COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Can You Prove Who Deleted a File?

Deletion Artefacts, Audit Trails and the Attribution of an Absence

Guide 95 asked whether missing evidence was lost or destroyed; this guide asks the harder follow-up: by whom. Deletion is an act with an actor, and the platforms and file systems record it more often than the person deleting expects: cloud audit logs name the account that sent an item to the recycle bin and the account that emptied it; file-system journals and metadata record the removal even when the content is gone; recycle-bin structures keep the original path, the deletion time and the user profile; and the deliberate-erasure tools that promise to leave nothing leave their own installation and execution artefacts instead. What none of these records is a person: they record accounts, profiles and sessions, and the investigation must join them to hands through the same corroboration this series has built for every attribution question. This guide sets out for UK lawyers where deletion is recorded on each platform, what survives the deletion itself, how to attribute it to an account and then a person, and how the finding is deployed in spoliation, employment and fraud proceedings.

⏱ Estimated reading time: 24 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. Deletion attribution is among its most-instructed examinations: who emptied the mailbox, who wiped the laptop, who purged the shared folder the week the dispute began: answered from audit logs, file-system journals, recycle-bin structures and anti-forensic tool artefacts, joined to a person through corroboration, and reported under CPR Part 35 for spoliation, employment and fraud proceedings.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | DELETION & WIPING ATTRIBUTION | FILE-SYSTEM JOURNAL ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: DELETION IS RECORDED BY THE PLATFORM, THE FILE SYSTEM AND THE ERASURE TOOL ITSELF: THE RECORD NAMES AN ACCOUNT OR PROFILE, THE CORROBORATION NAMES THE PERSON, AND THE TIMING AGAINST THE DUTY NAMES THE CONSEQUENCE

Cloud and servers (§3): Microsoft 365 and Google Workspace log deletion events with the acting account, item, client and timestamp: soft deletes to recycle, purges from recycle, hard deletes and administrative deletions each as distinct events: with the recycle stages (first and second stage, recoverable-items) preserving the item for a period and its deletion record for longer. File servers with object-access auditing log delete operations in security events; without it, the file system's own structures (§4) are the only witness. **Local deletion (§4):** the Windows recycle bin keeps per-user metadata files recording the original path, size and deletion time for each deleted item under the deleting profile; the NTFS master file table and change journal record file removal as transactions with timestamps; macOS and mobile file systems keep equivalent structures; and deleted content persists in unallocated space until overwritten (guide 95's recovery), carrying the guide 87 metadata that dates and attributes the file's life. **Deliberate erasure (§5):** wiping tools, secure-delete utilities, history cleaners and factory resets remove content more thoroughly and leave characteristic traces: installation records, execution artefacts (prefetch, application logs, registry keys), the pattern of overwritten space, and the abrupt cessation of routine artefacts: the anti-forensics itself becoming the evidence, timed against the dispute. **Attribution (§6):** the deleting account or profile from the log or the bin; the session from sign-in and logon records; the device from endpoint context; the person from physical and behavioural corroboration: guide 105 §7's lattice, with shared logins, administrative scripts and automated retention addressed as alternatives. **Deployment (§7):** the attributed deletion, dated against the preservation duty (guide 95 §6), supports adverse inference and costs, grounds employment and fraud allegations, and: where the actor is an administrator running a scheduled policy: exonerates.

- **Platforms log the deleter:** the acting account is in the audit event: exported inside retention, or lost with the item's history.
- **The bin keeps the path and the profile:** local deletion attributes to a user profile and records what was deleted, from where, when.
- **Journals outlive content:** file-system transaction records prove the removal after the data is unrecoverable.
- **Wiping tools sign their work:** the erasure that leaves nothing leaves the eraser's own footprint.
- **Timing is the consequence:** who deleted matters; when, against the duty, decides what it means.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: deletion is an act, and acts have actors

The person who deletes a file experiences it as making something disappear. The system experiences it as a transaction: an authenticated session issued an instruction, the platform or file system executed it, and both wrote records of having done so. Those records were never meant for litigation; they exist for recovery ("restore from recycle bin"), for integrity (the journal that lets a file system recover from a crash), and for administration (the audit trail that shows what happened to the tenant). But they answer the litigator's question directly: this account, this session, this item, this time.

