draw an adverse inference?

On a proven record, yes: destruction evidenced, timed against the duty, with recovery exhausted: the inference calibrated to what the file shows: and on suspicion alone, no: §7's whole architecture exists because courts punish demonstrated conduct, not gaps as such. Build Example 1's schedule; skip Example 1's indignation.

We have discovered our own client's gap. What now?

Investigate it exactly as you would an opponent's: existence, cause, recovery: then preserve everything about the investigation, take conduct advice where §4's findings warrant it, and ensure the certificate and any witness evidence state the position accurately: the honest, evidenced account (Example 3's defence) is both the ethical course and, in practice, the winning one. What converts a gap into a catastrophe is almost never the loss; it is the account of it that unravels.

§ 14 · REFERENCE

Glossary

Adverse inference
The court inferring destroyed material harmed its destroyer.

Duty clock
The timeline of contemplation, holds and suspensions a gap is dated against.

Existence file
The assembled traces proving the vanished item was once there.

Hold notice
The preservation instruction suspending deletion for a matter.

Negative-space analysis
Volume and pattern evidence outlining what is absent.

Recovery window
The closing period in which a store still yields deleted items.

Selectivity
Curated absence: the pattern routine processes cannot produce.

Spoliation
Destruction or alteration of evidence relevant to proceedings.

Suspension record
Proof that deletion processes were actually halted under a hold.

Wiping artefacts
Tool and execution traces left by deliberate erasure.

Sources and authoritative references

The missing-evidence disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (deletion analysis, recovery, spoliation reporting under CPR Part 35): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Identification and Phase 03 · Preservation (hold machinery, recovery routes and the preservation file as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/preservation
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- PD 57AD (the preservation duty, hold notices and the disclosure certificate): justice.gov.uk, PD 57AD · CPR Part 31 (including r.31.17 third-party disclosure): justice.gov.uk, Part 31
- CPR Part 35: justice.gov.uk, Part 35 · ISO/IEC 27037 (identification and preservation of digital evidence): iso.org, 27037 · ICO, UK GDPR guidance: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Gap work at the laboratory runs the §1 sequence at instruction speed: the existence file assembled from survivors and bookkeeping; the recovery map swept while its windows are open (the recoverable-items check is a same-week task, and Example 1's ninety threads existed because someone ran it in time); deletion and wiping artefacts read before devices are handled further; and the cause analysis: policy, negligence or engineering: reported honestly, because the supportable finding is the one that survives cross-examination. On the defence side, the same machinery builds Example 3's winning file: the policy records, the duty analysis, the visible recovery diligence. Reports are prepared under CPR Part 35 for applications from specific disclosure to adverse inference and beyond. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a gap has just surfaced in either direction, the recovery clocks are already running: this week beats next month, every time.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace