



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

Slack eDiscovery

Channels, DMs, Threads, Edits, Retention Tiers and Exports: Disclosing the Workspace Where Work Actually Happens

In thousands of UK businesses, Slack is not a chat tool beside the work: it is the work: decisions made in channels, deals discussed in DMs, culture recorded in reactions, and the candour that email lost twenty years ago alive and disclosable. Its evidential character is distinctive: plan tier decides what even exists to collect, retention settings run deletion on schedules nobody remembers configuring, edits and deletions behave differently from every platform covered so far, and the export routes range from complete corporate archives to fragments a departed employee kept. This guide gives UK lawyers the working model: Slack's data structures and where each conversation type lives, how the plan-and-retention lattice decides survival, what edit and deletion history can be recovered and under what tier, the export and collection routes with their fidelity trade-offs, and the review strategies that stop channel evidence drowning the case that needed it.

© 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. Slack collections feature across its commercial, employment and investigations casework: plan-and-retention audits, export-route selection, edit and deletion history recovery, and the processing that turns JSON archives into reviewable conversations. Its eDiscovery arm, **e-discovery.uk**, runs channel evidence through the same disciplined pipeline as email and documents.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

SLACK & WORKSPACE COLLECTIONS

RETENTION & EXPORT ANALYSIS

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: the office that talks in channels
03	The data model: channels, DMs, threads, files, apps
04	The lattice: plan tiers, retention settings and what survives
05	Edits, deletions and message history
06	Collection routes: exports, APIs and their fidelity
07	Processing and review: making channels reviewable
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: IN SLACK, THE SUBSCRIPTION TIER AND A SETTINGS PAGE DECIDE WHAT EVIDENCE EXISTS: AUDIT THE LATTICE BEFORE PROMISING ANYTHING

Slack's evidential landscape is governed by a **plan-and-retention lattice** that must be audited before any preservation promise, collection plan or deletion argument: because the same workspace's history can be complete for a decade or gone in ninety days depending on choices nobody in the legal team made. **Plan tier decides capability:** free workspaces historically truncated visible history (with data handling evolving on the provider's schedule: verified per case, never assumed); paid tiers keep full history; and the export routes scale with tier: standard exports covering public channels, with **DMs and private channels reachable only via higher-tier corporate export mechanisms or compliance APIs** subject to eligibility and, in some configurations, employee-notification features: a gating that shapes what "we have collected the Slack" actually means and that opposing productions should be interrogated against. **Retention settings decide survival:** workspace-level and per-conversation retention rules delete messages and files on rolling schedules, can differ between channels and DMs, can be changed by admins (changes that are themselves logged), and: the recurring trap: keep running through litigation unless someone suspends them: guide 56's retention race, replayed with different switches. **Message dynamics decide fidelity:** Slack messages are edited and deleted natively; whether original versions and deletion records survive depends on tier, settings and collection route (compliance-grade exports can include edit and deletion history that ordinary views never show): so the completeness of a produced channel is a technical claim, checkable, and worth checking whenever chronology or candour is disputed. Around the platform sit the usual ecosystem members: local caches on desktop and mobile clients, connected apps and integrations holding mirrored content, huddle and call artefacts, user-side exports and screenshots, and the audit logs (tier-dependent) recording admin acts including the retention changes that matter most. The method, familiar by now from guides 51, 56 and 58: freeze first (retention suspended, legal-hold features engaged where available, the lattice documented), audit the lattice honestly, choose the collection route by fidelity need, and interrogate every production: yours and theirs: against what the tier and settings made possible.

- **Audit before promising:** plan tier, retention rules per conversation type, export eligibility: the lattice audit is day-one work, in writing.
- **DMs are the gated evidence:** the candid layer needs the corporate-export or API route, with its eligibility and notification wrinkles navigated deliberately.
- **Retention keeps running:** suspension is an act, not a default: the standing trap of this series, on Slack's switches.
- **Edit and deletion history is route-dependent:** compliance-grade collection sees what ordinary exports do not: fidelity is chosen, then defended.
- **Productions are interrogated against the lattice:** "complete Slack disclosure" from a standard export of a DM-heavy dispute is a contradiction: §11 asks the questions.

