



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

SMS and iMessage Evidence

Message Databases, Cloud Sync, Deleted Threads, Timestamps and Attribution on the Phone's Native Channels

Before the apps, there were texts: and the phone's native channels remain where disputes surface with peculiar force: the drunken message, the resignation by text, the harassment thread, the "as discussed" that was never discussed. SMS and iMessage look identical in a bubble and could hardly differ more underneath: one a carrier-borne service with operator records and no encryption story, the other an Apple-encrypted, multi-device, cloud-synced ecosystem whose messages exist on every signed-in device and in backup lineages reaching years back. This guide takes the pair together and apart: the message databases and their deleted layers, the sync behaviours that make deletion propagate and preservation multiply, what green versus blue actually means evidentially, the recently-deleted windows and recovery realities, operator records as the independent spine, and the timestamp and attribution disciplines that keep native-channel exhibits standing.

© Estimated reading time: 26 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. Native-channel messaging runs through its casework from matrimonial to commercial: message-database examination with deleted-layer recovery, iCloud and backup archaeology, multi-device sync analysis, operator-record correlation, and the authentication work that has retired more than one fabricated thread. Its eDiscovery arm, **e-discovery.uk**, renders message collections reviewable at disclosure scale.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

MESSAGE-DATABASE FORENSICS

CLOUD & BACKUP ARCHAEOLOGY

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: two services in one inbox
03	The stores: message databases and their deleted layers
04	iMessage's ecosystem: sync, devices and backup lineages
05	SMS's ecosystem: carriers, operator records and RCS
06	Deletion and recovery: windows, propagation, realities
07	Timestamps, attribution and authentication
08	Source architecture: where else the evidence lives
09	Worked examples
10	Common mistakes and technical limitations
11	Questions to ask · Suggested wording
12	Checklist and red flags · When to involve a digital forensic expert
13	Frequently asked questions
14	Glossary · References · Disclaimer · How a specialist laboratory can assist

Executive summary

THE HEADLINE POINT: ONE INBOX, TWO ARCHITECTURES: AND THE ARCHITECTURE DECIDES WHERE THE EVIDENCE LIVES AND HOW IT DIES

iMessage is an ecosystem: Apple-encrypted messages delivered to every device signed into the account (iPhone, iPad, Mac, Watch), stored in message databases on each, synchronised through iCloud (where Messages-in-iCloud is enabled: one store, all devices, deletions propagating) or captured in device backups (where it is not: per-device stores, snapshotted by iCloud and computer backups): which means an iMessage thread typically exists in several places with different retention fates, the paired Mac's database (guide 61's message-mirror rescue) frequently outliving the phone's tidy-ups, and backup lineages reaching years into the past. Its deleted layer is generous by modern standards: a **recently-deleted window (around 30 days)** inside the app, unvacuumed database records beneath that at FFS level, and every backup taken pre-deletion. **SMS/MMS** is a carrier service: stored in the same device databases (one store handles both channels: why the examination is unified even when the services are not), unencrypted in transit, and shadowed by **operator records**: the independent, provider-held spine of who texted whom, when (traffic data on retention schedules; content not retained by UK operators): obtainable by appropriate legal process and immune to anything done to handsets. **RCS**, now flowing between platforms, sits between: richer features, provider infrastructure, evolving evidential behaviour checked per case rather than assumed. The practical method the split dictates: establish the account and settings facts first (Messages-in-iCloud on or off; which devices signed in; backup habits): because they determine whether deletion propagated or was captured, where the surviving copies sit, and which of the three recovery routes (window, database layer, lineage) is live; collect the device census, not the handset alone; and put contested threads through the §7 authentication stack: database internals, cross-device convergence, counterpart extraction, operator-record correlation: the native-channel version of the standard this series holds all messaging evidence to.

