



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

Collecting Evidence from Microsoft Teams Private and Shared Channels

The Conversations That Live Outside the Team's Own Mailbox

Guide 53 covered Teams as a whole; this guide covers the corner where collections go wrong. Standard channels store their messages in the team's group mailbox and their files in the team's SharePoint site: a known, collectable place. Private channels and shared channels do not: their messages are stored in the mailboxes of the individual members (private) or in a dedicated storage arrangement (shared), and their files live in separate SharePoint sites created per channel. A collection scoped to "the team" silently omits them. In restructuring disputes, harassment claims, cartel investigations and leaver cases, the private channel is frequently where the candid conversation happened. This guide explains for UK lawyers where these channels actually store their data, how membership and lifecycle affect what survives, how to scope holds and collections so nothing is missed, and how to prove the collection was complete.

⌚ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its eDiscovery arm, **e-discovery.uk**, collects from Microsoft 365 estates daily and has audited enough opposing Teams productions to know that private and shared channels are the most commonly omitted source in the platform: the census, hold and collection disciplines in this guide are the ones that close that gap.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

MICROSOFT 365 COLLECTIONS

TEAMS CHANNEL CENSUS

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the team is not the channel
- 03 Where the data actually lives: standard, private and shared channels compared
- 04 Membership, lifecycle and what survives departures and deletions
- 05 Holds and collection: scoping so nothing is missed
- 06 Reconstruction, review and the shape of channel evidence
- 07 Proving completeness and challenging the opponent's collection
- 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: PRIVATE AND SHARED CHANNELS STORE MESSAGES AND FILES SOMEWHERE OTHER THAN THE TEAM'S OWN MAILBOX AND SITE: A COLLECTION SCOPED TO THE TEAM MISSES THEM, AND THE CENSUS THAT FINDS THEM IS THE FIRST TASK

Teams channels come in three storage models. **Standard channels** keep message copies in the parent team's group mailbox and files in the team's SharePoint site. **Private channels** keep message copies in each *member's* individual mailbox (a hidden folder) and files in a *separate* SharePoint site created for that channel: there is no group mailbox for the channel, and the parent team's site does not contain its files. **Shared channels** (which can include members from other teams and even other organisations) keep messages in a dedicated storage location associated with the channel and files, again, in a separate SharePoint site. The consequences for disclosure are direct: a hold or collection targeting "the team" (its group mailbox and site) captures standard channels only; private-channel messages must be reached through the members' mailboxes, and both private and shared channel files through their own sites: which must first be enumerated, because they do not appear under the team's site. Membership changes and channel deletion alter what survives, on retention clocks the platform sets. The disciplines are: a channel census across the tenant before scoping; holds placed on member mailboxes and channel sites, not just the team; collection through the compliance tooling with channel scope explicit; reconstruction that stitches conversations from the right stores; and a completeness record that lists every channel, its storage locations and its custodians: the record that answers the opponent's completeness challenge, or grounds your own.

- **Three storage models:** standard, private and shared channels live in different places: the team-level collection reaches only the first.
- **Private channel messages are in member mailboxes:** every member's; the hold follows the people, not the team.
- **Files are in per-channel sites:** enumerated separately, held separately, collected separately.
- **Lifecycle governs survival:** member removal, channel deletion and retention policies each change what is recoverable and for how long.
- **The census is the completeness proof:** tenant-wide enumeration recorded before scope is agreed: the exhibit both sides need.

The problem in plain English: the team is not the channel

To a user, a Teams team is a single thing: a name in the sidebar with channels beneath it. To the platform, it is a collection of storage arrangements that happen to be displayed together. When a team was created, Microsoft 365 built a group mailbox and a SharePoint site for it, and standard channels write into those. When someone later created a private channel: to discuss a restructuring with three colleagues, say: the platform did something different: it created a new SharePoint site nobody outside the channel can see and began copying the channel's messages into the members' own mailboxes. A shared channel, added to collaborate with another department or an external partner, did something different again.