The problem in plain English: the office that talks in channels

Slack restored what email formality suppressed: speed, candour, jokes, the real-time texture of how decisions actually form: and recorded all of it. For disputes this is gold and hazard together: the gold is contemporaneous candour ("just ship it, legal can catch up" lives in channels, not memos); the hazard is that the recording's existence depends on administrative choices: tier purchased, retention configured, exports enabled: made for budget and storage reasons long before anyone contemplated litigation. Email's evidential defaults were set by decades of practice; Slack's are set by a pricing page.

The practitioner's stance follows: treat every Slack matter as beginning with an audit rather than a request: what tier, what retention, what export rights, what has already rolled off: because the answers determine whether the exercise is collection (the evidence exists: go get it properly) or archaeology-and-inference (it rolled off: date the roll-off, test its innocence against the dispute's chronology, and look to the ecosystem's other copies). Both are workable cases; confusing them wastes months.

§ 0 3 · THE DATA MODEL

The data model: channels, DMs, threads, files, apps

COMPONENT	EVIDENTIAL CHARACTER
Public channels	The open record: joinable, searchable, covered by standard exports: decisions, announcements, working chatter: with membership and join/leave events part of the story.
Private channels	The selective record: invitation-only, invisible to non-members, gated behind higher-tier export routes: where sensitive projects and, often, the disputed conduct live: their existence enumerable by admins even where content needs the corporate route.
Direct messages & group DMs	The candid layer: one-to-one and small-group traffic, maximally informal, export-gated like private channels: the Slack equivalent of guide 63's territory, and usually the collection's point.
Threads	Replies nested under parents: chronology's complication: thread context must travel with messages or review reads conversations shredded: a processing requirement, not a nicety (§7).
Files & canvases	Uploads, snippets, canvases and their comment layers: stored platform-side, linked from messages, subject to the same retention lattice: collected with their linkage or orphaned into noise.
Reactions, pins, bookmarks	The paralinguistic layer: acknowledgment, approval, sentiment (a thumbs-up on the instruction is evidence of receipt): captured by good exports, flattened by bad ones.
Huddles & calls	Ad-hoc audio/video: minimal content retention by default: event records and any user captures: the guide 45 lesson in Slack form: the meeting happened; the record is thin.
Apps & integrations	Bots, workflow apps, connected services posting into channels and mirroring content outward: each integration a potential second home for the same evidence (§8), and app-posted messages part of the record.
Slack Connect	Cross-organisation channels: shared with external firms: two workspaces' retention lattices governing one conversation, and a counterpart organisation holding its own copy: the multi-party wrinkle flagged for preservation letters.

The lattice: plan tiers, retention settings and what survives

- **Tier gates capability:** history depth, export scope, compliance features (legal holds, audit logs, DM export eligibility) scale with subscription: the first audit question, answered from admin screens and billing records, not memory.
- **Retention runs per scope:** workspace defaults with per-channel and per-DM overrides: message retention and file retention separately configurable: mapped completely, because the disputed DM may sit under a rule the channel audit never saw.
- **Changes are logged:** retention edits, export events and admin acts land in audit logs on eligible tiers: the conduct layer where settings moved mid-dispute: guide 57's method on Slack's logs.
- **Legal holds where available:** higher-tier hold features preserve custodian messages against retention and user deletion: engaged day one where the tier permits; where it does not, retention suspension is the cruder substitute, documented in writing.
- **Roll-off is datable:** what a retention rule destroyed, and when, reconstructs from the rule's history and the gaps' shape: the innocence of a roll-off is tested against when the rule was set: ninety-day retention configured years pre-dispute reads one way; configured the week the claim landed, another.