- **The settings facts come first:** Messages-in-iCloud state, device list, backup habits: three questions that route every deletion and recovery analysis.
- **The Mac is the quiet archive:** desktop message databases capture threads and outlive handset deletions: in the census, imaged early, repeatedly decisive.
- **The recently-deleted window is a gift with a clock:** around 30 days of recoverable deletions inside the app itself: checked before anything else, preserved by extraction.
- **Operator records are the independent spine:** traffic data proving message events regardless of handset fate: window-bound, requested early, content-free and honest about it.
- **Green versus blue matters evidentially:** channel determines encryption, provider posture and record trails: the bubble colour is the first classification, not a design note.

The problem in plain English: two services in one inbox

Users see one conversation stream; the law of evidence inherits two services with opposite characters.

iMessage is private in transit and promiscuous at rest: encrypted past interception, then copied to every Apple device the account touches and snapshotted by every backup: deletion is a project the user rarely completes. SMS is public in transit and singular at rest: one device store, no sync ecosystem: but shadowed for its traffic by an operator who cannot be texted into silence. Each service's weakness is the other's strength, and threads mix them freely: which is why the competent examination classifies before it concludes, and why "the texts" as a category conceals the first question every native-channel matter must answer.

The good news for practitioners: this is the most examined evidence class in mobile forensics, its stores and behaviours deeply understood, its recovery routes well-mapped, and its authentication methods mature. The failures in native-channel matters are almost never capability failures: they are the settings facts unasked, the Mac unimaged, the window missed, the operator request sent late: process failures this guide's checklists exist to end.

The stores: message databases and their deleted layers

- **One database, both channels:** the device's message store holds SMS, MMS and iMessage together (Android's equivalents likewise unify carrier and RCS traffic): per-message service flags, handles, timestamps at multiple stages, read states, attachment linkage and thread structure: the primary record, reached properly at FFS level per guide 61.
- **The deleted layers beneath:** the app-level recently-deleted store (its own table, its own window); flagged-unvacuumed records in the main store; journal and write-ahead residue: the three-deep recovery stack the examiner walks in order.
- **Attachments live adjacent:** media in linked stores and folders, persisting after messages delete: guide 63's attachments-outlive-chats rule, native edition.
- **Drafts, edits and unsends:** modern iMessage permits editing and unsending within short windows: both acts leave records (edit histories visible in-thread; unsend events with residue at recipients whose devices predate the feature or captured notifications): small windows, loud traces.
- **Desktop stores are full peers:** the Mac's message database is the same evidence class with its own deleted layer and its own backup presence (Time Machine): examined as a first-class source, not a curiosity.

iMessage's ecosystem: sync, devices and backup lineages

- **Messages-in-iCloud, on:** one synced store across devices; deletions propagate everywhere signed in; the cloud holds current state (collectable by the account-side route, guide 149) and device backups slim down accordingly: recovery leans on the window, the database layer and any device that fell out of sync.
- **Messages-in-iCloud, off:** per-device stores diverge; deletions are local; iCloud device backups and computer backups snapshot whole stores: recovery leans on the lineage and the unpurged peers: divergence itself dating deletions per guide 63's method.
- **The device census:** every signed-in device (phones, tablets, Macs, the Watch's cache) is a copy with its own fate: enumerated from account records and imaged by priority: the census question this block asks of everything, at its most productive here.
- **Backup lineages:** iCloud device backups (rolling, settings-dependent) and computer backups (iTunes/Finder, Time Machine: often years deep, encrypted ones richer): the time machines enumerated and preserved before any deletion is conceded: guide 158 takes them fully.
- **Family and shared wrinkles:** shared devices, children's synced iPads surfacing parents' threads, relay behaviours: the attribution complications flagged for §7 rather than discovered at trial.