Disclosure teams that scope by team name therefore collect the public conversation and miss the private one: the restructuring discussion, the "keep this off the main channel" thread, the file shared only with the inner group. Sometimes the omission is discovered by the other side, who notice a reference to a channel that never appeared in the production; sometimes it is never discovered, and the disclosure certificate is signed over a gap. The remedy is knowledge of the storage model and a census discipline that enumerates every channel type across the tenant before anyone agrees a scope: the technical fact this guide exists to make legal common knowledge.

Where the data actually lives: standard, private and shared channels compared

- **Standard channels:** messages are held in the Teams service and copied into the team's group mailbox for compliance purposes; files sit in a folder per channel within the team's SharePoint site: the model most collection workflows assume for everything.
- **Private channels:** messages are copied into each member's individual mailbox (in a hidden compliance folder, not visible to the user), so the complete conversation exists across the members' mailboxes rather than in one place; files sit in a dedicated SharePoint site created for the channel, linked to but separate from the team's site: the channel's owner set and membership are recorded in directory and Teams administration data.
- **Shared channels:** messages are held in a dedicated storage location associated with the channel (not the individual members' mailboxes as with private channels), with cross-team and cross-tenant membership possible; files sit in a dedicated SharePoint site per channel: with the additional complexity that external members' organisations hold their own view of the channel under their own tenant's controls.
- **The compliance-tooling view:** Microsoft Purview eDiscovery can locate and collect all three types when the search is scoped correctly: which means knowing the channel type, its storage locations and its members before the search is built: the census of §5.
- **Administration data as the index:** Teams admin reports, Graph API enumeration and audit logs list channels by type, with creation dates, owners, members and site URLs: the index from which the storage map for a given matter is drawn, and the record that proves what existed.

Membership, lifecycle and what survives departures and deletions

- **Member removal:** when a member leaves a private channel, the messages already copied to their mailbox remain there subject to that mailbox's retention: the departed member's mailbox is still a source for the channel's history up to their removal, and their absence from the current membership list does not remove them from the census.
- **User departure and mailbox deletion:** a leaver whose mailbox is deleted takes their copy of every private channel they belonged to: guide 103's territory applied to channels: with the platform's soft-deletion and hold-driven inactive-mailbox mechanisms determining recoverability: the leaver process is the private channel's greatest threat.
- **Channel deletion:** deleted channels enter a recovery window (currently around 30 days, subject to the platform's current settings) during which they can be restored; after it, message copies persist in member mailboxes only as retention allows, and the channel's SharePoint site follows site-deletion and retention rules of its own: two clocks, checked separately.
- **Retention policies:** Teams retention policies for channel messages and private channel messages are configured separately and can differ; SharePoint retention governs the files: a matter's preservation analysis maps all three against the relevant period.
- **Cross-tenant shared channels:** external members' organisations control their own retention and holds; the host tenant's collection captures the channel's messages but the external files and views may need the other organisation's cooperation or a third-party disclosure route.

Holds and collection: scoping so nothing is missed

- **The channel census first:** enumerate every team, every channel and its type, owners, members (current and historical where recoverable), creation and deletion dates, and storage locations: tenant-wide for the relevant custodians and topics: recorded as the completeness exhibit before any scope is agreed.
- **Holds that follow the storage model:** for private channels, holds on every member's mailbox (present and departed, including inactive mailboxes) and on the channel's SharePoint site; for shared channels, holds on the channel's storage location and site; for standard channels, the team's group mailbox and site: with the hold's coverage verified against the census, not assumed from the team name.
- **Collection through compliance tooling:** Purview eDiscovery searches scoped explicitly to the channel types and locations, exporting messages with their metadata (sender, timestamps, edit and deletion markers, reactions, thread structure) and files with theirs: the export documented as guide 53's disciplines require, and the guide 71 reproducibility principle applied: query saved, results hashed.
- **Custodian-based and location-based scope combined:** private-channel messages are collected from custodian mailboxes; a member outside the custodian list may hold the only surviving copy of a departed custodian's contributions: the census reveals when a non-custodian's mailbox must be searched for channel content, with proportionality argued from the census.
- **External and cross-tenant material:** shared channels with external members: the host tenant collection recorded as such, the external organisation's holding identified, and the third-party route (request, then CPR 31.17 where the tests are met) started early where the material matters.

