COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Proving Who Created or Edited a Document

Authorship From Metadata, Version Ladders, Platform Logs and Endpoints

"Who wrote this?" is asked of the contract clause that appeared between drafts, the board minute nobody remembers approving, the report whose conclusions changed after the client saw it, the anonymous letter, the threatening message. Documents carry authorship evidence in several strata: the internal metadata guide 87 taught lawyers to read with care (author fields, last-saved-by, revision counts, template origins), the version ladders of guide 102 that attribute each save to an account, the platform audit logs that record edits server-side, the endpoint artefacts that show a document open on a particular machine, and the linguistic and structural fingerprints of the writer themselves. None of it names a person on its own; the discipline is the corroboration lattice this series has applied to every attribution question, with authorship's own traps: shared templates, copied metadata, co-authoring's attribution rules, and the difference between the account that saved and the hands that typed. This guide sets out the method for UK lawyers.

⏱ 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. Authorship examinations run through its casework: the disputed clause, the anonymous document, the report edited after the fact, the "I never wrote that" defence: answered from metadata, version histories, platform logs and endpoint artefacts joined into a corroborated finding, and reported under CPR Part 35 and CrimPR Part 19 where authorship is the issue.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | AUTHORSHIP & EDIT ATTRIBUTION | METADATA & VERSION ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: AUTHORSHIP IS PROVED BY JOINING FOUR STRATA: WHAT THE DOCUMENT SAYS ABOUT ITSELF, WHAT THE PLATFORM RECORDED, WHAT THE ENDPOINT REMEMBERS, AND WHAT THE WRITING REVEALS: EACH FALLIBLE ALONE, EACH CORROBORATING THE OTHERS, WITH THE TRAPS NAMED BEFORE THE FINDING IS MADE

Internal metadata (§3): Office and PDF files carry author, last-modified-by, company, template and revision fields, editing-time counters and, in some formats, embedded identifiers: evidence of the environment in which the document was created and saved, with the standing caveats that author fields are inherited from templates and prior documents, copied wholesale when a file is used as a starting point, editable by anyone, and blank or generic on many machines: guide 87's discipline, sharpened. **Platform evidence (§4):** cloud version ladders (guide 102) attribute each save to an authenticated account with a timestamp; platform audit logs record edit events server-side; DMS systems record check-ins with user and comment: the strongest attribution stratum, subject to co-authoring's rules (the account that triggered the save may not be the only editor in the session) and to the account-versus-person gap. **Endpoint and transmission (§5):** the machine on which the document was open (recent-file lists, application artefacts, temporary and autorecovery files carrying drafts), the account that sent it and when (guides 51-58, 104), and the hash-matching of sent copies to rungs: placing the document on a device and in a session. **Content (§6):** linguistic and stylistic features (vocabulary, idiom, error patterns, formatting habits) compared to known writing: forensic-linguistic evidence that supports or undermines the technical attribution, with its own methodological standards. **The lattice (§7):** the four strata joined on guide 96's frame, alternatives addressed: template inheritance, copied metadata, shared machines, co-authoring, delegated drafting: and the finding graded to what the corroboration supports.

- **Author fields are environment, not signature:** inherited, copied, editable: read as evidence of the machine and template, never as proof of the hands.
- **Version ladders attribute saves:** account, time, content per rung: the platform's record is the strongest stratum, with co-authoring's caveats.
- **Endpoints place the document:** the machine it was open on, the drafts it left behind: independent of the platform.
- **Writing carries fingerprints:** stylistic evidence supports the technical case, with methodology stated.
- **The traps are the cross-examination:** template inheritance, shared devices, delegation: named in the report before the opponent names them.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: documents remember their authors, imperfectly

Every document is created somewhere, by someone, using something, and each of those leaves marks. The word-processor writes the registered user's name into the file; the cloud platform records which account saved which version; the machine keeps a list of recently opened files; the email system records who sent the attachment; and the writer's own habits: the double space after the full stop, the favoured phrase, the recurring typo: travel with the text. Taken together, these strata answer "who wrote this?" with useful precision.