SMS's ecosystem: carriers, operator records and RCS

- **Operator traffic records:** UK operators retain traffic data: numbers, timestamps, cell context for messages and calls: on limited retention schedules, disclosing under appropriate legal process (civil orders against operators being possible but exceptional; the criminal/regulatory routes better-worn): the independent record that survives every handset event, requested early because the windows do not wait.
- **No content from operators:** UK operators do not retain message content: the traffic spine proves events, not words: stated plainly in advice, with the words proved from devices and counterparts.
- **Delivery reports and service artefacts:** device-side delivery records and carrier service messages add texture: read with their semantics, claimed at their weight.
- **RCS's arrival:** the richer carrier-adjacent channel now bridging platforms: provider infrastructure, encryption postures and record trails in flux: per-case verification replaces assumption, and the classification question of §2 gains a third answer.
- **Number provenance:** SIM records, porting history and account ownership from operators: the number-to-person foundation attribution builds on (§7).

Deletion and recovery: windows, propagation, realities

- **The recovery order:** recently-deleted window (check first, extract fast) → database layer (FFS, before vacuum) → backup lineages (sets bracketing the deletion) → peer devices out of sync → counterpart phones: five rungs, walked in order, each honestly bounded.
- **Propagation cuts both ways:** synced deletion empties every live device: and misses the Mac left offline, the old iPad in the drawer, the backup taken Tuesday: the ensemble's standing rescue, found by the census.
- **Whole-thread deletion versus message picking:** selective deletion inside preserved threads reads differently from thread clears: the pattern layer, with the neighbours as context.
- **Unsend and edit residue:** the short-window features leave the traces §3 listed: checked whenever a thread's completeness is disputed.
- **Deletion as chronology:** window contents dated, vacuum states read, lineage brackets drawn, divergence compared: the act reconstructed even where content is not: and pleaded against the duty's dates per the series' standing method.

Timestamps, attribution and authentication

- **Timestamp semantics:** message stores record multiple stages (sent, delivered, read where enabled) in platform-specific epochs and zones: converted and stated explicitly, because chronology arguments have died on epoch arithmetic before now (guide 108's territory, previewed).
- **Attribution's ladder:** number → account → device → hand: operator provenance and account records fix the first two rungs; device artefacts and usage context the third; the series' join (guide 255) the fourth: pleaded to the rung the evidence reaches.
- **Cross-device convergence:** the same thread in the phone, the Mac and the backup, matching at record level: internal authentication before any counterpart is needed.
- **Counterpart extraction:** the other end's store, independently extracted: the two-ends standard (guides 53, 63) applied natively: the checkmate for contested threads.
- **Fabrication signatures:** impossible epochs, sequence anomalies, absent counterpart and backup presence, store internals inconsistent with the claimed history: the workup that ends screenshot cases (guide 63's Example 3 transfers whole).

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine one handset's messages in isolation. The thread's evidence spans: every signed-in Apple device with its own store and deleted layer; the iCloud account (synced store or device backups, on the account-side route); computer backup lineages (iTunes/Finder, Time Machine) on every machine that ever hosted them; the counterpart's equivalent stack; operator traffic records for the carrier-borne channels; the Watch and companion caches at the edges; and the export/screenshot trail participants created. When the primary handset is locked, wiped or hostile: guide 62's posture: the Mac, the lineage and the counterpart carry the case, and the operator spine frames the events whatever became of the words.

EVIDENCE	PRIMARY DEVICE (FFS)	PEER DEVICES (MAC, IPAD)	ICLOUD (SYNC/ BACKUPS)	COMPUTER BACKUPS	COUNTERPART + OPERATOR	DELETED / RECOVERABLE
iMessage threads	Y + window + database layer	Y: the quiet archive	Y, per settings	Y: years deep	Their stack; no operator record	Five-rung ladder; propagation's misses
SMS/MMS threads	Y + layers	Relay copies sometimes	In device backups	Y	Their store + operator traffic	Device layers + counterpart; operator events regardless
Attachments	Y + adjacent stores	Synced	Y	Y	As received	Outlive messages
Deletion acts	Window + vacuum + flags	Divergence dating	Bracketing backups	Bracketing sets	Their intact copy	The act reconstructs
Edits / unsends	Histories + residue	Pre-sync states	As at backup	As at backup	Recipient-side traces	Short windows, loud traces

Fallback strategy in one line: ask the Mac, then the lineage, then the counterpart, and let the operator prove the events: the native channels are the best-shadowed evidence in mobile practice, and the shadow rarely all fails at once.

