COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

WhatsApp Evidence

Databases, Backups, Deleted Messages, Groups and Linked Devices: the App That Runs UK Business on the Side

WhatsApp is where the candid version of UK commerce happens: deals sketched, instructions given, warnings shared, all in an app people treat as private conversation and courts treat as disclosure. Its end-to-end encryption protects messages in transit and does almost nothing to keep them out of litigation: the evidence lives at the ends, in device databases, computer and cloud backups, linked-device copies and the other participants' phones. This guide maps the WhatsApp architecture for lawyers: where the databases sit and what their internals betray, how backups extend reach into the past, what delete-for-me and delete-for-everyone each actually leave, why groups multiply both evidence and preservation duty, how disappearing messages change the race, and the authentication work that separates a real thread from a fabricated screenshot.

⏱ Estimated reading time: 27 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. WhatsApp analysis features in most of its employment, commercial and matrimonial casework: FFS-level database examination, backup archaeology, deleted-message recovery within honest limits, group reconstruction across participants, and the authentication work that screenshots alone can never carry. Its eDiscovery arm, **e-discovery.uk**, renders chat collections reviewable at disclosure scale.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | WHATSAPP & CHAT FORENSICS | BACKUP & DELETED-DATA ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: WHATSAPP'S ENCRYPTION GUARDS THE WIRE, NOT THE ENDS: AND LITIGATION LIVES AT THE ENDS

End-to-end encryption means providers cannot read messages in transit: it says nothing about the copies at rest, which are the evidence. **On the device:** WhatsApp keeps its messages in local databases (msgstore-family stores on Android, ChatStorage-family on iOS) whose internals: reached at FFS level per guide 61: include delivery and read timestamps, edit and deletion traces, and records flagged deleted but unvacuumed: the routine recovery layer. Media lives separately in app folders and caches, outliving the chats that carried it. **Around the device:** backups extend reach into the past: local Android backup files, iCloud and Google Drive backup sets (whose own encryption status depends on the user's settings), and iTunes/Finder computer backups that snapshot the whole store: each a point-in-time WhatsApp that survives on-device deletion, making backup enumeration the first move of every deleted-message dispute. **Across devices:** linked devices (WhatsApp Web, desktop apps, companion phones) hold their own synced copies and their own artefacts (session records, cached media, browser traces): the census question again. **At the other ends:** every chat exists on every participant's phone: the counterpart layer that rescues cases when the primary device is locked, wiped or hostile, and that makes group chats evidence multiplied by membership. Deletion is architecture-specific: **delete-for-me** removes the local display and leaves the database layer, the backups and every other participant untouched; **delete-for-everyone** requests removal at all ends within its time window, works only prospectively, leaves a "message deleted" placeholder and notification residue, and does nothing to backups already taken: so "the messages are gone" decomposes, as always, into which copies, at which layer, against which clocks. The clocks that matter: backup rotation and settings, **disappearing-message timers** (which delete on schedule at every end and convert preservation into a genuine race: §6), and the linked-device session lifetimes: all answered by the same discipline this block keeps teaching: freeze the ecosystem on day one, then argue.

- **The database layer is the evidence class:** FFS-level extraction reaches internals: timestamps, deletion traces, unvacuumed records: that no export or screenshot carries.
- **Backups are time machines:** local, cloud and computer backup sets each snapshot the store: enumerated and preserved before anyone concedes deletion.
- **Delete-for-everyone is loud:** placeholders, notification residue and counterpart copies pre-window make it among the most detectable deletions in mobile evidence.
- **Groups distribute the archive:** N participants means N copies plus N backup lineages: preservation letters go to the membership, not just the opponent.
- **Screenshots are claims, not evidence:** trivially fabricated, routinely challenged: authentication runs through extractions, database internals and counterpart convergence (§7).

