



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

Signal and Ephemeral Messaging

Disappearing Messages, Designed Forgetting and What Litigation Can Still Reach

Signal, Telegram's secret chats, Snapchat and the disappearing modes now built into every mainstream app represent something genuinely new in disclosure: communication engineered to leave no record. The engineering is often good: Signal in particular keeps its promises: and yet ephemeral-messaging matters are litigated and won every year, because the forgetting is rarely as total as its users assume: residue survives at the edges, counterparts capture what senders destroy, the choice of an ephemeral channel is itself disclosable conduct, and the duty to preserve reaches these apps exactly as it reaches email. This guide covers the ephemeral landscape app by app, what forensic examination can and honestly cannot recover, the preservation duties that attach the moment litigation is contemplated, the adverse-inference and conduct arguments that fill evidential gaps, and the corporate-governance questions that decide whether a business's Signal habit is privacy hygiene or spoliation in waiting.

🕒 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. Ephemeral-messaging questions arrive in its fraud, regulatory and employment casework with increasing frequency: device-level residue analysis, counterpart capture, channel-choice chronologies and the honest capability statements that keep expectations tethered. Its eDiscovery arm, **e-discovery.uk**, integrates what survives into disclosure.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

EPHEMERAL-APP ANALYSIS

RESIDUE & COUNTERPART CAPTURE

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: engineered forgetting meets the duty to remember
- 03 The landscape: Signal, Telegram, Snapchat and disappearing modes
- 04 What examination can still reach: the residue map
- 05 Preservation duties and the moment they bite
- 06 Channel choice as conduct: inference and chronology
- 07 Corporate governance: business use of ephemeral apps
- 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: EPHEMERAL APPS MOSTLY KEEP THEIR PROMISES: AND LITIGATION STILL REACHES THEM THROUGH RESIDUE, COUNTERPARTS, CONDUCT AND DUTY

Honesty first: **well-implemented ephemeral messaging genuinely destroys content.** Signal's disappearing messages, secret-chat modes and view-once media, executed as designed, leave no recoverable message body on the expiring device: the flash-resurrection mythology guide 61 §6 retired applies here with extra force, and any provider promising routine recovery of expired Signal messages is selling something other than forensics. What litigation reaches instead runs on four tracks. **Track one, residue:** the edges where implementation meets operating system: notification records and their caches, media saved or screenshot before expiry, database fragments where housekeeping lagged, app metadata (conversation existence, participant identifiers, settings and timer states, call logs) that survives after bodies expire, and desktop-client artefacts whose deletion hygiene sometimes trails the phone's: enumerable at FFS level, honestly variable, and worth the look every time. **Track two, counterparts:** ephemerality is a pact that any participant can break: the recipient who screenshots, exports, or simply has expiry off at their end; the participant whose device is extracted before timers fire: the membership walk of guide 63 §5, run faster. **Track three, conduct:** the move to an ephemeral channel is itself a recorded, datable act: invitation messages on ordinary channels ("let's take this to Signal"), install dates, timer-setting changes: and where it postdates the duty to preserve, it reads as it is: the channel-choice chronology of §6 is frequently the case's most damaging exhibit. **Track four, duty:** preservation obligations attach to ephemeral apps exactly as to email: a party who continues auto-deleting after litigation is contemplated is spoliating on a timer, regulators have said so in terms about off-channel messaging, and the remedies: adverse inference, costs, strike-out in extremity: fill gaps the technology created. The strategy this guide teaches: race what can be raced (§5's immediate steps), capture the counterparts, map the residue with honest expectations, and build the conduct-and-inference case in parallel: because in ephemeral matters, what the messages said is often proved by what their destruction cost.