The investigation's difficulties are the familiar ones: the records expire, they name accounts rather than people, and the deliberate deleter may have used tools designed to defeat them. This guide takes each in order. Its underlying point is the one guide 95 made about absence: a deletion is never just a gap. It is an event with a signature, and the signature is usually readable by someone who knows where to look, before the clocks that govern it run out.

§ 0 3 · CLOUD AND SERVER DELETION

Cloud and server deletion: audit logs, recycle stages and admin actions

- **Microsoft 365 events:** SharePoint and OneDrive log file deletions, recycle-bin deletions (purges) and second-stage removals with the acting account, item path, client and timestamp; Exchange mailbox auditing records soft-deletes, hard-deletes and folder purges (guide 104 §6): each a distinct event type, read per §5 of guide 105 for what it proves.
- **Google Workspace events:** Drive audit records trash, permanent deletion and trash-emptying with actor and item; Gmail and Vault audit records mail deletion and admin actions: the same discipline, different vocabulary.
- **Recycle stages as evidence:** the recycle bin's contents (with deleter, deletion time and original location) until purged; the second-stage or recoverable-items store afterwards; and the audit record of each stage's transition: the item's afterlife, each stage timestamped and attributed.
- **Administrative and policy deletions:** retention-policy expiry, admin purges, bulk clean-ups and leaver processes (guide 103) appear as system or admin actions with their own attribution: distinguished from user deletions by event type and acting identity: the innocent explanation, when it is one, is in the log.
- **File-server auditing:** where object-access auditing with delete permissions is configured, security events record the deleting account and object; where it is not (guide 105 Example 2), the server itself is silent and §4's file-system structures on the server volume become the source.

§ 0 4 · LOCAL DELETION

Local deletion: recycle bins, file-system journals and metadata residue

- **The Windows recycle bin:** per-user folders under the deleting profile's security identifier, each deleted item paired with a metadata file recording original path, size and deletion timestamp: attribution to profile and time, and the original location, from the bin's own structure: surviving until the bin is emptied, and recoverable from unallocated space for a period afterwards.
- **NTFS structures:** the master file table retains entries for deleted files (marked unused) with their names, timestamps and metadata until reused; the change journal records create, modify, rename and delete operations as timestamped transactions: the file's removal proven from the journal after its content is gone.
- **macOS and mobile equivalents:** the macOS trash with its per-volume structures and file-system event records; iOS and Android application databases with deletion flags and freelist residue (guides 145-175's territory): the same principle across platforms.
- **Shift-delete and bypassed bins:** deletions that skip the recycle bin still write file-system transactions: the journal and the MFT record them without the bin's convenience: the act proven, the profile inferred from session context.
- **Metadata residue and carving:** guide 95 §5's recovery applied for attribution: recovered file fragments carrying internal metadata (author, last-saved-by, timestamps) that place the file's life in a profile and a period, corroborating the deletion's context.

§ 0 5 · DELIBERATE ERASURE

Deliberate erasure: wiping tools, anti-forensics and their own artefacts

- **Tool installation and execution:** secure-delete utilities, disk cleaners and privacy tools leave installation records, prefetch and execution artefacts, registry keys, application logs and, often, their own settings files recording what was targeted: the tool's presence and use proven, and dated.
- **Overwrite patterns:** wiped space shows characteristic patterns (zeros, random data, repeated passes) distinguishable from normal unallocated residue: the wipe's extent and timing inferred from the pattern's boundaries and the surviving neighbours.
- **The cessation signature:** routine artefacts (browser history, recent files, event logs) that stop abruptly at a date, or restart empty: the cleaner's fingerprint in the negative space, per guide 95 §3.
- **Factory resets and reimaging:** device resets and OS reinstalls leave installation timestamps, and the pre-reset state may survive in backups, cloud syncs and, on some devices, residual partitions: the reset dated, its context established, and the guide 110 anti-forensics catalogue applied.
- **The evidential inversion:** deliberate erasure after a duty arose is stronger evidence of consciousness than the deleted material would have been: the tool's execution timestamp against the letter of claim is frequently the case's decisive exhibit.