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: encrypted in transit, everywhere at rest

WhatsApp's marketing and its evidential reality point in opposite directions, and both are true. The encryption is real: interception is not a route, and provider disclosure yields account records rather than message content. And the ubiquity is real: the same message rests on the sender's phone, every recipient's phone, several backup lineages and any linked desktops: five, ten, fifty copies for a busy group: each governed by its own owner, settings and clocks. The practical consequence inverts the lay expectation: WhatsApp evidence is usually not hard to obtain: it is hard to obtain from one uncooperative place, and easy to obtain from somewhere, provided the map is drawn and the preservation moves early.

The lawyer's task is therefore mapping and racing: identify the chats and their membership, enumerate the devices and backup lineages, issue the preservation instructions (including to third-party participants where the case justifies it), and beat the timers: disappearing messages, backup rotation, departing custodians: that are the only genuine destroyers in the architecture. Everything after that is guide 61's ordinary craft.

§ 0 3 · THE ARCHITECTURE

The architecture: databases, media, backups, linked devices

COMPONENT	WHAT IT HOLDS · WHAT MATTERS
Device databases	The message stores with per-message metadata: timestamps (sent/delivered/read where enabled), sender identifiers, quoted-message linkage, edit and deletion traces: plus the unvacuumed deleted layer FFS extraction reaches. The primary record; everything else corroborates it.
Media stores	App media folders, caches and thumbnails: attachments persisting after chats are deleted; sent media in device galleries; media referenced across chats by hash: the layer that outlives conversations.
Local backups (Android)	Rotating encrypted backup files on-device: a short archaeology of recent store states, imaged with the device.
Cloud backups	iCloud (iOS) and Google Drive (Android) backup sets on user-controlled schedules and encryption settings: point-in-time stores surviving device loss and deletion; preserved via the account-side legal route; end-to-end-encrypted backups depend on the user's key material.
Computer backups	iTunes/Finder and equivalent device backups containing the WhatsApp store as at backup date: guide 158's territory, and the quiet star of deleted-message recovery.
Linked devices	Desktop apps, WhatsApp Web sessions, companion devices: synced message copies, session artefacts, cached media, browser traces: enumerated in the census, imaged where they matter.
Exports and forwards	User-generated chat exports, forwarded threads, email-to-self copies: secondary evidence with its own authentication needs, and often the first thing a client produces.

§ 0 4 · WHAT DELETION LEAVES

Deletion: for-me, for-everyone, and what each leaves

- **Delete-for-me:** local display removal only: the database layer may retain the record unvacuumed; backups pre-deletion retain it entirely; every other participant retains it untouched: the weakest deletion in the architecture, and the easiest recovery brief.
- **Delete-for-everyone:** removal requested at all ends, within the app's time window, prospectively only: leaving "this message was deleted" placeholders (themselves timestamped evidence of the act), surviving in any backup taken before the deletion, and frequently surviving in notification records and counterpart artefacts: loud, dated, and often more probative than the message would have been.
- **Chat and account deletion:** whole-chat clears and account removals follow the same logic at scale: local stores affected, backups and counterparts not: plus account-level events (deregistration, number changes) that are themselves chronology.
- **The vacuum caveat:** database housekeeping eventually purges flagged records: recovery windows are real but finite, which is one more reason extraction happens early rather than eventually.
- **Deletion as conduct:** placeholders clustered against duty dates, chats cleared selectively among intact neighbours, backup settings changed mid-dispute: the pattern layer, read per guide 60's method and pleaded with its dates.

§ 0 5 · GROUPS

Groups: multiplied evidence, multiplied duty

- **Membership is the evidence map:** the participant list: with join/leave events, admin actions and name changes, all recorded: defines where copies live and who owes preservation: the group's history is often as probative as its messages ("who added the competitor's director, and when").
- **Every member is a source:** the locked primary phone is one of N: cooperative members' devices, extracted properly, carry the thread with their own database internals: the standing rescue of hostile-custodian cases.
- **Divergence is chronology:** members' copies differ by their deletions, join dates and clearing habits: differencing the copies dates the deletions: the multi-device comparison that turns "gone" into "gone from his phone on the 14th".
- **Business groups are disclosure populations:** deal groups, project groups, management groups: scoped, preserved and collected as custodial sources in commercial matters, with PD 57AD's cooperation machinery applied to their membership.
- **Third-party members raise their own questions:** preservation requests, non-party disclosure applications and proportionate handling for members outside the litigation: planned, not improvised.