- **Honest capability first:** expired, well-implemented ephemeral content is gone: strategies built on recovering it fail; strategies built on the four tracks succeed.
- **Metadata outlives bodies:** that conversations existed, between whom, under what timers, with what calls: routinely recoverable, and often enough for the inference work.
- **Counterparts break ephemerality:** one participant's screenshot, export or timer-off setting defeats the design: the membership walk is track one in practice.
- **"Let's take this to Signal" is an exhibit:** the migration message on the ordinary channel dates the intent: searched for in every ephemeral matter.
- **Continuing timers after the duty is spoliation:** the preservation letter names the apps and the timers: and non-compliance builds the inference case daily.

The problem in plain English: engineered forgetting meets the duty to remember

Disclosure law grew up assuming communication leaves records by default: the argument was over finding and producing them. Ephemeral messaging inverts the default: records exist briefly by design, and the parties' settings: not their diligence: decide what survives to be disclosed. The law's answer has not been to surrender but to relocate the obligation: if your communications self-destruct, your duty is to stop them self-destructing once litigation is in prospect, and to account for the channel choices you made. The technology changed what exists; it did not change what is owed.

For practitioners this creates a two-sided brief. Against an ephemeral-using opponent: move immediately (their timers are running), capture counterparts, demand settings and preservation, and build the conduct chronology that makes their forgetting expensive. For your own client: audit the ephemeral estate on day one, suspend the timers in writing, and address the historic channel choices honestly: because "we always used Signal for commercial sensitivity" is a defensible governance position when documented, and an inference magnet when improvised at disclosure.

§ 0 3 · THE LANDSCAPE

The landscape: Signal, Telegram, Snapchat and disappearing modes

APP / MODE	EVIDENTIAL CHARACTER
Signal	The reference implementation: E2EE, no provider content, disappearing timers per chat, view-once media, screen-security options: expired content genuinely gone; app metadata, settings, call records and edge residue remain the device-side yield; desktop client artefacts worth separate attention. Provider legal process yields effectively nothing beyond registration timestamps.
Telegram	Split personality: ordinary cloud chats are provider-stored and device-synced (substantial evidence, closer to ordinary apps); secret chats are device-bound, E2EE, with self-destruct timers (the ephemeral rules apply). The first question in any Telegram matter: which mode were the chats in?
Snapchat	Ephemerality as product: default expiry for snaps and chats, with saved-message exceptions, Memories storage, and screenshot notifications: provider holds some account data and limited content classes; device residue and counterpart captures carry most cases.
Disappearing modes in mainstream apps	WhatsApp timers (guide 63 §6), Instagram vanish mode, and equivalents: ephemeral behaviour inside otherwise recordful apps: the settings history and the surrounding ordinary-mode traffic frame the disappearing windows.
Self-hosted / niche ephemeral tools	Wickr-class enterprise tools, burner apps: governed by their deployment records (enterprise consoles sometimes retain more than users assume) and the same four tracks.

What examination can still reach: the residue map

- **App metadata:** conversation lists, participant identifiers, timestamps of activity, timer settings and their change history, call logs: the skeleton that survives after bodies expire: proving relationships, cadence and the disappearing configuration itself.
- **Notification residue:** message previews captured by notification systems and their caches before expiry: platform- and settings-dependent, checked at FFS level, and the source that rescued guide 63's Example 1.
- **Saved and captured content:** screenshots, saved media, message-save features (Snapchat), exports: the participants' own breaches of the pact, living in galleries, caches and cloud photo libraries.
- **Housekeeping lag:** fragments in databases, journals and caches where deletion hygiene trailed the promise: variable by app, version and platform: enumerated honestly, promised never.
- **Desktop and companion clients:** secondary installations whose artefact hygiene differs from the phone's: session records, cached content, and their own OS-level traces (guides 41-42): the census question, again.