Worked examples

EXAMPLE 1 · THE MAC THAT REMEMBERED THE RESIGNATION

A director denied sending the late-night iMessage resigning his position and "confirming" the transfer of his loan account: his iPhone, produced weeks later, showed no such thread, and Messages-in-iCloud had synced the deletion everywhere. Almost everywhere: his office iMac, powered down for a fortnight's leave when the deleting happened, rejoined the world with the thread intact in its message database: record-level content, sent-timestamps in the store, and the deletion's date bracketed by the iMac's last-sync marker. The chairman's phone: the counterpart: converged exactly. The denial was withdrawn at the door of court; the iMac's fortnight of sleep appears in the judgment as "a fortunate hibernation".

EXAMPLE 2 · THE WINDOW THAT CAUGHT THE WEEKEND EDIT

A harassment respondent, served on a Friday, spent the weekend curating: sixty-one messages deleted from three threads before his Monday handover of the phone. He had not known about the recently-deleted store: the extraction, run Tuesday, recovered all sixty-one from the window with their deletion timestamps (Saturday 22:10 to 23:35), alongside the intact threads showing exactly what the curation had tried to reshape. The tribunal read the messages, then the deletion chronology, then the selection pattern: the worst messages gone, the context kept: and its findings on credibility begin there. Thirty days of grace, spent by the person it was never designed to help.

EXAMPLE 3 · THE OPERATOR RECORDS THAT OUTLIVED BOTH PHONES

A loan dispute turned on whether demand texts were sent across 2023: by trial, the claimant's phone was long-replaced and the defendant's "lost in a house move". The words were gone; the events were not: operator records, obtained by order early in proceedings while the retention window lived, showed forty-two messages from the claimant's number to the defendant's across the pleaded dates, clustering around each missed instalment: and the defendant's own sporadic replies. Content-free, the traffic pattern still did the work: demand, response, demand: and the defence of "no demand was ever made" did not survive its own reply timestamps. The early operator request, made when both phones still existed, had future-proofed the case against both their fates.

Common mistakes and technical limitations

Common mistakes

- **Settings facts unasked:** recovery strategies built without the iCloud-sync state: propagation surprises both ways.
- **The census as handset-only:** Example 1's iMac never imaged; the Watch, iPad and desktops outside scope.
- **The window missed:** extraction scheduled past thirty days while the recently-deleted store held everything.
- **Operator requests sent late:** Example 3's inverse: retention windows lapsed while correspondence pondered.
- **Channel-blind analysis:** SMS and iMessage undifferentiated: operator spines unpursued for carrier traffic, impossible provider routes pursued for Apple traffic.
- **Screenshot tenders:** guide 63's disease, native strain: exhibits without extractions.
- **Epoch arithmetic fumbled:** chronologies argued on unconverted or zone-naïve timestamps.
- **Lineages unpreserved:** computer backups overwritten on schedule mid-dispute: the time machines left running.

Technical limitations

- **Windows and vacuums close:** the recovery ladder's rungs are time-bound: early extraction is the only guarantee, as everywhere in this block.
- **Operator retention is finite and content-free:** the spine proves events within its window, words never: both limits stated in advice.
- **Synced deletion is genuinely effective:** a disciplined deleter with all devices live and no lineage can succeed: the honest case exists, and the report says when it is this one.
- **Read receipts are settings-dependent:** their absence proves a setting, not ignorance: claimed accordingly.
- **Attribution stops at the rung reached:** the ladder's honest summit varies per case: number-level findings are not hand-level findings, and the report keeps the rungs distinct.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The settings facts: Messages-in-iCloud state, full device list, backup habits (computer and cloud): today, in writing?
- Which threads matter, mixing which channels: and has anyone deleted, edited or unsent anything the file should honestly record now?
- Are the operator requests justified and in motion while the retention windows live?