§ 0 6 · THE RACE

Disappearing messages and the preservation race

- **Timers delete at every end:** disappearing-message settings (24 hours to 90 days) remove messages on schedule from all participants' devices: the one mechanism in the architecture that genuinely destroys across the ensemble: and its enabling is itself a recorded, dated act.
- **Backups complicate the timer:** messages backed up before expiry can persist in backup sets: the timer races the backup schedule, and the enumeration of §3 decides who won.
- **View-once media is designed evanescence:** minimal residue by design: notification records, screenshots where taken, and recipient-device artefacts are the honest limits.
- **The enabling event is evidence:** a business chat switched to disappearing mode the week a dispute crystallised reads exactly as it is: the settings history, recovered from database internals and counterpart devices, joins the conduct layer.
- **The race is won in hours:** where disappearing modes are suspected, extraction and counterpart preservation are same-week work: the only section of this guide with a genuine stopwatch.

§ 0 7 · IS IT REAL?

Authentication: threads, exports and the screenshot problem

- **Screenshots are the weakest tender:** trivially fabricated with off-the-shelf tools, unmoored from metadata, and routinely challenged: never the foundation where anything better exists, and corroboration-only where nothing does.
- **Chat exports are better, not sufficient:** user-generated text/media exports carry structure but are editable artefacts: authenticated by comparison against extracted stores, not accepted on format.
- **The database is the authenticity anchor:** internal consistency (identifiers, sequence, timestamp coherence, quoted-message linkage) is difficult to fabricate at depth: the examiner's first read on any challenged thread.
- **Counterpart convergence is the checkmate:** the same thread extracted from independent participants' devices, matching at the record level: the two-ends method this series runs for email (guide 53), applied to chat, and the standard to which contested WhatsApp exhibits are put.
- **Fabrication has signatures:** impossible timestamps, sequence anomalies, absent database residue on the alleged sender's device, divergence from every counterpart: the §7 workup that has ended more than one case in this series' examples: and ends one below.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine one phone's WhatsApp in isolation. The thread's evidence spans: the primary device's databases, media stores and local backups; the account's cloud backup lineage (iCloud/Google Drive, on the account-side legal route); computer backups on every machine the phone ever synced with; linked desktop and web sessions with their artefacts; every other participant's equivalent stack; notification records and paired wearables' caches at the edges; provider records (account, registration, group metadata via legal process: not content); and the export/forward trail the participants themselves created. When the primary device is locked, wiped or hostile: guide 62's position: the counterpart stacks and backup lineages are the case, and the day-one preservation letters to the membership are what keep them alive.

EVIDENCE	PRIMARY DEVICE (FFS)	CLOUD BACKUP LINEAGE	COMPUTER BACKUPS	LINKED DEVICES	COUNTERPART PARTICIPANTS	DELETED / RECOVERABLE
Messages	Y + unvacuumed layer	Point-in-time stores	Point-in-time stores	Synced copies	Y: N further copies	For-me: routinely; for-everyone: pre-window copies + placeholders
Media	Y + caches, galleries	In backup sets	Y	Cached	As received	Outlives chats
Group history	Y: events in store	Snapshotted	Snapshotted	Synced	Y, per member tenure	Join/leave/admin events persist
Deletion acts	Placeholders, traces, vacuum state	Bracketing sets	Bracketing sets	Placeholder sync	Divergence dating	The act outlives the message
Settings (timers etc.)	Y: store internals	As at backup	As at backup	Synced state	Their records of the change	The enabling event is evidence