Taken separately, each misleads. The author field says "Sarah Jones" because the document was started from a template Sarah made in 2019. The version ladder names the assistant's account because the assistant pressed save in a co-authored session the director controlled. The recent-files list shows the document open on a shared machine in an open-plan office. The style matches because the writer was imitating a colleague. Authorship attribution is the discipline of joining the strata so that each one's weakness is covered by another's strength, and of naming the alternatives before the other side does: which is why the honest report reads "the evidence is consistent with authorship by X and inconsistent with the alternatives Y and Z", and why the confident report reads like an assertion.

§ 0 3 · INTERNAL METADATA

Internal metadata: author fields, revision data and what they actually record

- **Author and last-modified-by:** set from the application's registered user name at creation and at each save: recording the identity configured on the machine, which may be a person, a generic name ("User", "Admin", the company), or a predecessor's name inherited from a template or a copied document: evidence of environment, verified against the machine's actual configuration before it is read as identity.
- **Template and origin fields:** the template used, the company and manager fields, and application-version identifiers: placing the document's creation in a particular software environment: guide 87's anachronism tests (a 2019 document from a 2023 application build) run from these.
- **Revision counts and editing time:** total editing time, revision number, and creation-versus-last-saved intervals: the drafting effort's shape: a "long-standing" document with a revision count of one and four minutes' editing time is a reconstruction (guide 98 Example 2's pattern).
- **Tracked changes and comments:** where retained, the per-change author names and timestamps inside the file: the richest internal attribution, and the one most often stripped before production (or, per guide 93, left in by mistake).
- **PDF and image metadata:** producer and creator fields, creation and modification dates, embedded XMP data: the conversion environment's fingerprint (which application, on what platform, produced this PDF) rather than the author's, read accordingly.

§ 0 4 · PLATFORM EVIDENCE

Platform evidence: version ladders, audit logs and co-authoring attribution

- **The version ladder:** guide 102's method: each rung's modifying account and timestamp, with diffs localising which account's save introduced which change: "the indemnity was removed in the version saved by account X at 23:40": the platform's own attribution, independent of the document's internal fields.
- **Audit-log edit events:** SharePoint, OneDrive and Drive record modification events with account, client and session (guide 105 §3): corroborating the ladder from a different log, and surviving where the ladder was flattened.
- **Co-authoring's attribution rules:** in real-time co-authored sessions, a version's "modified by" reflects the account whose client triggered the save, while several accounts may have edited content within it: the platform's per-paragraph attribution (where the application retains it) and the audit log's concurrent-session records distinguish who typed what, and the report states the granularity honestly.
- **DMS check-in records:** document-management systems attribute each version to the checking-in user with comments and timestamps, and log views and edits per user: the legal sector's strongest authorship record, with the delegation caveat (the secretary checking in the partner's draft).
- **Account to person:** the platform names authenticated accounts; sign-in records add device and context; the guide 104-105 lattice joins them to a person: the standing gap, closed by corroboration or stated open.

§ 0 5 · ENDPOINT AND TRANSMISSION EVIDENCE

Endpoint and transmission evidence: where the document was open, and who sent it

- **Recent-file and application artefacts:** LNK files, jump lists, application most-recently-used lists and registry entries recording the document open on a specific machine under a specific profile at recorded times: placing the drafting on a device, independent of any platform.
- **Autorecovery, temporary and print artefacts:** the application's autosave and temporary files holding intermediate drafts (often with tracked changes the final lost), print-spool remnants, and thumbnail caches: the drafting process preserved in the machine's working files.
- **Local file-system metadata:** creation, modification and access timestamps on the local copy, with guide 87's rewrite rules applied: corroborating the platform's timeline where they agree, and explained where they do not.
- **Transmission records:** the sending account, time and recipients of every copy (guides 51-58, guide 104's send-as caveats), with attachment hashes matched to version rungs (guide 102 §6): who circulated which state of the document, and when: authorship's public face.
- **Device attribution:** the machine's ownership and use (asset register, login history, physical location, guide 96's physical layer): the endpoint joined to a person as the platform account is: shared and hot-desked machines flagged as the trap they are.