Ask your opponent

- Please preserve all message data of [custodians] across all devices signed into the relevant accounts, all iCloud data, and all computer backups: with no deletion, unsend, settings change, device removal or backup overwrite: and state the Messages-in-iCloud position and complete device list.
- For produced threads: please state source device, extraction level and tool, and whether any message in the period was deleted, edited or unsent, with dates from the recently-deleted store and database layer.
- Where a device is said to be lost or replaced: please give particulars and confirm the position on its backups and peer devices.

Ask your eDiscovery / forensic provider

- What do the window and database layer hold for the disputed threads: and how long before the rungs close?
- What does the census add: peers, lineages: and in what imaging order?
- For the contested exhibit: what does the convergence-and-counterpart workup support?

SUGGESTED WORDING · NATIVE-CHANNEL LIMB FOR THE PRESERVATION LETTER

"Your client must immediately preserve all SMS, MMS, RCS and iMessage data relating to the issues, including: (a) message stores on every device signed into the relevant Apple ID or Google account, none of which may be wiped, reset, synced-out or disposed of; (b) the recently-deleted message store, from which nothing may be cleared; (c) all iCloud data including Messages-in-iCloud and device backups, with no settings change to synchronisation or backup; (d) all computer backups (iTunes/Finder, Time Machine or equivalent), which must not be overwritten or pruned; and (e) all message threads as they stand, with no deletion, editing or unsending. Please confirm within [3] days, stating the Messages-in-iCloud position and listing every signed-in device with its location."

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

The native-channel checklist

- ☐ Settings facts established day one: sync state, device list, backup habits
- ☐ Census run beyond the handset: Macs, iPads, Watch, old devices in drawers
- ☐ Recently-deleted window checked and extracted inside its clock
- ☐ FFS extraction early; database layer walked before vacuum
- ☐ Backup lineages enumerated and preserved; bracketing sets identified
- ☐ Operator requests assessed and issued while retention windows live
- ☐ Channel classification run per thread: SMS, iMessage, RCS
- ☐ Timestamps converted and stated with epochs and zones explicit
- ☐ Contested threads put to convergence and counterpart workups
- ☐ Attribution pleaded to the ladder rung actually reached

Red flags

- Deletions clustered against service or duty dates: Example 2's weekend.
- A "lost" phone with unexplored peers and lineages.
- Threads produced from screenshots with extraction declined.
- Messages-in-iCloud toggled, or devices signed out, mid-dispute.
- Selective in-thread deletion among preserved context.
- Unsend and edit features exercised in the relevant window.
- Operator windows allowed to lapse unrequested.

When to involve a digital forensic expert

At the settings-and-census stage, where the routing facts are fixed and the quiet archives found (Example 1's iMac); inside the windows, where the recently-deleted store and vacuum clocks make extraction urgent (Example 2's rescue); at the operator interface, where the request's technical content and timing decide whether the spine exists (Example 3's foresight); and at authentication, where convergence, counterparts and fabrication signatures are the laboratory's stock method. Reported under CPR Part 35 with rungs, windows and semantics stated: and through **e-discovery.uk**, native threads land in review beside the case's other channels, assembled per guide 70.

§ 1 3 · COMMON QUESTIONS

Frequently asked questions

Can deleted texts be recovered?

Walk the ladder: the recently-deleted window (about 30 days: routinely yes); the database layer at FFS (yes while unvacuumed); backup lineages bracketing the deletion (yes where habits existed); out-of-sync peers (Example 1's answer); counterpart devices (their copy, regardless). A disciplined deleter can defeat all five: rarely does: and the deletion's own chronology survives in any event. The realistic answer, most cases: substantially, if extraction moves early.

Can we get message content from the phone companies?

No: UK operators retain traffic data (numbers, times, cell context) on limited schedules, not content: Example 3 shows what the traffic spine can nonetheless prove. Content lives at the ends: devices, backups, counterparts: and for iMessage the operator holds nothing at all (Apple-carried, not carrier-borne). The advice pairing: operator requests early for events; device work for words.