Reconstruction, review and the shape of channel evidence

- **Stitching private channels:** each member's mailbox holds messages as the compliance copies were written; the conversation is reconstructed by deduplicating across members (guide 82's method) and ordering by message identifiers and timestamps (guide 96's normalisation): with gaps visible where a member's mailbox is missing or their membership was partial.
- **Threads, replies and edits:** channel conversations are post-and-reply structures with edit and deletion histories: guide 83's threading discipline adapted; edited messages carry their edit markers, deleted messages may survive as compliance copies with deletion flags: reviewed as history, not as the current view.
- **Files and their versions:** channel files in the per-channel site carry SharePoint version histories (guide 75, guide 102): the collaboratively edited document's lineage available where the site was held in time.
- **Unitisation for review:** channel messages produced per message or per conversation segment, with the guide 81 chat-unitisation decisions made explicitly and disclosed in the protocol (guide 94): reviewable, producible units that preserve context.
- **Meetings, calls and attached artefacts:** channel meeting chats, recordings and transcripts (guide 53's related sources) stored under their own rules: enumerated alongside the channel, collected where relevant.

Proving completeness and challenging the opponent's collection

- **The completeness record:** the census, the hold coverage map, the collection queries and their result counts, and the reconciliation from census to production: the document that turns "we collected Teams" into "we collected these 47 channels, of these types, from these locations, with these results".
- **The certificate's foundation:** the disclosure certificate's search statements rest on the completeness record: a certificate signed over a team-level collection of an estate with private channels is a certificate with a known gap.
- **Reading the opponent's production:** references to channels absent from the production, private-channel folder artefacts in produced mailboxes, files whose site URLs indicate per-channel sites never collected: the tells that a team-scoped collection missed the rest: raised with §11's requests.
- **The disclosure application:** where the opponent's methodology statement cannot account for private and shared channels, specific disclosure of the census and re-collection: PD 57AD's cooperation expectations giving the request its weight.
- **Neutral verification:** on contested completeness, an independent examiner enumerating the tenant's channels under agreed terms (guide 71 §7's pattern): the census done once, for both sides.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: private and shared channel evidence is distributed by design, which makes it fragile in one place and redundant across several. A private channel's messages exist in every member's mailbox: the loss of one custodian's mailbox (deleted, purged, never held) is covered by the others', and the departed member's inactive mailbox may hold what the current members' do not. The channel's files live in their own site, with version histories and the site's recycle and retention mechanisms behind them. The administration layer (Teams admin data, directory records, audit logs) holds the channel's existence, membership and lifecycle even where content is gone: the guide 95 existence evidence for channels. Client-side caches on members' devices (the Teams desktop and mobile clients' local databases) hold recent channel content independently of the tenant (guides 59-66's methods). And for shared channels, the external organisation's tenant holds its own copy under its own controls. When the primary path is closed: the team collected without its private channels, the custodian's mailbox purged, the channel deleted past its window: the map names the alternates in the table's columns.

EVIDENCE	MEMBER MAILBOXES (COMPLIANCE COPIES)	PER-CHANNEL SHAREPOINT SITE	ADMIN / DIRECTORY / AUDIT LAYER	CLIENT-SIDE CACHES	EXTERNAL TENANT (SHARED)	DELETED/RECOVERABLE
Channel messages	Y: every member, private channels	n/a	Existence + activity logs	Recent content	Y: their view	Inactive mailboxes; deletion window
Channel files	n/a	Y: with versions	Site existence + access logs	Sync client copies	Their copies	Site recycle + retention
Membership history	Membership-period inference	Site permissions history	Y: the direct record	n/a	Their membership records	Audit log retention bound
Channel existence + lifecycle	Folder artefacts	Site creation/deletion	Y: creation, deletion, restore	Cached channel lists	Their records	30-day channel restore window
Edits and deletions	Y: compliance copies with markers	Version history	Audit events	Sometimes	n/a	Varies

Fallback strategy in one line: when the team-level collection missed the channel, go to the members' mailboxes, the channel's own site and the admin layer that proves it existed: and for departed members, the inactive mailbox before the leaver process reaches it.

