

Collecting Evidence From Google Workspace

Understand the forensic collection of Google Workspace evidence for UK litigation. This guide details preservation, collection routes, and common pitfalls across Gmail, Drive, Chat, and Admin data, providing essential insights for legal practitioners.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
<https://e-discovery.uk/library/collecting-evidence-from-google-workspace>

GOOGLE WORKSPACE EVIDENCE · A GUIDE FOR UK LAWYERS Collecting Evidence from Google Workspace Gmail, Drive, Shared Drives, Chat, Meet and Admin Data: the Other Tenant, Mapped 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: same instincts, different geography 03 The estate map: service by service 04 Preservation: holds, retention and the leaver licence trap 05 Collection routes: Vault, Takeout, API and their fidelity 06 Drive evidence: ownership, Shared Drives and revision histories 07 The admin layer: audit reports and account records 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: THEM365DISCIPLINESTRANSFERWHOLE; ONLYTHEMECHANICS ARE GOOGLE ' S 52 framework: trust, structures, downstream: chooses among them here exactly as there. The distinctly

§ 02 · FIRST PRINCIPLES The problem in plain English: same instincts, different geography

§ 03 · THEMAP The estate map: service by service SERVICE WHAT IT HOLD S · WHAT MATTERS EVIDENTIALLY

§ 04 · STOPPINGTHECLOCKS Preservation: holds, retention and the leaver licence trap

§ 05 · GETTINGITOUT Collection routes: Vault, Takeout, API and their fidelity

§ 06 · THECROWNJEWELS Drive evidence: ownership, Shared Drives and revision histories

§ 07 · THEDIARYHERE The admin layer: audit reports and account records

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE (VAULT SYNC / AUDIT EXPORT WORKSPACE DEVICE ADMIN / BACKUP / REACH) CACHES REPORTS LAYER COUNTERPART DELETED / TENANTS RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEREVISIONSTREAMTHATDATEDTHEDEALMEMO EXAMPLE2 · THEHISTORY - OFFSPACEANDTHETWOPHONES EXAMPLE3 · THEDELETEDACCOUNTINSIDETHE20DAYS

§ 10 · WHERE IT GOES WRONG Common mistakes and technical limitations Common mistakes
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 · WORKS PAC ELIMB FORTHE WEEK- ON E INSTRUCTION

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

§ 13 · COMMON QUESTIONS Frequently asked questions Is Google Vault the same kind of
thing as Microsoft Purview? Can deleted Gmail be recovered? How reliable are Google Docs
revision histories as evidence? The space had history off. Is the chat genuinely gone? What
happens to a departed employee's My Drive files? We are a Microsoft firm facing a
Google-estate opponent. What do we ask first?

§ 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. INSTRUCT THE LAB
NEW ENQUIRIES EMAIL - DISCOVERY

Questions and answers

Is Google Vault the same kind of thing as Microsoft Purview?

Functionally sibling: holds, retention, search, export over the tenant's services: and the same jurisprudence of use applies: defensible for scope and bulk, structurally limited at the edges (revision series, history-off Chat), operator-dependent for trust. Guide 52's three questions: trust, structures, downstream: choose between Vault and independent routes exactly as they choose around Purview; guide 59 examines Vault's capabilities and limits in full.

Can deleted Gmail be recovered?

Run the layer walk: user trash within its window; Vault-held mail regardless of deletion (the hold date governs); retention-rule coverage; then the architecture: device mail caches, counterpart recipients, backup platforms. Google-specific wrinkle: labels mean "deleted from Inbox" often just means relabelled: the message may simply be else where in the mailbox. The four facts of guide 53 translate: hold status and date, retention rules, window position.

How reliable are Google Docs revision histories as evidence?

Highly, within stated limits: platform-maintained, editor-attributed, timestamped, and effectively impossible for users to falsify retrospectively: Example 1's decisiveness is typical. The caveats are granularity (old revisions can be consolidated: the stream's resolution is stated per document), shared-credential attribution (the join, as ever) and collection route (streams survive as series only via the structural route). Collected properly, they are among the strongest drafting evidence in either ecosystem.

The space had history off. Is the chat genuinely gone?

From the tenant, very largely yes: that is what the setting does, and Vault cannot reach what was never kept. But Example 2 is the standard answer: participants' device caches, the other or g an is at i on in external conversations, screenshots and forwards as corroboration, and the setting's own change history as potential conduct evidence. "History off" ends the tenant inquiry and starts the architecture one.

What happens to a departed employee's My Drive files?

They ride the account: suspension preserves everything; deletion starts the 20-day restore clock, with an option at deletion to transfer Drive ownership to another user (which preserves content but rewrites provenance: the transfer is documented and stated). Shared Drive files are unaffected by member departure: the design reason disputes increasingly turn on which regime owned the file. The advice is unchanging: suspend, decide later.

We are a Microsoft firm facing a Google-estate opponent. What do we ask first?

Three requests, all in this guide's §11: hold scope and dates plus retention rules with change history (the preservation position); the admin audit reports for the period (the diary, before its windows roll); and route-and- fidelity c on firm at i on for their collection (what their exports preserved of labels, threads and revisions). The answers map their estate and their conduct at once: and nothing in them requires you to run Workspace yourself. 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

Source: <https://e-discovery.uk/library/collecting-evidence-from-google-workspace>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.