Edits, deletions and message history

- **Edits are native and common:** typo culture makes edits routine: and compliance-grade routes can capture original versions with edit timestamps, where ordinary views show only the "(edited)" flag: the disputed instruction's history is reachable, route permitting.
- **Deletions are user acts with route-dependent traces:** deleted messages vanish from view; whether deletion records and prior content survive depends on tier, settings and hold status: the audit answers what the recovery question is worth.
- **Admin and bulk deletions:** workspace-level removals and user-deletion cascades: logged acts on eligible tiers, with the logs outliving the content: the pattern layer again.
- **Client caches as residue:** desktop and mobile Slack clients cache conversation data locally: FFS and disk examinations (guides 61, 41-42) sometimes hold messages the platform no longer shows: the endpoint layer that rescued more than one rolled-off fragment.
- **User exports and keepers:** employees export threads, screenshot exchanges, forward to email: the unofficial archive, surfaced by custodian interviews and endpoint review: never the primary route, repeatedly the surviving one.

Collection routes: exports, APIs and their fidelity

- **Standard workspace export:** public-channel JSON with files: the baseline: no DMs, no private channels: sufficient only where the case genuinely lives in public.
- **Corporate export (eligible tiers):** the full-workspace route including DMs and private channels: eligibility criteria and process requirements navigated deliberately, timing and scope documented, and the export's own generation logged.
- **Discovery/compliance APIs:** the eDiscovery-tooling route: continuous or targeted collection with edit/deletion history where configured: the fidelity ceiling, plan permitting, and the route serious disputes budget for.
- **Targeted alternatives:** channel-level exports, custodian-side captures, endpoint caches: the proportionate fragments route for narrow issues, with limitations stated.
- **Route selection is a defensibility decision:** chosen against the issues (are edits disputed? are DMs central?), documented against the lattice, and disclosed with the production: because "which route, and why" is now a standard opponent question: §11 makes it yours too.

Processing and review: making channels reviewable

- **JSON is not a review format:** raw exports are developer artefacts: processing reconstructs conversations: threading, user-ID resolution to names, timestamp conversion, file re-linkage, reaction and edit-history rendering: guide 56 §13's disciplines, Slack dialect.
- **Unitisation decides everything downstream:** messages reviewed atomised down reviewers in fragments; sensible windowing (conversation-day units, thread units) keeps context and sanity: agreed in the protocol where possible (guide 94's territory).
- **Search adapts to chat:** keyword strategies tuned for brevity, slang, emoji semantics and the absence of subject lines: guide 84's craft with chat-specific tuning, and sampling to test it (guide 85).
- **Privilege review meets informality:** lawyers chat in channels too: privileged threads interleaved with business traffic, flagged by participant- and channel-aware protocols rather than domain rules alone (guide 91 previewed).
- **Presentation to the tribunal:** threads rendered readably, edits and deletions annotated, the paralinguistic layer preserved where it carries meaning: the thumbs-up that proved receipt survives to the bundle.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the workspace is the hub, not the whole. Slack evidence also lives in: desktop and mobile client caches on every custodian device; connected apps and integrations mirroring channel content into ticketing, CRM and storage platforms; email, in notification digests and user-forwarded threads; user-side exports and screenshots; Slack Connect counterpart organisations holding their own copies of shared channels; audit and access logs on eligible tiers; huddle/call event records; and the surrounding estate: the email, Teams and document systems whose traffic brackets and corroborates the channel record (guide 70's assembly). When the workspace's history has rolled off, this periphery: plus the roll-off's own datable innocence or guilt: is the case.

EVIDENCE	WORKSPACE (ROUTE-DEPENDENT)	CLIENT CACHES	INTEGRATIONS / MIRRORS	EMAIL (DIGESTS, FORWARDS)	CONNECT COUNTERPART	DELETED / RECOVERABLE
Public channel messages	Y: standard export	Partial, recent	Where connected	Digest fragments	If shared	Per retention + route
DMs / private channels	Corporate/API routes only	Partial: the rescue layer	Rarely	User forwards	n/a mostly	Route + hold dependent
Edit / deletion history	Compliance routes where configured	Pre-edit fragments sometimes	Mirror timing may capture originals	Notification text sometimes	Their view	The route decides
Files / canvases	Y with linkage	Downloads	Y where synced	Attachments forwarded	Shared copies	File retention separate
Admin / retention acts	Audit logs (tier)	n/a	n/a	Change notifications	Their admins' logs	Logs outlive content

Fallback strategy in one line: when the workspace's record fails, walk the caches, the mirrors, the forwards and the counterpart workspace: and date the failure itself, because a roll-off's timing is evidence either way.

