Forensic Evidence From Dropbox Box And ShareFile

This guide details how to uncover forensic evidence from independent file platforms such as Dropbox, Box, and ShareFile. It covers platform records, desktop client artefacts, and external collaboration trails. Learn about preservation, collection, and deployment strategies for cloud evidence, including common mistakes and expert involvement.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/forensic-evidence-from-dropbox-box-and-sharefile

FILE - SHARINGPLATFORMS · A GUIDE FOR UK LAWYERS Forensic Evidence from Dropbox, Box and Share File Sync Artefacts, Activity Logs and Sharing Trails on the Independent File Platforms COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES FILE-PLATFORM COLLECTION SYNC-CLIENT ARTEFACT ANALYSIS CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: DROPBOX, BOXANDSHAREFILEEACHKEEPAPLATFORM - SIDE EVERY MACHINE: COLLECTBOTH, BECAUSETHEPLATFORMPROVESWHATHAPPENED ANDTHECLIENTCORROBORATESITWHERETHEACCOUNTISDENIEDORGONE

§ 02 · FIRST PRINCIPLES The problem in plain English: the third file platform nobody mapped

§ 03 · THEPLATFORMRECORD The platform record: version histories, activity logs and sharing trails

§ 04 · THEDESKTOPCLIENTS The desktop clients: local sync databases and machine artefacts

§ 05 · SHARING, LINKSANDEXTERNALCOLLABORATION Sharing, links and external collaboration: who reached the data

§ 06 · PRESERVATION AND COLLECTION Preservation and collection: admin export, API and legal process

§ 07 · DEPLOYMENT Deployment: disclosure, exfiltration and the account nobody admits to

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION CLIENT (PROXY/ PLATFORM LOG + COLLABORATORS PROVIDER BEHAVIOURAL + VERSION + COUNTERPARTS RECORDS EXPENSE LAYER HISTORY DESKTOP- NETWORK DATABASE CASB)

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEDEALROOMANDTHECOLLABORATORWHOLINGERED EXAMPLE2 · THEACCOUNTNOBODYPUTINTHEDATAMAP EXAMPLE3 · THESHAREFILEPORTALANDTHESANCTIONEDSHARE

§ 10 · WHEREITGOESWRONG 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

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

§ 13 · COMMON QUESTIONS Frequently asked questions Do Dropbox, Box and Share File keep the kind of logs we need? The account has been deleted. Is the evidence gone? Someone shared a folder externally. How do we find out who reached it? We found a Dropbox client on a laptop but nobody admits to the account. What now? The other side accuses us of leaking through our sharing platform. How do we answer? How is this different from One Drive or Google Drive?

§ 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

Do Dropbox, Box and Share File keep the kind of logs we need?

Business and enterprise tiers do: activity logs of views, downloads, edits, shares and deletions with user and timestamp, plus version histories and sharing records (§3): personal and small-business tiers log less and retain shorter, and export capability varies by product. The account's actual tier and retention are established first, and the desktop client corroborates what ever the platform kept.

The account has been deleted. Is the evidence gone?

Not necessarily: the desktop-client database on every machine that synced it survives the account, naming the files and the account (§4, Example 2 in reverse); the platform provider's server-side records are reachable by process; and collaborators hold their side of every share. The two-record method exists precisely so that a deleted account is not a dead end.

Someone shared a folder externally. How do we find out who reached it?

From the sharing and activity logs: the link's creation names the creator and time, and: where the platform logs link usage: the access record names who followed it and from where (§5, Example 1's lingering collaborator). Where the platform logs only that a link exists, the "who reached it" question is answered as far as it allows, and the collaborators' own records fill the gap.

We found a Dropbox client on a laptop but nobody admits to the account. What now?

The local database names the account and lists what it held (§4, Example 2); the network and expense records confirm its use and who paid; and the account is then reached through the party's cooperation once its existence is undeniable, or through process if it is personal. Shadow IT hides in exactly this way, and the end point is where it surfaces.

The other side accuses us of leaking through our sharing platform. How do we answer?

With the platform's own record: the sharing and activity logs show exactly what was shared, with whom, and who accessed it (§3, §5), and the governance and engagement baseline shows what was sanctioned (Example 3's client-requested delivery). The same log that would prove a leak proves its absence; run the two-record method and let the platform speak.

How is this different from One Drive or Google Drive?

The principles are the same: platform log plus client artefact, versions, sharing, retention: but the specifics differ per product, and these platforms are far more likely to be unmapped shadow IT and to be used for external collaboration and deal rooms (§2, §7). The examiner reads each on its own terms, and the data-mapping discipline matters more, not less, because nobody put them on the list. 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