§ 0 6 · CONTENT EVIDENCE

Content evidence: linguistic, structural and stylistic attribution

- **Stylistic markers:** vocabulary and idiom, sentence structure, punctuation habits (the double space, the Oxford comma, the dash preference), spelling conventions and characteristic errors, salutation and sign-off patterns: features compared between the questioned document and a corpus of known writing by each candidate.
- **Structural and formatting habits:** heading conventions, list styles, font and spacing choices, date formats, the way tables are built: the document's construction reflecting its builder's habits, particularly in unsigned or anonymous material.
- **Forensic linguistics as a discipline:** where the stakes justify it, a forensic linguist's comparative analysis under stated methodology: distinct from the digital examiner's work and instructed as such (guide 100's specialism-matching), with the limits of authorship attribution from short texts acknowledged.
- **Machine-generated and AI-assisted text:** guide 126's territory: content drafted with generative tools carrying its own signatures, and the attribution question shifting to who prompted and who adopted: named as a live complication, addressed with current methods.
- **Content as corroboration, not proof:** stylistic evidence weighs alongside the technical strata; it rarely stands alone, and the report says which role it plays.

§ 0 7 · THE LATTICE AND THE TRAPS

The lattice and the traps: joining sources and addressing alternatives

- **The join:** internal metadata, platform ladder, endpoint artefacts and transmission records normalised to one frame (guide 96) and cross-checked: the strongest attributions are those where independent strata agree on account, device, time and content: the report showing the agreement and the residual gaps.
- **Template inheritance:** the author field naming whoever made the template or the document copied as a starting point: the commonest false attribution, excluded by checking the field against the platform ladder's first rung and the machine's configured identity.
- **Copied and edited metadata:** internal fields are editable and travel with copies: a document's fields matching a candidate prove the environment was theirs or was made to look so: guide 109's manipulation tests apply.
- **Shared machines, shared accounts, delegation:** the open-plan PC, the generic login, the assistant drafting for the principal: the alternatives that every authorship finding must address, from session evidence, physical presence and the drafting relationship's own records.
- **Grading the finding:** "created in an environment configured for X", "saved by account X", "open on X's device", "consistent with X's writing": each a distinct claim at its own confidence: the report stating which it makes, and refusing the leap to "written by X" the evidence has not earned.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: authorship evidence is layered by design, and each layer covers the others' failures. The document's internal metadata is portable and editable but travels with every copy, so it survives in the counterparty's version when the original is gone. The platform ladder is authoritative but prunable and flattenable (guide 102 §4), so the audit log and the sent copies stand in when it is short. The endpoint remembers the drafting session independently of the cloud, so a document created offline or on a machine that never synced still leaves LNK files, autorecovery drafts and application histories. Transmission records place each state of the document with a sender and a time regardless of what the file itself claims. The content's style survives every technical stripping. And the counterpart's copy: the recipient's attachment, the opponent's produced version: carries the metadata the author may have cleaned from their own. When the primary source is compromised: the ladder gone, the device wiped, the fields scrubbed: the table names what remains.

QUESTION	INTERNAL METADATA	PLATFORM LADDER + AUDIT LOG	ENDPOINT ARTEFACTS	TRANSMISSION RECORDS	CONTENT / STYLE	COUNTERPART COPIES
Which environment created it	Y: author, template, app	First-rung account	Y: the machine's configuration	n/a	Formatting habits	Same fields, uncleaned
Which account saved each change	Tracked changes, if kept	Y: per rung, with diffs	Autorecovery drafts	Hash-matched states	n/a	Intermediate states as sent
Which device it was open on	n/a	Client info in events	Y: LNK, MRU, temp files	Sending client	n/a	n/a
Who circulated which state	n/a	Share events	Sent-items caches	Y: sender, time, recipients	n/a	Y: as received
Whose writing it is	Comment author names	Per-paragraph attribution where kept	n/a	Cover-note style	Y: the linguistic case	n/a