Worked examples

EXAMPLE 1 · THE RETENTION RULE WITH A BIRTHDAY

A competition claim sought two years of a distributor's Slack; the response produced ninety days and cited "standard retention". The lattice audit told a longer story: the audit log showed workspace retention at "keep everything" from workspace creation until a change to ninety days: dated eleven days after the claimant's letter before action: made by an admin account, with the log capturing the actor and hour. The roll-off that followed was retention working as configured; the configuration was the conduct. The specific-disclosure application exhibited the log entry beside the letter's delivery receipt, the inference sought was granted in terms, and the endpoint-cache harvest across four custodian laptops recovered enough of the destroyed period to make the inference concrete.

EXAMPLE 2 · THE DM LAYER THE EXPORT NEVER REACHED

An employment respondent disclosed "the complete Slack record": a standard export, public channels only: and certified completeness. The claimant's team, running §11's route questions, established the tier supported corporate export and that the dispute's protagonists barely used public channels: their traffic was DMs. The corrected collection, ordered after a contested application, produced the DM layer: including the group DM in which three managers coordinated the sidelining the claim alleged, message by message across the pleaded months. The tribunal's remarks distinguish sharply between a production limited by capability and one limited by route selection: the tier had made the fuller export possible all along, and the certificate had said "complete".

EXAMPLE 3 · THE EDIT HISTORY THAT REVERSED THE READING

A joint-venture dispute turned on a channel message: "agreed: proceed on the revised terms": which the defendant said referred to the claimant's version of the term sheet. The compliance-route collection captured what the ordinary export could not: the message's edit history. As first posted, it read "agreed: proceed on YOUR revised terms": edited four minutes later, the pronoun removed, the "(edited)" flag sitting in plain sight all along. Four minutes and one word: the original text, timestamped before the edit, resolved which terms had been agreed, and the editing itself: contemporaneous with a phone call the metadata placed: became part of the narrative. The fidelity choice at collection had decided whether the case's best fact existed.

Common mistakes and technical limitations

Common mistakes

- **The lattice unaudited:** promises and applications made before tier, retention and export rights are known: strategy built on guesswork.
- **Retention left running:** the standing trap: suspension nobody performed, roll-off continuing through the hold.
- **Standard exports certified complete:** Example 2's certificate: DM-centric disputes answered with public channels.
- **Fidelity chosen by default:** edit and deletion history forgone by route selection in cases where §5's dynamics were the issue.
- **Threads shredded in processing:** messages reviewed contextless; the conversation's meaning left in the JSON.
- **Endpoint caches ignored:** the client-side layer unexamined while roll-off is mourned platform-side.
- **Connect counterparts forgotten:** shared channels' second workspace unpreserved and unasked.
- **Opponent productions unquestioned:** route, tier and scope taken on trust: §11 exists because they should not be.

Technical limitations

- **Rolled-off is rolled off:** retention-destroyed content is not platform-recoverable: the periphery and the inference case are the honest remainder.
- **Route ceilings are real:** a tier without compliance features cannot produce compliance-grade history retroactively: fidelity is bounded by what was configured when the messages lived.
- **Caches are partial and volatile:** the endpoint layer is a rescue, not an archive: recent, incomplete, and examined early or lost.
- **Huddles keep their thinness:** ad-hoc calls leave event records, not transcripts: expectations set per guide 45's meeting rule.
- **Provider process yields little content:** the practical routes are workspace-side rights and orders against parties: platform legal process is not the plan.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The lattice, in writing today: tier, retention rules per scope with their change history, export and hold eligibility?
- Where do the issues actually live: channels, private channels, DMs, Connect: and which custodians' caches back them up?
- Is retention suspended and the hold engaged: by whom, when, evidenced how?