§ 0 6 · ATTRIBUTION

Attribution: from account and profile to the person at the keyboard

- **The acting identity:** the audit log's account, the recycle bin's profile, the journal's session context: the first link, established from the record itself.
- **Session and device:** sign-in and logon records (cloud and local) joining the identity to a device, IP, time and authentication method: guide 104 §6's second layer.
- **Physical and behavioural corroboration:** badge and presence records, the person's own messages ("clearing my laptop tonight"), calendar entries, CCTV, and the guide 96 lattice generally: the independent sources that close the gap between account and hands.
- **Alternatives, addressed:** shared credentials; an unlocked workstation; an administrator's script or a retention policy acting under a system identity; a sync client propagating a deletion made elsewhere (a file deleted on a phone vanishing from a laptop by sync, with the laptop's log showing the client as actor); malware or compromise: each tested against the session evidence and either excluded or stated open.
- **The honest grade:** attribution reported at the level the evidence supports: "account X, session on device Y" is a finding; "person Z" is a finding only with the corroboration in place: guide 100 §6's method transparency applied to the most contested word in the report.

§ 0 7 · DEPLOYMENT

Deployment: spoliation, employment, fraud and the innocent explanation

- **Spoliation:** the attributed, dated deletion against the preservation duty (guide 95 §6-§7): specific disclosure of recovery efforts, evidence about the deletion, adverse inference where timing and selectivity support it, costs and beyond: the deletion record as the application's exhibit.
- **Employment:** the departing employee's clean-up (guide 97 §4's anti-forensic tail) or the manager's purge of a subordinate's complaint record: attributed deletion grounding misconduct findings, with guide 97 §5's process discipline.
- **Fraud and concealment:** the deleted second ledger, the purged supplier correspondence, the emptied mailbox before audit (guide 98 §3): deletion attribution as consciousness-of-guilt evidence, and as the map to the counterpart sources that still hold the content.
- **The innocent explanation, proven:** the deletion attributed to a retention policy, an administrator's routine clean-up, a sync propagation or a documented leaver process before the duty arose: guide 95 Example 3's defence, with the attribution record as its foundation: the party facing the allegation served as well by the discipline as the party making it.
- **Criminal and regulatory edges:** destruction to pervert the course of justice, regulatory record-keeping breaches, and data-protection dimensions where personal data was destroyed or, conversely, retained unlawfully: flagged for specialist advice where the attribution reaches them.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a deletion is recorded in layers that fail independently, and the attribution is built from whichever survive. The platform audit log records the account and event. The recycle stages hold the item and its deletion metadata for their windows. The file system's own structures (bin metadata, MFT entries, change journal) record the transaction on the device or server volume. The session layer joins identity to device. The erasure tool's artefacts record deliberate destruction where it occurred. And the estate's redundancy (guide 95 §5, guide 103 §6): counterpart copies, backups, sync mirrors, other members' Teams copies: proves what was deleted even where nothing records who. When the primary record is gone: audit retention expired, bin emptied, journal wrapped, the device wiped: the table names the survivors: the sync mirror's log records the deletion propagating; the backup dates the file's last existence; the tool's prefetch entry dates the wipe; the counterpart's copy proves the content.