Fallback strategy in one line: when one end goes dark, the thread survives at every other end and in every backup taken before the trouble: preserve the membership and enumerate the lineages before conceding a single message.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DELETE-FOR-EVERYONE THAT DATED ITSELF

A director denied instructing a below-cost bid, and the key messages showed only as "this message was deleted" on the recipient's phone. The layered analysis rebuilt everything: the recipient's device retained notification records preserving the messages' first lines; the sender's own FFS extraction held the records flagged deleted with the deletion timestamps: 23:47, the night the audit was announced: and his Google Drive backup, taken on its weekly schedule two days before the deletion, held the complete thread. The tribunal read the instruction from the backup, the panic from the timestamps, and the character of the exercise from the placeholders. Delete-for-everyone had worked exactly as designed: and evidenced exactly as this guide describes.

EXAMPLE 2 · THE GROUP THAT OUTVOTED THE WIPED PHONE

A departing sales head factory-reset his phone on his last day: guide 61's Example 3 move: and the "Projects: Confidential" group he had run went with it, he assumed. The group had eleven members. Four cooperated immediately; their extractions each carried the full thread with matching record-level content, including his instructions to divert two accounts to his new employer: and the divergence analysis dated his own selective deletions (three specific messages, deleted-for-everyone, six weeks before departure: inside the window on two members' phones whose backups predated the deletion). One phone was ash; the archive had ten backups. The injunction application quoted the thread with four independent sources footnoted, and the reset became the conduct exhibit it always becomes.

EXAMPLE 3 · THE SCREENSHOT THREAD THAT NEVER EXISTED

A claimant in a partnership dispute produced screenshots of a WhatsApp exchange in which the respondent allegedly conceded a 40% profit share. The respondent denied the conversation entirely: and the forensic workup agreed with him. His device's FFS extraction showed no trace of the thread at any layer: no records, no deletion flags, no placeholders, no vacuum residue: in a store whose other chats with the claimant were intact and continuous; the claimant declined extraction of her own device, offering only further screenshots; and image analysis of the screenshots found font-rendering and layout inconsistencies matching a chat-mockup generator's output. The claim's central exhibit was withdrawn mid-trial, and the costs judgment's language about screenshot evidence tendered without underlying extraction has been quoted in seminars since.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Screenshot cases:** Example 3's tender: exhibits without extractions, standing until challenged, falling when met.
- **Single-device thinking:** the locked or wiped primary treated as the archive's death: Example 2's inverse.
- **Backup lineages unenumerated:** cloud and computer sets unpreserved while deletion is litigated: the time machines left running toward overwrite.
- **The race unrun:** disappearing-mode suspicions met with ordinary timescales: the only genuinely destructive mechanism, given its head start.
- **Group membership unpreserved:** letters to the opponent alone, ten other archives left to their habits.
- **Logical-level absence findings:** guide 61's Example 1 replayed on WhatsApp: "no messages" from extractions that never reached the database layer.
- **Linked devices forgotten:** the desktop session and companion phone outside the census.
- **Export-as-evidence:** user exports produced as primary where extraction was available: authentication debt incurred for no reason.

Technical limitations

- **Vacuum windows close:** the unvacuumed layer is finite: early extraction is the only guarantee.
- **End-to-end-encrypted backups gate on key material:** user-held keys govern access to E2EE backup sets: the credentials conversation extends to backups.
- **Provider content is not a route:** account and group metadata via legal process, yes; message content, no: the architecture's design, stated plainly in advice.
- **View-once and expired timers keep their promises:** residue is minimal by design: the honest limit, with notification and counterpart edges the only softening.
- **Attribution is the number, not the hand:** a WhatsApp account proves a registered number's participation: the join to a person runs through guide 61's method and guide 255's discipline.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which chats and groups carry the issues: membership lists, admin history, and any disappearing-mode settings?
- The lineage census: cloud backup account and schedule, computer backups, linked devices: enumerated and preserved today?
- Has anyone deleted, cleared, exported or screenshot anything: and is the honest account of that in the file before the other side finds it?