Worked examples

EXAMPLE 1 · THE RESTRUCTURING CHANNEL THAT WAS NOT IN THE PRODUCTION

In an unfair-dismissal and discrimination claim, the employer produced the "HR Transformation" team's channels: nothing damaging. The claimant's review noticed a produced message reading "moving this to the private channel". The §11 request followed: had a private channel existed, who were its members, where were its messages? The employer's provider had collected the team's group mailbox and site only. The census, run belatedly, found a private channel of four members created three days before the claimant's role was flagged "at risk", with messages in the four members' mailboxes (one, a departed HR partner, in an inactive mailbox held only because a different matter's hold covered it). The reconstructed conversation was the case. The employer's completeness position was irrecoverable; the guide's §5 census would have cost a morning.

EXAMPLE 2 · THE LEAVER PROCESS AND THE LAST COPY

A competition investigation needed a private channel's full history. Three of five members remained; two had left, and one leaver's mailbox had been deleted in the routine process after the retention period, taking their compliance copies with it. The reconstruction from the remaining members' mailboxes recovered every message they had been present for; the departed member had been in the channel for its first four months alone, before the others joined. The §8 map supplied the alternates: the channel's SharePoint site, held in time, carried files and version histories from the early period; the audit log recorded the departed member's channel activity (existence, not content); and the leaver's device, still in IT storage, held a Teams client cache with the early messages. The early period was reconstructed from three sources none of which was the primary one: which is the whole argument for holding every member's mailbox the day the matter arises.

EXAMPLE 3 · THE SHARED CHANNEL WITH AN EXTERNAL PARTNER

A joint-venture dispute turned on a shared channel between the two companies' project teams. The host tenant's collection captured the channel messages; the files each side had uploaded sat in the host's per-channel site; but the counterparty's own tenant held their members' view and, it emerged, files their members had shared into the channel from their own storage. The host-side collection was complete for what the host tenant held and was recorded as such; the counterparty's holding was identified in the completeness record; and the disclosure exercise reached it through the counterparty's own obligations as a party. The example is the shared-channel discipline: state exactly what the host tenant holds, identify what it does not, and route the rest through the parties rather than pretending one tenant's export is the whole channel.

Common mistakes and technical limitations

Common mistakes

- **Team-level scoping:** Example 1's omission: the group mailbox and site collected, the private channels never enumerated.
- **Holds on the team, not the members:** private-channel messages left unprotected in member mailboxes the hold never named.
- **Departed members forgotten:** the census taken from current membership; the early contributor's inactive mailbox missed or already purged: Example 2's near-loss.
- **Per-channel sites uncollected:** files assumed to sit under the team's site; the separate sites never searched.
- **Shared channels treated as internal:** the external tenant's holding unstated: Example 3's half-collection presented as whole.
- **Retention assumed uniform:** private-channel and channel-message policies differing unnoticed; the preservation analysis wrong for one of them.
- **Certificates over gaps:** search statements signed without the completeness record that would have revealed the omission.
- **Reconstruction without deduplication:** the same message from five mailboxes produced five times, or worse, threads stitched inconsistently.

Technical limitations

- **Platform behaviour changes:** storage locations, restore windows and tooling scope are Microsoft's to alter: verified against current documentation per matter, per this series' standing rule.
- **Historical membership may be partial:** audit-log retention bounds how far back membership changes can be reconstructed: inferred from mailbox content where the log is silent, and stated as inference.
- **Compliance copies are copies:** the mailbox copy reflects the message as written to compliance storage; certain rich content and later platform features may render differently: the export's fidelity documented.
- **Cross-tenant reach is legal, not technical:** the external organisation's data is theirs; §5's routes take the time they take.
- **Licence tiers gate tooling:** Purview capabilities and audit depth vary with the tenant's licensing (guide 105's caveat): the collectable story bounded by the subscription.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which teams touch the matter, and has anyone enumerated their private and shared channels, with membership history: the §5 census?
- Which relevant people have left, and are their mailboxes inactive-and-held, or already in the leaver process?
- What do the Teams and SharePoint retention policies say for channel messages, private channel messages and channel sites over the relevant period?

