# Slack EDiscovery

Slack's architecture, including channels, DMs, and retention tiers, significantly influences what evidence is available for electronic disclosure. This guide details the data model, collection methods, and common pitfalls, helping practitioners navigate Slack e-discovery challenges.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30. https://e-discovery.uk/library/slack-ediscovery

SLACK EDISCOVERY · A GUIDE FOR UK LAWYERS Slack e Discovery Channels, DMs, Threads, Edits, Retention Tiers and Exports: Disclosing the Workspace Where Work Actually Happens COMPUTER FORENSICS LAB

## § ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ 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

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: INSLACK, THESUBSCRIPTIONTIERANDASETTINGSPAGE DECIDEWHATEVIDENCEEXISTS: AUDITTHELATTICEBEFOREPROMISINGANYTHING

§ 02 · FIRST PRINCIPLES The problem in plain English: the office that talks in channels

§ 03 · THE DATA MODEL The data model: channels, DMs, threads, files, apps COMPONENT EVIDENTIAL CHARACTER

§ 04 · THELATTICE The lattice: plan tiers, retention settings and what survives

§ 05 · MESSAGEDYNAMICS Edits, deletions and message history

§ 06 · GETTINGITOUT Collection routes: exports, APIs and their fidelity

§ 07 · INTO REVIEW Processing and review: making channels reviewable

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE (ROUTE- (DIGESTS, WORKSPACE EMAIL DEPENDENT) FORWARDS) CLIENT INTEGRATIONS / CONNECT DELETED / CACHES MIRRORS COUNTERPART RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THERETENTIONRULEWITHABIRTHDAY EXAMPLE2 · THEDMLAYERTHEEXPORTNEVERREACHED EXAMPLE3 · THEEDITHISTORYTHATREVERSEDTHEREADING

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes JSON. Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · SL AC KLIMBFORTHEPRESER VAT I ON LETTER

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The Slack checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can we get employees' Slack DMs, or are they private? Our client's Slack only goes back 90 days. Is the case dead? Are Slack messages disclosable documents like email? The key message says "(edited)". What can we find out? How should Slack evidence be presented to a tribunal? What about Teams, Discord, and the other chat platforms?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

## Questions and answers

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

On eligible plans, workspace owners can law full y 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 (end point 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 in form a l 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 what ever 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. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 15 of 17