Preservation duties and the moment they bite

- **The duty attaches to the app, not the medium's habits:** once litigation is reasonably contemplated, disappearing timers on relevant chats must be turned off, auto-delete settings suspended, and existing content preserved: the client instruction goes out day one, in writing, naming the apps.
- **The stopwatch is real:** content inside running timers is destroyed on schedule: the first 48 hours of an ephemeral matter are triage: identify relevant chats, disable timers, extract what stands: guide 63 §6's race, generalised.
- **Opponents are put on notice specifically:** the preservation letter names ephemeral apps, timers and settings, demands confirmation of suspension, and reserves the inference position: the letter's date starts the conduct clock.
- **Regulatory context sharpens everything:** off-channel messaging enforcement (financial services record-keeping, competition dawn-raid contexts) has made unpreserved ephemeral business communication a standalone compliance failure: advice to regulated clients leads with this.
- **Documentation of compliance:** the settings screenshots, suspension confirmations and extraction records that prove your own side stopped the timers: taken at the time, because proving a negative later is miserable.

Channel choice as conduct: inference and chronology

- **The migration message:** "call me on Signal", "taking this off email": sent, necessarily, on the recordful channel being abandoned: searched for across mail, Teams and WhatsApp in every ephemeral matter, and dated against the dispute's chronology.
- **Install and adoption dates:** app installation records, account registration, first-use artefacts: when did the ephemeral habit begin, and what was happening then?
- **Timer chronologies:** settings changes recovered from metadata and counterparts: a chat run recordful for two years and switched to 24-hour expiry the week of the whistleblower's email is an exhibit needing no message bodies.
- **Selective ephemerality:** ordinary channels for routine business, disappearing modes for the disputed topic: the pattern itself, mapped across the estate, argues content.
- **Inference doctrine does the rest:** unexplained destruction, non-compliance with preservation, refusal to account for channel choices: the adverse-inference and costs machinery, pleaded with the chronology attached: what the messages said, proved by what hiding them was worth.

Corporate governance: business use of ephemeral apps

- **Legitimate uses exist:** security-sensitive communications, protection of sources and personal data, executive travel hygiene: ephemerality is a defensible tool with a policy behind it.
- **The policy is the defence:** documented rules on which apps, which purposes, what must be preserved elsewhere (decisions minuted, instructions confirmed on record channels), and litigation-hold override procedures: the difference between privacy hygiene and inference bait.
- **Record-keeping obligations trump preference:** regulated sectors' communication-retention rules reach ephemeral channels used for business: the compliance mapping is done before regulators do it.
- **Litigation readiness:** holds that name ephemeral apps, custodian attestations of timer suspension, and audit of the estate at matter-open: the §5 duties, institutionalised.
- **Advice moment:** clients adopting Signal-class tools for business get this section as advice before disputes, not commentary after: the cheapest spoliation prevention available.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: ephemeral apps are examined as ecosystems, not screens. What survives expiry lives in: the device's residue layers (metadata, notifications, fragments, saves); every counterpart participant's device with its own settings and captures; desktop and companion clients with their laggier hygiene; cloud photo libraries and galleries holding screenshots and saved media; the recordful channels around the ephemeral one (the migration messages, the parallel ordinary-mode traffic, the decisions confirmed by email because someone insisted); provider records (thin for Signal, thicker for Telegram cloud chats and Snapchat account data, via legal process); enterprise consoles where business-grade ephemeral tools were deployed; and the conduct record itself: installs, settings, preservation compliance: which is evidence whatever happened to the words. When the bodies are truly gone, this map is what remains: and §6's point is that it is frequently enough.

EVIDENCE	EXPIRING DEVICE (RESIDUE)	COUNTERPART DEVICES	DESKTOP / COMPANION CLIENTS	RECORDFUL SURROUND (EMAIL, WHATSAPP, TEAMS)	PROVIDER / ENTERPRISE CONSOLE	DELETED / RECOVERABLE
Message bodies (expired)	Fragments/ notifications: sometimes	Captures, timer- off copies: the main hope	Hygiene-lag copies: sometimes	Quoted/ forwarded excerpts	Signal: no; Telegram cloud: yes; Snapchat: limited	Honest default: gone
Conversation existence / metadata	Y: routinely	Y	Y	Migration references	Registration/ account data	Skeleton persists
Timer / settings history	Y: metadata + change traces	Their view of changes	Synced state	n/a	Console policies where enterprise	The conduct layer
Saved / captured content	Galleries, caches	Their galleries + cloud photos	Downloads	Re-shares	Snapchat Memories class	Y where captured
Channel- choice chronology	Install/first- use artefacts	Their invitations received	Install records	Y: the migration messages	Registration dates	Fully reconstructable

Fallback strategy in one line: when the bodies expired, prove the skeleton, the captures, the migration and the timers: the four-track case that ephemeral matters are actually won on.