Someone unsent a message. Is it gone?

Rarely cleanly: the unsend window is short; recipients on older systems keep the message outright; notification residue captures first lines; the sender's own store carries the unsend event with residue; and any backup or peer syncing before the unsend holds the original. The feature is loud: the attempt is usually easier to prove than the message would have been to deny: the delete-for-everyone lesson of guide 63, restated for the native channel.

How do we prove who actually sent a text from a shared or accessible phone?

The ladder's fourth rung, built not assumed: device-side context (unlock methods and their users, usage artefacts around the sending, location consistency), account context (who else knew the passcode: the pool named honestly), style and content coherence, and the surrounding conduct. Sometimes the summit is reached; sometimes the honest finding is number-and-device level with the pool stated: guide 255 takes the full question, and this series' standing rule applies: the report claims the rung, never the assumption.

The thread mixes green and blue bubbles. Does the analysis change mid-conversation?

Yes, message by message: the store's service flags classify each record, and each class carries its own transit posture, provider shadow and recovery ecosystem: an operator record exists for the green message and not its blue reply; the blue message syncs to the Mac and the green may not. The unified examination handles this natively: the point for lawyers is not to argue channel-specific propositions ("the operator will confirm it") across a mixed thread unclassified.

What single step best protects a native-channel case this week?

The pairing this guide keeps repeating: early FFS extraction (the window and vacuum clocks) plus the operator request (the retention clock): the two moves with genuine stopwatches. Everything else: census, lineages, counterparts: improves with time or at least survives it; those two only decay. If the matter has texts at its centre and neither is in motion, that is today's work.

§ 1 4 · REFERENCE

Glossary

Bracketing sets

Backups before and after a deletion; the dating pair.

Census (device)

Every signed-in device; the ecosystem's copy list.

Epoch conversion

Platform timestamp arithmetic; chronology's unglamorous foundation.

Ladder (attribution)

Number → account → device → hand; pleaded to the rung reached.

Messages-in-iCloud

The sync setting routing every deletion and recovery analysis.

Operator traffic records

Provider-held event data; the independent spine, content-free.

Quiet archive

The out-of-sync peer (typically a Mac) that missed the deletion.

Recently-deleted store

The app's ~30-day recoverable deletion window.

Service flags

Per-record channel classification: SMS, MMS, iMessage, RCS.

Unsend residue

The traces the short-window features leave at both ends.

Sources and authoritative references

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

- cflab.uk, digital forensics services (message-database forensics, backup archaeology, operator-record correlation, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation, Phase 03 · Collection and Phase 04 · Processing (ecosystem preservation; threads into review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- College of Policing, extraction guidance: college.police.uk · communications data and operator disclosure context: [IPCO](https://ipco.org.uk)
- ISO/IEC 27037: iso.org, [27037](https://iso.org/27037) · Forensic Science Regulator: gov.uk/forensic-science-regulator
- PD 57AD and CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad) · justice.gov.uk, [Part 35](https://justice.gov.uk/part-35) · ICO: ico.org.uk

DISCLAIMER

This publication provides general information about SMS and iMessage evidence as at August 2026. Platform behaviour, sync mechanics, recovery windows and operator retention practices change and vary by version, configuration and provider; verify the current position for the devices and services in the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Native-channel matters at the laboratory run on the two stopwatches: early FFS extraction inside the window and vacuum clocks, and operator-request support while retention lives: with the settings facts and device census fixed in the first calls. The recovery ladder is walked rung by rung with honest bounds; the quiet archives (Example 1's iMac class) are found by the census and imaged early; deletion chronologies (Example 2's machinery) are built from windows, flags and brackets; and contested threads get the convergence-counterpart-fabrication workup as standard. Reporting is CPR Part 35 with rungs, windows, epochs and semantics stated; through **e-discovery.uk**, native threads join the estate's other channels in one assembled record. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a message-centred matter has neither extraction nor operator request in motion, that pairing is today's instruction.



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