Ask your opponent

- Please preserve, and confirm preservation of, all WhatsApp data of [custodians]: device stores, local and cloud backups, computer backups and linked devices: with no deletion, clearing, settings change (including disappearing-message settings) or account action.
- Please state, per produced thread: the source (extraction level, device, tool) and whether any message in the period was deleted (for-me or for-everyone), with dates.
- Where screenshots or exports are tendered: please produce the underlying extraction or confirm none exists, and make the source device available for examination.

Ask your eDiscovery / forensic provider

- What does the database layer show for the disputed thread: internals, deletion traces, vacuum state?
- Which backup sets bracket the alleged deletions, and what does the divergence analysis date?
- For the challenged exhibit: what does the counterpart-convergence workup support?

SUGGESTED WORDING · WHATSAPP LIMB FOR THE PRESERVATION LETTER

> "Your client must immediately preserve all WhatsApp evidence relating to the matters in issue, including: (a) all device message stores and media, with no deletion (for-me or for-everyone), chat clearing, archiving changes or account actions; (b) all backups: local, Google Drive/iCloud and computer backups: with automatic backup settings left unchanged and no backup deleted or overwritten so far as within your client's control; (c) all linked devices and sessions, which must not be unlinked; and (d) all settings relevant to retention, including disappearing-message timers, which must not be enabled, changed or relied upon. Please confirm within [3] days that these steps have been taken, identify all groups relevant to the issues with their current membership, and confirm that this letter has been forwarded to any group administrator within your client's control."

§ 12 · QUICK CONTROL

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

The WhatsApp checklist

- ☐ Chats, groups and membership mapped; preservation to the membership where justified
- ☐ Lineage census: cloud schedule, computer backups, linked devices: enumerated day one
- ☐ Disappearing-mode check run; the race recognised where timers exist
- ☐ FFS extraction early: the vacuum window respected
- ☐ Deletion findings tied to layer: for-me vs for-everyone vs vacuumed: with dates
- ☐ Backup sets bracketing key dates identified and preserved
- ☐ Counterpart extractions pursued for contested threads
- ☐ Screenshots and exports treated as leads, authenticated or replaced
- ☐ Settings histories (timers, backups) recovered and read as conduct where they date suspiciously
- ☐ Attribution built to the number-then-person standard, never assumed

Red flags

- Placeholders clustering against duty dates: Example 1's signature.
- Disappearing mode enabled after the dispute crystallised.
- A tendered thread absent from the alleged sender's store at every layer: Example 3's tell.
- Backup settings changed, or sets deleted, mid-dispute.
- "No messages found" from logical-level examinations.
- Refusal to submit the source device behind screenshot exhibits.
- A wiped phone whose group had cooperative members nobody asked.

When to involve a digital forensic expert

At preservation, where the lineage census and the membership letters decide what survives; at the race, where disappearing modes make extraction same-week work; at recovery, where the database layer, backup bracketing and divergence dating are laboratory craft (Examples 1-2's machinery); and at authentication, always: contested threads get the counterpart-convergence workup, and screenshot exhibits get Example 3's treatment before they get into bundles. Reported under CPR Part 35 with layers, windows and limits stated: and through **e-discovery.uk**, chat collections rendered threaded and reviewable beside the estate's other sources, per guide 70's cross-platform assembly.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can WhatsApp itself give us the messages?

No: end-to-end encryption means the provider holds no readable content, and legal process against the platform yields account, registration and group metadata at most. The content routes are the ends: devices, backups and participants: which is why this guide is an architecture map rather than a subpoena template. Business API deployments (companies running WhatsApp through business tooling) are the exception worth checking: their message flows may be archived enterprise-side.

Messages were deleted months ago. Realistic prospects?