Ask your opponent

- Please state your Slack plan tier, workspace retention settings (with all changes in the relevant period, from the audit log), and whether legal hold or retention suspension has been applied: with dates and actors.
- Please identify the collection route used (standard export, corporate export, discovery API), its scope (public channels, private channels, DMs), and whether edit and deletion history was captured.
- Please confirm preservation of client caches on custodian devices, Connect counterpart notice, and connected integrations mirroring workspace content.

Ask your eDiscovery / forensic provider

- Which route reaches the evidence this case needs at the fidelity it needs: and what does the lattice permit?
- How will threads, edits and the paralinguistic layer be preserved into review?
- What do the endpoint caches add: and how fast must they be imaged?

SUGGESTED WORDING · SLACK LIMB FOR THE PRESERVATION LETTER

"Your client must immediately preserve all Slack data relating to the issues, including: (a) all messages in public channels, private channels, direct messages and group direct messages, together with threads, files, canvases, reactions and edit and deletion history so far as capturable on your client's plan; (b) all retention settings, which must be suspended or set to preserve indefinitely for relevant conversations, with no change other than such suspension; (c) legal hold features, which must be engaged for the custodians listed; (d) audit logs and analytics; and (e) local Slack client data on custodian devices, which must not be cleared, reinstalled or wiped. Please confirm within [3] days, stating your plan tier, the retention settings applied over the relevant period with any changes and their dates, and the collection route by which disclosure will be given."

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

The Slack checklist

- ☐ Lattice audit day one: tier, retention per scope, change history, export and hold rights
- ☐ Retention suspended and holds engaged, documented with dates and actors
- ☐ Issue geography mapped: channels, private channels, DMs, Connect
- ☐ Collection route selected against fidelity needs and recorded with reasons
- ☐ Edit/deletion history captured where the dynamics are in issue
- ☐ Endpoint caches imaged early on priority custodians
- ☐ Integrations and mirrors enumerated; Connect counterparts noticed
- ☐ Processing preserves threads, identities, timestamps and reactions
- ☐ Opponent lattice and route interrogated per §11
- ☐ Roll-offs dated against rule history and the dispute's chronology

Red flags

- Retention shortened after the dispute arose: Example 1's birthday.
- "Complete" productions from standard exports in DM-centric matters.
- Edited flags on the key messages with no history captured.
- Audit logs unavailable on a tier that should have them, unexplained.
- Custodian devices reimaged or Slack clients reinstalled mid-hold.
- Integrations that mirrored content quietly disconnected.
- A Connect channel whose counterpart was never told to preserve.

When to involve a digital forensic expert

At the lattice audit, where tier and settings interpretation decides strategy; at route selection, where fidelity trade-offs (Example 3's decisive choice) need technical grounding; at the endpoint layer, where cache imaging runs on the usual clocks; at processing, where thread reconstruction and history rendering are craft; and wherever roll-off, deletion or settings conduct needs dating and reporting: the Example 1 exercise, run under CPR Part 35 with routes and bounds stated. Through **e-discovery.uk**, channel evidence joins email, documents and mobile in one reviewable, cross-referenced record per guide 70's assembly.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can we get employees' Slack DMs, or are they private?

On eligible plans, workspace owners can lawfully reach DMs via corporate export or discovery APIs: subject to the platform's eligibility process and, critically, UK employment and data protection law: necessity, proportionality, transparency obligations and any workspace privacy commitments weighed before the switch is thrown (the guide 51 balance, Slack edition). "Private" in the interface means private from colleagues, not from properly governed disclosure: but the governance is the point, and it is documented before, not after.

Our client's Slack only goes back 90 days. Is the case dead?

Not before three questions: when was that retention set (a rule predating the dispute is misfortune; Example 1's timing is conduct); what does the periphery hold (endpoint caches, integration mirrors, email forwards, Connect counterparts: §8's map); and what does the roll-off's shape support by inference? Cases survive roll-offs regularly: on the periphery's fragments and the destruction's own story: what dies is the assumption that the workspace was the only copy.