QUESTION	PLATFORM AUDIT LOG	RECYCLE STAGES	FILE-SYSTEM STRUCTURES	SESSION / DEVICE LAYER	ERASURE-TOOL ARTEFACTS	ESTATE REDUNDANCY
What was deleted	Item identifiers	Y: the item itself, for a window	Y: names, paths, metadata residue	n/a	Target lists sometimes	Y: the surviving copies
When	Y: event timestamp	Y: deletion time	Y: journal transaction	Session brackets	Y: execution time	Last-backup bracket
Which account / profile	Y: acting account	Y: profile folder	Session context	Y: authenticated identity	Installing / running profile	n/a
Which person	n/a	n/a	n/a	Device + location + method	n/a	Their own messages about it
Deliberate or routine	Event type: user vs system	Purge vs expiry	Shift-delete vs bin	Interactive vs scheduled	Y: the tool's presence	Selectivity across copies

Fallback strategy in one line: when the log has expired, the bin still names the profile; when the bin is emptied, the journal still records the act; when the device is wiped, the tool's own artefacts date the wipe: and the estate's copies prove what it was.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE PURGE AT 23:12 AND THE ACCOUNT THAT DID IT

A shareholder dispute produced a defendant's OneDrive with a conspicuous gap: no documents on the disputed transaction. The §3 export (run before the tenant's audit window closed) told the story: 214 files deleted from a "Deal" folder in one session at 23:12, four days after the letter of claim; the recycle bin purged forty minutes later by the same account; and a second-stage purge the following morning by an administrator account: the defendant's own, which held global admin rights. The sign-in log placed all three sessions on his laptop at his home IP. The estate's redundancy (guide 95 §5) recovered most of the content from a colleague's shared copies and the tenant backup; the attribution record made the recovery unnecessary for the inference: the court drew it on the log alone. The deletion was a deletion; the purge sequence, timed and attributed, was the case.

EXAMPLE 2 · THE CLEAN LAPTOP AND THE CLEANER'S RECEIPT

A departing sales director returned a laptop with an almost empty user profile and no browser history. The employer alleged deliberate wiping; the director said he had "tidied up personal files". The §5 examination found the tool: a privacy-cleaner utility installed eleven days before departure, with prefetch entries for four executions on the final two evenings, a settings file listing "Documents", "Downloads" and all browser profiles as targets, and overwrite patterns across the unallocated space consistent with the tool's documented method. The change journal, which the cleaner had not targeted, recorded the deletion transactions for 3,100 files by name in the final session, including the client-list exports the employer was looking for. The tool had erased the content and written its own confession. The employment tribunal and the confidence claim both proceeded on the cleaner's receipt.

EXAMPLE 3 · THE DELETION THAT WAS A POLICY, AND THE ALLEGATION THAT WAS WITHDRAWN

An opponent alleged that a finance manager had deleted a year of supplier correspondence before disclosure, citing the absence and the manager's role. The §3 audit export answered it: the deletions had been executed under a system identity by a retention policy, in nightly batches over three weeks, eleven months before contemplation of proceedings; the policy's configuration history showed it had been set at that period by IT two years earlier; and the manager's account had no deletion events on the mailbox in the disputed period at all. The §6 attribution reached a policy, not a person, and dated it before the duty. The allegation was withdrawn with costs. The discipline that proves the guilty deletion is the same discipline that proves the innocent one, and the party that runs it first holds the initiative.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Audit log left to expire:** the deleter's identity lost while the absence was argued: guide 105 §6's clock, for deletions.
- **The device handled first:** IT's "look" overwriting bin and journal residue before imaging: guide 97 Example 2's afternoon.
- **Attribution from role:** Example 3's allegation: the person who "would have" deleted, pleaded without the record.
- **System deletions read as user acts:** retention and admin events attributed to individuals: event types unread.
- **Sync propagation missed:** the laptop's client logged as deleter of a file removed on the phone: the origin device never identified.
- **The wipe tool unexamined:** "the drive was empty" reported without the §5 artefacts that show why and when.
- **Timing unread against the duty:** attribution complete, consequence unargued: guide 95 §6 forgotten.
- **Alternatives unaddressed:** the shared-login and unlocked-desk possibilities ignored, and raised by the other side.