Fallback strategy in one line: when the file's own fields are cleaned or inherited, the platform's ladder attributes the saves; when the ladder is gone, the endpoint places the session and the sent copies date the states: and the counterpart's copy usually still carries what the author's does not.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE CLAUSE THAT ARRIVED BETWEEN DRAFTS

A shareholders' agreement acquired a drag-along clause between the circulated draft and the executed version; both sides denied inserting it. The §3 fields were useless: the author field read the law firm's template name; last-modified-by read a generic "Legal" account. The §4 ladder was decisive: the DMS check-in history attributed the version introducing the clause to a named associate's credentials at 19:52, with a check-in comment "per client call"; the diff isolated the clause; and the §5 transmission record showed that version sent by the associate to the other side's solicitor at 20:04 with a cover note listing "minor conforming changes". The §7 alternatives: delegation, shared login: were closed by the associate's own time-recording entry for the call and the sign-in log placing the session on her workstation. The clause had an author; the internal metadata had merely declined to name her.

EXAMPLE 2 · THE ANONYMOUS LETTER AND THE TEMPLATE IT WAS BORN FROM

An anonymous letter to a regulator alleging misconduct was produced as a PDF; the company suspected a named manager. The §3 examination of the PDF's XMP data recovered the source document's internal fields: author "K. Patel", a template identifier matching the company's internal memo template, and an application build deployed only to the finance department's machines. The §5 endpoint work on the manager's laptop found an autorecovery file containing an intermediate draft of the letter with tracked changes, and a jump-list entry for the source document at a time consistent with the PDF's creation stamp. The §6 stylistic comparison against the manager's known emails added a characteristic construction and two recurring misspellings. The §7 alternatives: a colleague using his machine, a template shared department-wide: were addressed from badge records (he alone was present) and the autorecovery file's location in his profile. The finding was graded "consistent with authorship by the manager and inconsistent with the alternatives considered"; the employment proceedings that followed turned on whistleblowing protection, not authorship.

EXAMPLE 3 · THE REPORT THAT CHANGED AFTER THE CLIENT SAW IT

A professional-negligence claim alleged a surveyor had softened a report's conclusions after the developer client complained. The surveyor's firm produced the final report with an author field naming the surveyor and a last-modified date preceding the complaint. The §4 ladder in the firm's cloud storage told a different story: the version containing the original, adverse conclusions saved by the surveyor's account on the Tuesday; a co-authored session on the Thursday: after the client's call: with three saves attributed to a partner's account; and the diffs showing the conclusions rewritten in that session. The internal last-modified date was explained by a later "save as" that reset it, visible in the ladder as a copy event. The §5 transmission record showed the softened version sent to the client from the partner's mailbox with no cover note. The surveyor had authored the report; the partner had authored the change; and the metadata that said otherwise had been the accident of a copy, not a lie: which the report stated, because honest attribution includes the innocent mechanism.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Author field as signature:** the template's creator pleaded as the document's author: the commonest error in the field.
- **Ladder unread:** the platform's per-save attribution never collected (guide 102 Example 3's default) while the argument ran on internal fields.
- **Co-authoring overclaimed:** the saving account named as sole editor of a shared session: §4's granularity ignored.
- **Endpoint released:** the machine holding the autorecovery draft reissued before imaging: guide 97 §3's afternoon, for authorship.
- **Style as proof:** a linguistic impression pleaded without methodology or the technical strata: §6's role inverted.
- **Alternatives unaddressed:** the shared PC, the generic login, the delegating principal: raised first by the opponent.
- **Copies examined, originals not:** the email attachment's fields read while the platform original's ladder sat uncollected.
- **The leap to the name:** "account X saved it" reported as "X wrote it" without the lattice: the grade the evidence did not earn.