Are Slack messages disclosable documents like email?

Entirely: they are documents under CPR 31 and PD 57AD, within the duty to preserve from the moment litigation is contemplated, and within adverse-document obligations however informal the tone. The practical differences are logistical: the lattice, the routes, the processing: not jurisprudential. Parties who treated channels as off-the-record have learned otherwise at cost: the candour that makes Slack valuable evidence was typed by people making that exact assumption.

The key message says "(edited)". What can we find out?

Route-dependent, per §5: compliance-grade collections capture original versions with edit timestamps; ordinary exports show final text and flag only. If the collection has not happened, the fidelity choice is live: make it (Example 3's lesson); if it has, interrogate what the route captured; and either way the edit's timing: recovered from history or bracketed by caches and mirrors: joins the chronology. An edit contemporaneous with the dispute's crystallisation is a fact worth having whatever the original said.

How should Slack evidence be presented to a tribunal?

As conversations, not exhibits-by-message: threads rendered in order with identities resolved, dates and times explicit, edits and deletions annotated, reactions preserved where they carry meaning, and enough surrounding traffic that context survives challenge: with the collection route and its fidelity stated in the evidence's pedigree. The completeness attack on selective chat quotation is now routine; the answer is built at processing, per §7, not improvised at trial.

What about Teams, Discord, and the other chat platforms?

The method transfers; the lattices differ. Teams is guide 56's territory (Purview-governed, Exchange-linked storage); consumer platforms (Discord, Telegram groups) sit closer to guides 63-64's device-and-counterpart world; and each enterprise tool has its own tier-and-retention lattice to audit first. The transferable discipline is exactly this guide's: audit what can exist, freeze what does, choose the route by fidelity, and interrogate productions against capability: the platform names change; the questions do not.

§ 1 4 · REFERENCE

Glossary

Audit log

Tier-dependent record of admin acts; where retention changes surface.

Corporate export

The full-workspace route reaching DMs and private channels, eligibility permitting.

Discovery API

The compliance-tooling route; the fidelity ceiling for edits and deletions.

Huddle

Ad-hoc audio/video; thin retention, event records mostly.

Lattice

The plan-tier and retention-settings grid deciding what exists.

Legal hold (Slack)

Tier-dependent custodian preservation against retention and deletion.

Roll-off

Retention-scheduled destruction; datable, and judged by its timing.

Slack Connect

Cross-organisation channels; two lattices, two copies.

Standard export

The public-channels-only baseline route.

Unitisation

The windowing of messages into reviewable conversation units.

Sources and authoritative references

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

- cflab.uk, digital forensics services (workspace collections, endpoint cache imaging, settings-conduct analysis, 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 (lattice audits; route selection; chat 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
- Slack, security and compliance documentation: slack.com/trust/compliance · export documentation: slack.com/help, slack.com/help, [exports](https://slack.com/help)
- PD 57AD and CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk) · justice.gov.uk, [Part 35](https://justice.gov.uk)
- ICO, employment practices and UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, [27037](https://iso.org)

DISCLAIMER

This publication provides general information about Slack eDiscovery as at August 2026. Plan features, export mechanisms, retention behaviour and compliance capabilities change on the provider's schedule; verify the current position for the workspace 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

Slack matters at the laboratory begin with the lattice audit: tier, retention per scope, change history, export and hold rights: documented before anything is promised, with retention suspension and holds engaged the same day. Route selection follows the issues (Example 3's fidelity lesson applied at the start, not regretted at the end); endpoint caches are imaged on the priority custodians while they still hold anything; settings conduct is dated from the audit logs (Example 1's exercise); and processing delivers conversations: threaded, identified, annotated: rather than JSON. Opponent productions are interrogated against their lattice per §11, and completeness certificates read with Example 2 in mind. Reporting is CPR Part 35; through **e-discovery.uk**, channel evidence takes its place beside the estate's other sources in one assembled record. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a workspace retention rule is running on your matter's conversations today, its suspension is this afternoon's work.



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