Worked examples

EXAMPLE 1 · THE MIGRATION MESSAGE THAT FRAMED THE SILENCE

A cartel-adjacent commercial claim faced an evidential void: the two managing directors' relevant discussions had happened on Signal with 24-hour timers, and the extractions honestly recovered nothing but the conversation's skeleton: eighteen months of near-daily contact, timers confirmed, bodies gone. The case was built around the void instead: the email in which one MD wrote "better on the app for this one" three days after the first competitor meeting; Teams messages showing price discussions stopping dead on the migration date while volumes continued; call metadata clustering before each parallel price move; and the timer setting itself, enabled the same week. The tribunal's decision treats the pattern as it reads: the silence, framed, spoke: and the costs of the framing exercise were a fraction of what message recovery would have cost to fail at.

EXAMPLE 2 · THE COUNTERPART WHO KEPT RECEIPTS

A fraud respondent ran his side of a joint venture on Snapchat: "nothing in writing" as lifestyle: and told his solicitors the record was unrecoverable. It was, from him. The claimant: patronised for years as the junior partner: had screenshot everything, contemporaneously, into a cloud photo library with intact EXIF chronology; her device extraction corroborated capture dates against the app's metadata; and two saved-message threads survived in the app itself where she had used the save feature he never noticed. The authentication workup (capture-time metadata, device provenance, app-metadata convergence) survived a fabrication challenge comfortably: and the respondent's own expert conceded the ecosystem point this guide teaches: ephemerality is a pact, and she had never joined it.

EXAMPLE 3 · THE TIMERS THAT KEPT RUNNING

An employment respondent received a preservation letter naming Signal and demanding timer suspension for three named custodians. Nothing was done: the letter sat in an inbox, the 7-day timers ran, and four months of the disputed period expired on schedule before disclosure. The forensic evidence proved exactly that: timer settings unchanged post-letter, message counts decaying week by week (the metadata skeleton dating the destruction), and no preserved extraction anywhere. The tribunal needed no message bodies: continuing automated destruction after specific notice was treated as deliberate, the inference drawn was the claimant's pleaded version of the conversations, and the remedies judgment added uplift for the conduct. The letter had cost an hour to write; ignoring it decided the case.

Common mistakes and technical limitations

Common mistakes

- **Recovery fantasies:** budgets spent chasing expired Signal bodies that §1's honesty paragraph priced correctly at zero.
- **The race unrun:** live timers left running during weeks of scoping: content destroyed that same-week extraction would have held.
- **Counterparts unwalked:** Example 2's claimant never asked: the pact assumed unbroken because the primary user said so.
- **The migration search skipped:** recordful channels never searched for the invitation that dates everything.
- **Generic preservation letters:** ephemeral apps and timers unnamed: Example 3's leverage forfeited by wording.
- **Client timers unsuspended:** your own side's auto-delete running post-duty: spoliation manufactured in-house.
- **Telegram undifferentiated:** cloud chats and secret chats treated alike: substantial evidence missed or impossible recovery promised.
- **Governance improvised at disclosure:** the Signal habit explained for the first time in a witness statement: §7's policy, needed years earlier.