Technical limitations

- **Metadata is editable and inheritable:** internal fields prove environment at best: always corroborated, never relied on alone.
- **Ladders prune and flatten:** guide 102 §4's clocks and traps bound the platform stratum; the alternates of §8 extend it.
- **Co-authoring blurs:** real-time sessions attribute at save granularity; per-paragraph attribution exists only where the application retained it.
- **Short texts resist stylometry:** linguistic attribution needs sufficient questioned and known material: the method's limits stated by the specialist who applies it.
- **Generative tools complicate authorship:** AI-assisted drafting shifts the question from typist to prompter and adopter: guide 126's evolving methods, applied with current caution.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Where does the original live: the platform, library and path: so the ladder, not just the copy, is collected?
- Who else had access to the drafting environment: shared machines, generic accounts, assistants: the §7 alternatives, listed now?
- Is there known writing by each candidate for the §6 comparison, and is the endpoint still unhandled?

Ask your opponent

- Please disclose the complete version history of [document] from its original platform location, with the modifying account, timestamp and content of each version, together with the audit-log edit events and any DMS check-in records for [period].
- Please identify the device(s) on which [document] was created and edited, the user profiles configured on them, the registered application user name at the relevant time, and the template from which the document was created.
- Please confirm preservation of those devices unaltered and disclose all transmissions of any version of [document], with sender, time and recipients.

Ask your eDiscovery / forensic provider

- Do the four strata agree on account, device, time and content: and where do they diverge?
- Has template inheritance been excluded for every author field relied on?
- What grade does the lattice support: environment, account, device, or person: and which alternatives remain open?

SUGGESTED WORDING · INSTRUCTION FOR AUTHORSHIP ATTRIBUTION

> "You are instructed to examine [document] and the sources listed in Schedule 1 to determine, so far as the evidence permits, the environment in which the document was created, the accounts and devices through which it was created and edited, the sequence and attribution of material changes, and the transmission of each version. Please examine internal metadata (with template inheritance and editability addressed), platform version histories and audit logs (with co-authoring attribution stated at its true granularity), endpoint artefacts including autorecovery and temporary files, and transmission records, and [where instructed] compare the content stylistically against the known writing at Schedule 2 under a stated methodology. Please address alternative explanations including shared devices or accounts, delegated drafting and metadata copying, grade each conclusion to the evidence supporting it, 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 authorship checklist

- ☐ Original platform location identified; ladder and audit log collected
- ☐ Internal fields read as environment; template inheritance checked
- ☐ Tracked changes, comments and revision data examined where retained
- ☐ Co-authoring sessions identified; attribution stated at true granularity
- ☐ Endpoint imaged; autorecovery, temp and recent-file artefacts examined
- ☐ Transmission records collected; sent states hash-matched to rungs
- ☐ Known-writing corpus assembled for stylistic comparison where warranted
- ☐ All strata normalised to one timeline; agreements and gaps shown
- ☐ Alternatives (shared, generic, delegated) addressed from evidence
- ☐ Finding graded: environment, account, device, person

Red flags

- Author fields naming template creators or generic users: Example 1's "Legal".
- Last-modified dates reset by copy or save-as: Example 3's accident.
- Ladders flattened or version export never enabled.
- Drafting on shared or hot-desk machines.
- Authorship allegations resting on style alone.
- Devices reissued before examination.
- Opposing findings that leap from account to name without corroboration.

When to involve a digital forensic expert

At preservation, so the ladder, the endpoint and the transmission records survive (guide 102 §5, guide 97 §3); at examination, where the four strata are collected, normalised and joined with template inheritance and co-authoring handled correctly (Examples 1-3's method); where content attribution is warranted, in instructing the right specialist under guide 100's disciplines; and at deployment, where the graded finding is evidenced under CPR Part 35 or CrimPR Part 19: or an opponent's overclaimed attribution is dismantled by the alternatives it never addressed. Through **cflab.uk** and **e-discovery.uk**, authorship work runs from the original's hold to the graded finding: because the document remembers its author, imperfectly, and the discipline is in the imperfections.