Ask your opponent

- Please confirm whether the Teams collection underlying your disclosure included private channels and shared channels, identifying each such channel by name, type, membership (current and historical), creation and any deletion date, and the storage locations from which its messages and files were collected.
- Please confirm that litigation holds were applied to the individual mailboxes of all private-channel members, including departed members' inactive mailboxes, and to each per-channel SharePoint site, and the dates on which those holds took effect.
- Please provide the completeness reconciliation from channel census to production for the teams identified in Schedule 1.

Ask your eDiscovery / forensic provider

- Is the census tenant-wide and recorded: every channel, type, members (historical), site URL?
- Does the hold map cover every member mailbox and per-channel site the census lists: and what is exposed if a leaver is processed tomorrow?
- How was the private-channel reconstruction deduplicated and ordered, and where are the gaps stated?

SUGGESTED WORDING · TEAMS CHANNEL PARAGRAPH FOR THE DRD / PROTOCOL

"Microsoft Teams sources shall be identified by a census of all teams relevant to the issues, enumerating each standard, private and shared channel with its type, owners, current and historical membership so far as recoverable, creation and deletion dates, and storage locations (including per-channel SharePoint sites and, for private channels, the member mailboxes holding compliance copies). Preservation shall extend to all such locations, including inactive mailboxes of departed members. Collection shall be scoped explicitly to each channel type and location, with queries and result counts recorded, and a reconciliation from census to production maintained and disclosed on request. For shared channels with external members, the collecting party shall state what its tenant holds and identify holdings of the external organisation."

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

The Teams channel checklist

- ☐ Tenant-wide channel census recorded: type, members, history, sites
- ☐ Private-channel member mailboxes held, departed members included
- ☐ Inactive mailboxes protected from the leaver process
- ☐ Per-channel SharePoint sites enumerated and held
- ☐ Shared-channel storage and external holdings identified
- ☐ Retention policies mapped separately for each channel type and for sites
- ☐ Collection queries scoped per type and location; results hashed
- ☐ Reconstruction deduplicated and ordered; gaps stated
- ☐ Meetings, recordings and transcripts enumerated alongside
- ☐ Census-to-production reconciliation ready for the certificate

Red flags

- Productions referencing channels that never appear: Example 1's tell.
- Collections described only by team name.
- Leaver processes running on relevant custodians during the matter: Example 2's clock.
- Files whose site URLs indicate per-channel sites never collected.
- Shared channels produced as if wholly internal: Example 3's half.
- Methodology statements silent on channel types.
- Certificates signed without a census.

When to involve a digital forensic expert

At scoping, where the census is run and the hold map built before the leaver process reaches anyone (Example 2's discipline); at collection, where the per-type queries are built, documented and reconciled; at review, where private-channel reconstruction is deduplicated and ordered honestly; and at challenge, where the completeness record is exhibited or the opponent's absence of one is exposed, under CPR Part 35 where needed. Through **e-discovery.uk**, Teams collections run channel-by-channel as standard: the private channel is where the candid conversation happened, and the collection either found it or signed over its absence.

§ 1 3 · COMMON QUESTIONS

Frequently asked questions

We collected the whole team. Why would private channels be missing?

Because "the whole team" means the team's group mailbox and SharePoint site, and private channels write to neither: their messages go to member mailboxes and their files to separate sites (§3). The collection was complete for standard channels and blind to the rest: Example 1's omission, and the reason the census comes first.

A private-channel member has left the company. Is their contribution lost?

Not necessarily: their compliance copies persist in their mailbox as long as it exists (inactive mailboxes under hold survive the leaver process), other members' mailboxes hold the same messages for their overlapping membership periods, and the channel site, audit layer and device caches supply alternates (§8, Example 2). What loses the contribution is a mailbox purged before anyone held it: the clock the census exists to beat.