Technical limitations

- **Journals wrap:** file-system change journals are finite and overwrite on busy volumes: the transaction record reaches back days to months, not years.
- **Bins empty:** emptied recycle bins lose their metadata files to unallocated space, recoverable for a period and then gone.
- **Good wiping works:** a thorough multi-pass wipe defeats content recovery; what survives is the wipe's own signature and the estate's other copies: stated as such.
- **System identities hide humans:** an administrator running a manual script under a service account attributes to the account: the human behind it found, if at all, from change-management records and session context.
- **Mobile platforms vary:** deletion residue in app databases depends on the app and OS version: guides 145-175's per-platform methods, verified per device.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What retention and clean-up policies run on the relevant platforms, and could the deletion be theirs: before anyone is named?
- Have the platform audit logs been exported, and are the devices concerned still unhandled?
- When was the duty engaged, and where does the deletion fall against it?

Ask your opponent

- Please disclose the audit-log entries recording the deletion, recycle-bin removal and any second-stage or administrative purge of [items] during [period], identifying the acting account, event type, client, IP address and timestamp for each, and the retention configuration applicable to the log.
- Please identify any retention policy, administrative action or automated process under which [items] were deleted, with its configuration history and execution records.
- Please confirm preservation of the devices used by [individuals] during [period] unaltered, and disclose any secure-deletion, cleaning or privacy software installed on them, with installation and execution records.

Ask your eDiscovery / forensic provider

- What do the audit log, bin and journal each show for the deletion: and do they agree on account, time and item?
- Is there an erasure tool on the device, and what does its execution record say against the dispute's dates?
- Which alternatives to the named person remain open after the session evidence?

SUGGESTED WORDING · INSTRUCTION FOR DELETION ATTRIBUTION

> "You are instructed to examine [platforms / devices] to determine whether [items] were deleted, and if so when, by which account or profile, from which device and session, and whether by user action, administrative action, automated policy or other process. Please identify and preserve all relevant records, including platform audit logs (with retention status), recycle-bin and recoverable-items contents and metadata, file-system journal and metadata residue, session and sign-in records, and any secure-deletion, cleaning or reset tool artefacts with their execution history. Please state the basis and confidence of any attribution to an account and, separately, to an individual, addressing alternative explanations including shared credentials, unattended sessions, synchronisation, compromise and system processes. Please date each deletion event against [the date of contemplation / the hold notice] and report in a form suitable for CPR Part 35 [/ CrimPR Part 19]."

§ 12 · QUICK CONTROL

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

The deletion-attribution checklist

- ☐ Platform audit logs exported inside retention; deletion events isolated
- ☐ Recycle and recoverable stages checked and preserved
- ☐ Devices sequestered unhandled; imaged before examination
- ☐ Bin metadata, MFT residue and change journal examined
- ☐ Erasure tools searched for; installation and execution dated
- ☐ Session, sign-in and logon records joined to each deletion
- ☐ System, policy and sync deletions distinguished from user acts
- ☐ Corroboration assembled: physical, behavioural, the person's own words
- ☐ Alternatives addressed in the report; attribution graded
- ☐ Each deletion dated against the preservation duty

Red flags

- Deletion sessions in the days after the letter of claim: Example 1's 23:12.
- Purges through all recycle stages in quick succession.
- Cleaning or secure-delete tools installed mid-dispute: Example 2's receipt.
- Artefact histories that stop abruptly at a date.
- Deletion allegations made from role rather than record: Example 3's withdrawal.
- Devices handled by IT before instruction.
- Administrative rights held by the person whose data is missing.

When to involve a digital forensic expert

At the first sign of a gap, because the audit window and the journal's wrap are running (Example 1's export); before any device is touched, so the bin and journal residue survive; at examination, where the platform, file-system and tool layers are read together and the attribution graded honestly (Example 2's receipt, Example 3's policy); and at deployment, where the dated, attributed deletion is evidenced under CPR Part 35 in spoliation, employment and fraud proceedings, or the innocent explanation is proven with the same rigour. Through **cflab.uk** and **e-discovery.uk**, deletion attribution runs from the same-day export to the graded finding: because "who deleted it" has an answer more often than the deleter hoped.