§ 13 · COMMON QUESTIONS

Frequently asked questions

The document's author field names my client. Doesn't that settle it?

No: the field records the application's registered user on the machine where the document (or its template, or the document it was copied from) was created, and it is editable (§3): Example 1's field named a template; Example 3's date was reset by a copy. It is evidence of environment, corroborated by the platform ladder and the endpoint before it becomes evidence of a person.

Can we prove who inserted a specific clause?

Frequently: the version ladder's diffs localise the change to a rung, the rung names the saving account and time, and the endpoint and transmission records corroborate the session (§4-§5): Example 1's 19:52 check-in. Co-authoring adds caveats about session granularity, and the account-to-person step needs its own corroboration, stated as such.

What about an anonymous document with all metadata stripped?

The stripping is rarely complete: PDF XMP data often preserves source fields, endpoints hold autorecovery drafts and recent-file entries, the template and application build narrow the population, and stylistic comparison adds weight (§3, §5-§6): Example 2's letter was attributed through all four. The counterpart's copy may also carry what the author cleaned from theirs (§8).

Several people edited the document together. Who is the author?

Each contributor of each change, at the granularity the platform retained: per-save attribution always, per-paragraph where the application kept it (§4): the report attributes the material changes to accounts and sessions and states where the granularity runs out. "Author" becomes a schedule, not a name: which is usually the truthful answer for collaborative documents.

Is linguistic analysis admissible and reliable?

Forensic linguistics is an established discipline with its own methodology and limits, instructed as a separate specialism (guide 100 §3) and weighed by courts on its stated method and the material available (§6): it corroborates the technical strata far more often than it stands alone, and short questioned texts limit it. The report should say which role it plays.

The document was drafted with an AI tool. Who is the author?

The question shifts to who prompted, who edited and who adopted the output: the prompting account and session, the platform ladder of subsequent edits, and the person who circulated it as their own (§6, guide 126): the technical strata still attribute the human acts around the generated text, and the legal question of responsibility follows those acts.

§ 14 · REFERENCE

Glossary

Attribution grade
The level a finding reaches: environment, account, device or person.

Author field
The internal metadata value set from the application's registered user.

Autorecovery file
An application's periodic draft save, preserving intermediate states.

Co-authoring attribution
Which account a shared session's save is credited to.

Editing-time counter
Office metadata's cumulative drafting-duration field.

Forensic linguistics
Authorship analysis from language features under stated method.

Registered user name
The identity an application writes into documents it saves.

Stylometry
Quantitative comparison of writing style across texts.

Template inheritance
Metadata carried from a template or copied source into a new document.

XMP data
Embedded metadata in PDFs and images, often preserving source fields.

Sources and authoritative references

The authorship-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 (authorship and edit attribution, metadata examination, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 07 · Analysis (version collection, metadata analysis and attribution as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft Learn, document properties and co-authoring: learn.microsoft.com, versioning · Adobe, XMP specification: adobe.com, XMP
- CPR Part 35 and PD 35: justice.gov.uk, Part 35 · CrimPR Part 19: justice.gov.uk, CrimPR 19 · PD 57AD: justice.gov.uk, PD 57AD
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Authorship work at the laboratory collects all four strata before it reads any of them: the original's platform ladder and audit log (guide 102's discipline), the endpoint imaged with its autorecovery and recent-file artefacts intact, the transmission records with sent states hash-matched to rungs, and the internal metadata read as environment with template inheritance excluded: then joins them on one timeline, addresses the shared-machine, generic-account and delegation alternatives from evidence, instructs forensic-linguistic comparison where the stakes warrant it, and grades the finding to what the lattice supports (Examples 1-3's method, including the innocent copy that reset a date). Reports run under CPR Part 35 and CrimPR Part 19; opposing attributions are audited for the leap from account to name. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a document's authorship is in dispute now, the version ladder and the drafting machine are the two sources that expire: hold them this week.

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