How do we know the census is complete?

From the administration layer: Teams admin data, directory records and Graph enumeration list channels by type with creation, membership and site details, and audit logs record channel lifecycle events: the census is drawn from those records and reconciled against them, not from asking users. On contested completeness, an independent examiner's enumeration under agreed terms settles it (§7).

Can deleted private channels be recovered?

Within the platform's restore window (currently around 30 days, verify per matter), the channel can be restored; afterwards, message copies survive in member mailboxes subject to retention, and the channel's site follows its own deletion and retention rules (§4). Two clocks, both checked: and the audit layer proves the channel existed either way.

The channel was shared with another company. Whose disclosure is it?

Both: the host tenant holds the channel messages and the host-side site; the external organisation holds its members' view and any files shared from its own storage (§4, Example 3). The host party discloses what it holds and identifies what it does not; the rest is reached through the other party's obligations or third-party disclosure.

Does this matter for small disputes, or only large investigations?

It matters wherever the candid conversation may have happened, which is exactly what private channels are for: an employment claim's decisive thread is as likely to sit there as a cartel's. The census is proportionate at any scale: a morning's work that determines whether the collection is complete or the certificate is wrong.

§ 1 4 · REFERENCE

Glossary

Channel census

The tenant-wide enumeration of channels by type, membership and location.

Compliance copy

The message copy written to a mailbox for retention and eDiscovery.

Group mailbox

The team-level mailbox holding standard-channel compliance copies.

Inactive mailbox

A departed user's mailbox preserved under hold after account deletion.

Per-channel site

The separate SharePoint site created for a private or shared channel.

Private channel

A channel whose messages live in member mailboxes and files in its own site.

Purview eDiscovery

Microsoft 365's compliance search and collection tooling.

Restore window

The period in which a deleted channel can be recovered.

Shared channel

A channel with cross-team or cross-tenant membership and dedicated storage.

Standard channel

A channel stored in the team's group mailbox and site.

Sources and authoritative references

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

- e-discovery.uk, EDRM Phase 02 · Identification and Phase 04 · Collection (Teams censuses, holds and channel-scoped collection as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- cflab.uk, digital forensics services (Microsoft 365 collections, completeness verification, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft Learn, Microsoft Purview eDiscovery and Teams: learn.microsoft.com, [eDiscovery for Teams](https://learn.microsoft.com/en-gb/purview/e-discovery) · Private channels: [learn.microsoft.com, private channels](https://learn.microsoft.com/en-gb/purview/e-discovery/private-channels) · Shared channels: [learn.microsoft.com, shared channels](https://learn.microsoft.com/en-gb/purview/e-discovery/shared-channels)
- PD 57AD: [justice.gov.uk](https://www.justice.gov.uk/procedures/PD/57AD), PD 57AD · CPR Part 31 (r.31.17): [justice.gov.uk](https://www.justice.gov.uk/procedures/PD/57AD), Part 31 · CPR Part 35: [justice.gov.uk](https://www.justice.gov.uk/procedures/PD/57AD), Part 35
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: [iso.org](https://www.iso.org), 27037

DISCLAIMER

This publication provides general information about collecting evidence from Microsoft Teams private and shared channels as at August 2026. Microsoft 365 storage models, retention behaviour, restore windows and tooling capabilities change; verify the current platform position for the tenant and 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

Teams work at **e-discovery.uk** starts with the census, not the team name: every channel enumerated by type with membership history and storage locations, the hold map built to cover member mailboxes (departed members' inactive mailboxes first, because the leaver process is the clock), per-channel sites and shared-channel storage; collection scoped per type with queries and counts recorded; private-channel reconstruction deduplicated and ordered with gaps stated; and the census-to-production reconciliation maintained as the certificate's foundation and the challenge's answer. The laboratory side audits opposing Teams productions for the §7 tells and verifies completeness as a neutral where the parties agree. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a relevant custodian's leaving date is this month, the inactive-mailbox hold is this week's task: the private channel's last copy may be in it.



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