Technical limitations

- **Good implementations win:** expired content from well-built ephemeral apps is unrecoverable: the capability statement is dated, app-specific and honest.
- **Residue is variable:** notification and fragment yield differs by platform, version and settings: enumerated per device, promised never.
- **Provider routes are thin by design:** Signal's legal-process yield is registration-level; expectations are set accordingly, and Telegram/Snapchat's partial exceptions checked per class.
- **Metadata proves shape, not words:** the skeleton supports inference and chronology: content claims need captures, counterparts or the tribunal's drawn conclusions.
- **Screenshots inherit guide 63 §7:** counterpart captures are authenticated: capture-time metadata, device provenance, app-metadata convergence: before they carry weight.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The ephemeral census: which apps, which chats, which timers: and are the timers suspended in writing today?
- Who were the counterparts, and which might hold captures, saves or timer-off copies?
- What is the honest history of the channel choice: and what policy, if any, governed it?

Ask your opponent

- Please confirm, within [3] days: all disappearing-message and auto-delete settings on [apps] for [custodians] have been disabled; existing content preserved by forensic extraction; and no chat, account or app deleted: identifying every relevant conversation and its timer history.
- Please disclose when each ephemeral app was installed and adopted for the relevant communications, and produce all communications on other channels referring to their use.
- If any relevant content has expired or been deleted since [duty date], please give particulars: what, when, under what settings, and why the settings were not suspended.

Ask your eDiscovery / forensic provider

- The dated, app-specific capability position: what can residue analysis honestly reach here?
- The counterpart map: who might hold captures, and in what order do we approach them?
- The conduct chronology: migrations, installs, timer changes: assembled from which sources?

SUGGESTED WORDING · EPHEMERAL LIMB FOR THE PRESERVATION LETTER

"Your client's preservation obligations extend to ephemeral and disappearing-message applications, including Signal, Telegram (including secret chats), Snapchat and disappearing modes within other applications. Your client must immediately: (1) disable all disappearing-message timers, self-destruct and auto-delete settings on all conversations relevant to the issues, and confirm the same with dated screenshots; (2) preserve existing content by forensically sound extraction before any timer expiry; (3) make no deletion of any chat, account or application; and (4) identify all relevant conversations on such applications, their participants, and the retention settings applied over the relevant period. Content destroyed by timers left running after receipt of this letter will be relied upon as deliberate spoliation, and all consequential inferences, costs and sanctions will be sought."

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

The ephemeral checklist

- ☐ Ephemeral census run day one: apps, chats, timers, counterparts
- ☐ Client timers suspended in writing with dated screenshots; extraction before expiry
- ☐ Preservation letter names the apps and timers specifically; confirmation demanded
- ☐ The race run: live-timer content extracted same week
- ☐ Migration-message searches run across the recordful estate
- ☐ Counterpart walk executed: captures, saves, timer-off copies pursued
- ☐ Telegram mode question answered before capability statements
- ☐ Residue analysis at FFS level with honest, per-device yield statements
- ☐ Conduct chronology assembled: installs, adoptions, timer changes, compliance
- ☐ Governance position documented: policy produced or its absence addressed

Red flags

- Timers still running after specific notice: Example 3's decided case.
- Ephemeral adoption or timer changes dated to the dispute's arrival.
- "Better on the app" messages in the recordful estate.
- Selective ephemerality tracking the disputed topic.
- Business-critical decisions with no recordful confirmation anywhere.
- Recovery promises for expired Signal content.
- A counterpart list nobody has approached.

When to involve a digital forensic expert

Immediately, where live timers make extraction same-week work and the census defines the race; at capability, where the app-specific honest position keeps strategy and budget sane; at the residue and counterpart analyses, where FFS-level enumeration and capture authentication are laboratory craft (Example 2's workup); and at the conduct case, where migrations, installs, timer chronologies and compliance failures are assembled into the framed-silence exhibits of Examples 1 and 3. Reported under CPR Part 35 with capability positions dated and yields stated per device: and through **e-discovery.uk**, what survives joins the estate's other channels in one reviewable record.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can deleted or expired Signal messages be recovered?

Expired under a running timer, from a healthy modern installation: no: and the honest practice says so at the first conversation. What examination recovers is the skeleton (metadata, settings, calls), edge residue where it exists, and everything counterparts captured: which, with the conduct tracks, wins these cases far more often than the impossible recovery would have. Distrust any contrary promise not tied to a specific device, version and dated capability basis.