Decomposed, per §4: for-me deletions: good prospects via database layer (if extraction comes before vacuum), backups and counterparts; for-everyone: placeholders plus any backup or notification residue pre-window, plus counterpart copies where the window missed; vacuumed and unbacked: the honest no, with the deletion's own record remaining. The single best predictor is backup lineage: a weekly cloud backup habit means the question is usually "which set", not "whether".

Are WhatsApp messages even admissible: aren't they hearsay?

They are documents, disclosed and admitted like any other, with hearsay rules applying to their contents as they would to a letter: the practical battleground is authenticity and completeness, not admissibility: which is why §7's workups matter more than evidence-law anxiety. Present threads threaded, sourced and complete (selective quotation invites the completeness attack), with the extraction pedigree stated: the presentation disciplines of guide 56 §13 apply.

The other side produced a chat export. Do we accept it?

As a start, not an end: exports are editable text artefacts. The §11 request asks for the underlying extraction and source-device access; the comparison (export against extracted store, and against your client's own copy of the thread) is quick and decisive; and divergences: messages present in one, absent in the other: are findings, not formalities. Accept nothing contested on format alone.

Our client screenshot everything and deleted the originals "to save space". How bad?

Recoverable, usually: the screenshots become leads; the database layer may retain the deleted records if extraction moves fast; backups predating the clear-out likely hold the threads; and counterparts hold their ends regardless. The honest account of the deletion goes in the file now: innocent housekeeping explained early reads entirely differently from the same facts excavated by the other side later. Then the ordinary machinery runs.

Do we need every group member's phone?

Rarely: two or three independent, cooperative members' extractions converging at record level authenticate a thread to the standard courts need (Example 2 used four of eleven); the selection favours members with long tenure, intact stores and backup habits. The full membership matters for preservation (letters) and for divergence analysis where deletion dating is itself in issue: collection scales to the questions, per the proportionality dial this series runs everywhere.

§ 14 · REFERENCE

Glossary

Counterpart convergence
Record-level matching across independent participants' extractions; the authentication standard.

Delete-for-everyone
All-ends removal within a window, leaving placeholders and pre-window copies.

Delete-for-me
Local display removal; the weakest deletion in the architecture.

Disappearing messages
Timer-based all-ends deletion; the genuine race.

E2EE backup
User-key-encrypted backup set; access gates on key material.

Lineage census
The enumeration of local, cloud and computer backup sets.

Linked devices
Desktop, web and companion sessions holding synced copies.

Placeholder
The "message was deleted" marker; timestamped evidence of the act.

Unvacuumed layer
Deleted-flagged records persisting in the database; the routine recovery class.

View-once
Designed single-view media; minimal residue by intent.

Sources and authoritative references

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

- cflab.uk, digital forensics services (WhatsApp and chat forensics, backup archaeology, authentication workups, 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 (chat preservation to the membership; threaded rendering 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 of material from digital devices: college.police.uk · Forensic Science Regulator: gov.uk/forensic-science-regulator
- ISO/IEC 27037: iso.org, 27037
- PD 57AD and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · ICO: ico.org.uk

DISCLAIMER

This publication provides general information about WhatsApp evidence as at August 2026. Application behaviour, backup mechanics and deletion features change on the provider's schedule and vary by platform and version; verify current behaviour for the devices 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

WhatsApp matters at the laboratory run on this guide's map: the lineage census and membership preservation in day one; the disappearing-mode check with its stopwatch; FFS extraction inside the vacuum window; backup bracketing and divergence dating for every deletion dispute (Examples 1-2's machinery); and the authentication workups: database internals, counterpart convergence, screenshot analysis: that Example 3 models and contested exhibits require. Business-API archive checks, provider metadata routes and the number-to-person join complete the method. Reporting is CPR Part 35 with layers and windows stated; through **e-discovery.uk**, threads land in review whole, threaded and beside the case's other channels per guide 70. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a disappearing timer may be running on your matter's chats, that call outranks reading the rest of this page.

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