§ 13 · COMMON QUESTIONS

Frequently asked questions

If a file is gone, how can anyone know who deleted it?

Because deletion writes records the deleter does not see: the platform's audit event naming the account, the recycle bin's metadata naming the profile and time, the file system's journal recording the transaction (§3-§4): Example 1's purge sequence was reconstructed entirely from those. The content's absence and the act's record are separate things.

Does emptying the recycle bin remove the evidence of deletion?

It removes the item and, in time, the bin's metadata file: but the emptying is itself an audited or journaled event, the metadata file persists in unallocated space for a period, and the platform's second-stage store holds cloud items longer (§3-§4). Emptying the bin usually adds a second attributed event rather than removing the first.

The laptop came back wiped. Is there anything to find?

Often the most important thing: the wiping tool's installation and execution records, its settings, the overwrite pattern and the change journal it did not target (§5, Example 2): deliberate erasure after a duty arose is stronger evidence than the erased files would have been. The device is imaged first and the tool's receipt read second.

Can we prove it was the person and not just their account?

To the extent the corroboration allows: session and device from sign-in records, presence from badges or calendar, their own messages about it, and the exclusion of alternatives (shared login, unattended desk, sync, policy) (§6): the report grades the attribution accordingly. "Account X on device Y at 23:12" is a finding; the name follows when the lattice supports it.

Our client did delete the files, but before any dispute. Does that matter?

Enormously: deletion before the preservation duty arose is retention or housekeeping, and the attribution record proves the timing (§7, guide 95 §6): Example 3's policy deletions eleven months before contemplation defeated the allegation with costs. Establish the date from the record; it is the whole difference between a gap and spoliation.

What if the deletion was done by a retention policy or an administrator?

Then the audit event says so: system identities, policy execution records and admin actions are distinguishable from user deletions by event type and acting account (§3), and the policy's configuration history dates its origin. Attribution to a policy is a finding that exonerates the individual: and, if the policy ran after a hold should have suspended it, a preservation failure of a different kind.

§ 14 · REFERENCE

Glossary

Change journal
NTFS's transaction log of file operations, including deletions.

Cessation signature
Routine artefacts stopping abruptly: the cleaner's negative-space trace.

Deletion event
A platform audit entry recording removal with acting account and time.

Erasure artefacts
Installation, execution and settings traces left by wiping tools.

MFT residue
Master-file-table entries for deleted files, retained until reused.

Overwrite pattern
The characteristic data a wiping tool leaves in freed space.

Purge
Removal from a recycle stage, itself an attributed event.

Recycle-bin metadata
Per-item records of original path, size and deletion time under a profile.

Second-stage recycle
A cloud platform's post-bin retention store.

System identity
The non-human account under which policies and scripts act.

Sources and authoritative references

The deletion-attribution 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 and wiping attribution, file-system analysis, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 07 · Analysis (audit export, recycle-stage preservation and deletion analysis as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft Learn, audit log activities (file and mailbox deletion events): learn.microsoft.com, audit activities · Recycle bin and recoverable items: learn.microsoft.com, recoverable items
- PD 57AD (preservation duty): justice.gov.uk, PD 57AD · CPR Part 31: justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (file-system artefacts): csrc.nist.gov, SP 800-86 · ISO/IEC 27037: iso.org, 27037 · ICO, UK GDPR guidance: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Deletion work at the laboratory runs the layers in order of perishability: platform audit logs and recycle stages exported and preserved the day of instruction (Example 1's sequence existed because the export beat the window), devices imaged before anyone handles them, and the file-system, tool and session layers read together so the attribution is graded to what the evidence supports: account, session, device, and person where the lattice closes. The same rigour proves the innocent version: the policy, the administrator, the sync, the deletion before the duty (Example 3's withdrawal): and reads the wiped laptop for the eraser's receipt (Example 2). Reports run under CPR Part 35 for spoliation, employment and fraud proceedings. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a folder emptied last week, the deleter's name is in a log with a retention clock: export it today, and the absence starts answering questions.

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