Is it unlawful for a business to use disappearing messages?

Not inherently: outside regulated record-keeping regimes, ephemerality for legitimate purposes under a documented policy is defensible privacy practice. It becomes a problem in three ways: regulated communications routed through it (a compliance breach in itself), timers left running after litigation is contemplated (spoliation), and adoption patterns that track disputes (inference). §7's governance is the line between tool and misconduct.

The opponent says the messages expired innocently under settings predating the dispute. Does that end it?

It changes the questions: pre-existing timers running to expiry before the duty attached destroy content lawfully: but the duty's arrival is the watershed: what expired after contemplation, why the timers were not suspended, what the preservation letter's date did (Example 3), and whether extraction was taken when it could have been. The settings history and compliance record answer all four: request them, in terms.

A witness offers screenshots of expired chats. How much weight can they carry?

Properly authenticated: substantial: Example 2's case rests on them. The workup is guide 63 §7 plus capture-specific checks: capture-time metadata and library chronology, device provenance, convergence with the app's surviving skeleton (conversation existence, participant identifiers, activity timestamps matching the captured content's claims). Unauthenticated, they are the weakest class in messaging evidence: the difference is the examination, not the format.

Do adverse inferences really substitute for the messages themselves?

Where destruction follows the duty and goes unexplained: yes, and increasingly robustly: tribunals infer the destroyed material's tenor from the destroyer's conduct, with costs and sanctions in support: Example 3's mechanics. The inference case is built, not assumed: specific notice, documented non-compliance, the destruction dated by metadata, innocent explanations closed off in correspondence: which is why the §11 wording and its confirmations exist.

What should a client adopting Signal for business do this week?

Write the policy (§7): which purposes, which chats, what gets confirmed on recordful channels, and the litigation-hold override that suspends timers on demand; train the users; and diarise the hold procedure against matter-open. An afternoon's governance converts the ephemeral estate from inference bait into defensible practice: and it is the single piece of advice in this guide best given before it is needed.

§ 1 4 · REFERENCE

Glossary

Channel-choice chronology

The dated record of migrations, installs and timer changes; §6's conduct case.

Framed silence

An evidential void surrounded by the pattern that explains it; Example 1's method.

Metadata skeleton

Conversation existence, participants, cadence and settings surviving expiry.

Migration message

The recordful-channel invitation to go ephemeral; the dating exhibit.

Notification residue

Preview content captured by the OS before expiry.

Pact, the

Ephemerality's dependence on every participant's compliance; broken by one.

Secret chat

Telegram's device-bound E2EE mode; the app's ephemeral half.

Timer suspension

The preservation act the duty requires; documented with dated screenshots.

View-once

Single-view media; minimal residue by design.

Void strategy

Building the case from tracks two to four when track one honestly yields nothing.

Sources and authoritative references

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

- cflab.uk, digital forensics services (ephemeral-app analysis, residue enumeration, capture authentication, conduct chronologies, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (timer suspension protocols; the four-track record into review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- College of Policing, extraction guidance: 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 ephemeral messaging evidence as at August 2026. Application behaviour, deletion mechanics and provider disclosure positions change frequently and vary by platform and version; verify the current position for the specific applications 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

Ephemeral matters at the laboratory begin with the stopwatch: the census, timer suspensions and pre-expiry extractions of \$5 in the first days, with the capability conversation had honestly at the start. The four tracks then run together: residue enumeration at FFS level with per-device yield statements; the counterpart walk with capture-authentication workups (Example 2's standard); the conduct chronology: migrations, installs, timers, compliance: assembled into the framed-silence exhibits of Examples 1 and 3; and governance advice for clients whose ephemeral estates need a policy before they need a defence. Reporting is CPR Part 35 with dated capability positions; through **e-discovery.uk**, what survives is threaded beside the recordful channels per guide 70. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a relevant chat is on a timer somewhere right now, everything else in this brochure can wait.



I N S T R U C T T H E L A B

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