COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Forensic Evidence from Dropbox, Box and ShareFile

Sync Artefacts, Activity Logs and Sharing Trails on the Independent File Platforms

Not all cloud storage is Microsoft or Google. Dropbox, Box, ShareFile and their peers sit in countless businesses as the file-sharing layer, the deal room, the client-collaboration space, the shadow-IT repository the finance team set up years ago. Each keeps its own forensic record: version histories, activity and access logs, sharing and link trails, and a desktop sync client that leaves a detailed local database on every machine it touches. The evidence is rich but platform-specific: the log a Dropbox admin can export differs from Box's, ShareFile's audit trail answers different questions again, and the sync client's local artefacts vary by product and version. For the lawyer, these platforms raise the familiar questions: what was stored, who accessed it, what was shared and with whom, what was deleted and when, and: because they are so often used for exactly this: what left the business through them. This guide sets out for UK lawyers where each platform records its evidence, how the desktop clients corroborate it locally, how to preserve and collect it, and how it is deployed.

⏱ 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 Dropbox, Box, ShareFile and comparable platforms across disclosure and investigation work, reading their admin logs and version histories against the desktop clients' local databases, and reaching accounts through admin export, API and legal process: with reporting under CPR Part 35 where a file platform's record is the issue.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | FILE-PLATFORM COLLECTION | SYNC-CLIENT ARTEFACT ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: DROPBOX, BOX AND SHAREFILE EACH KEEP A PLATFORM-SIDE RECORD (VERSIONS, ACTIVITY, SHARING) AND LEAVE A DESKTOP-CLIENT RECORD ON EVERY MACHINE: COLLECT BOTH, BECAUSE THE PLATFORM PROVES WHAT HAPPENED AND THE CLIENT CORROBORATES IT WHERE THE ACCOUNT IS DENIED OR GONE

The platform record (§3): each product keeps file version histories, an activity or audit log recording who did what (view, download, edit, share, delete, restore) with timestamps and, on business tiers, IP and device context, and a sharing record of links and collaborators: exportable by administrators and reachable through each platform's API, with the honest caveat that log depth, retention and export capability vary sharply by product and by subscription tier. **The desktop clients (§4):** the Dropbox, Box Drive and ShareFile desktop applications each maintain a local database and cache on the machines they run on, recording the files synced, their paths and states, and account details: a rich local artefact that survives independently of the platform and proves what a given machine held and mirrored, defeating the "I never had that account" and the deleted-account problems. **Sharing (§5):** shared links (with and without passwords and expiry), folder collaborators, external-guest access and deal-room permissions: the record of who could reach the data and, where the platform logs it, who did: the file-sharing platform's defining risk and its defining evidence. **Preservation and collection (§6):** administrator holds and exports where the business controls the account; API collection for completeness and version histories; and legal process (preservation letters, undertakings, orders, provider disclosure per guide 111 §6) where the account is personal or the platform outside the party's control. **Deployment (§7):** ordinary disclosure of relevant content; exfiltration proof where the platform was the route out (guide 111); and the recurring shadow-IT problem: the departmental Dropbox or client ShareFile nobody put in the data map, surfaced by the desktop clients and the network logs.

- **Two records per platform:** the server-side log and version history, and the desktop client's local database: collect both.
- **Coverage varies by tier:** log depth, retention and export differ by product and subscription: established per account, not assumed.
- **The client survives the account:** the local sync database proves what a machine held even when the account is denied or deleted.
- **Sharing is the risk and the evidence:** links and collaborators are what these platforms are for, and what their logs record.
- **Shadow IT hides here:** the unmapped departmental account, surfaced by the desktop clients and the proxy logs.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the third file platform nobody mapped

When a lawyer maps a client's data, they think of email, the file server, and the Microsoft or Google cloud. The Dropbox the marketing team has used since 2016, the Box deal room the corporate team stood up for a transaction, the ShareFile portal the accountants share statements through: these live in the blind spot, run on a corporate card nobody reconciles to IT, and hold exactly the material a dispute wants. They are not obscure; they are ubiquitous and unmapped, and a disclosure exercise that never asks "what else do you share files through?" will miss them as reliably as it misses Teams private channels (guide 101).

Each of these platforms is, forensically, generous: it keeps versions, it logs activity, it records every share, and it installs a desktop client that writes a detailed local database on every machine. The difficulty is not that the evidence is thin but that it is platform-specific and tier-dependent: what a Box administrator can export differs from what Dropbox offers, what a business tier logs differs from what a personal one keeps, and the desktop clients' local artefacts vary by product and version. The examiner reads each platform on its own terms, corroborates the server record with the client record, and: crucially: finds the accounts the data map forgot. This guide is that per-platform, two-record method.

§ 0 3 · THE PLATFORM RECORD

The platform record: version histories, activity logs and sharing trails

- **Version histories:** each platform retains prior versions of files (guide 102's discipline applied to independent platforms), with retention varying by product and tier: the drafting and alteration history available where the platform kept it, exported through admin tools or the API.
- **Activity and audit logs:** business tiers record events: view, preview, download, upload, edit, move, delete, restore, share, unshare, login: with the acting user, timestamp and, commonly, IP and device: Dropbox's team activity, Box's enterprise events, ShareFile's activity log: each with its own event vocabulary and retention, read per guide 105 §5's semantics discipline.
- **Deletion and recovery records:** deleted files in the platform's trash or recycle store for a retention period, with the deleting user and time (guide 106 §3), and restore events logged: the deletion attributed and dated on the platform's own record.
- **Administrative actions:** user provisioning and de-provisioning, permission changes, external-sharing policy settings and their changes: the account and governance history, relevant to who could do what and when.
- **The tier and retention caveat:** personal and small-business tiers log less and retain shorter than enterprise tiers; some events are logged only above a threshold; export capability itself varies: the account's actual configuration and retention established first, and the gaps stated in the methodology.

§ 0 4 · THE DESKTOP CLIENTS

The desktop clients: local sync databases and machine artefacts

- **The local sync database:** the Dropbox, Box Drive and ShareFile desktop clients each keep a local database recording the files synced to that machine, their paths, sizes, states and, often, hashes and timestamps: naming what the machine held and mirrored, independent of the platform: the artefact that answers "what was on this laptop?" when the account is gone.
- **Account and configuration artefacts:** client configuration files, credential stores and settings naming the account(s) signed in, the sync folders selected, and the linked devices: the destination or source account identified from the machine (guide 111 §4).
- **Cached content and placeholders:** locally cached file content (fully synced or on-demand placeholder), thumbnails and previews: the material itself, or evidence of its presence, on the endpoint.
- **Operating-system corroboration:** the platform's sync folder appearing in file-system metadata, recent-file and shortcut artefacts, and the client's own logs recording sync operations: the guide 105 §4 endpoint layer, specialised to the sharing client.
- **Multiple accounts and personal use:** the client signed into a personal account on a work machine, or a work account on a personal machine: the local database naming both, and the exfiltration and BYOD questions of guide 111 answered from the client's own record.

§ 0 5 · SHARING, LINKS AND EXTERNAL COLLABORATION

Sharing, links and external collaboration: who reached the data

- **Shared links:** links to files and folders, with or without passwords, expiry dates and download permissions: created, and (where the platform logs it) followed: the link's creation naming the creator and time, its usage log naming who reached the data and from where (guide 105 §5).
- **Folder collaborators and permissions:** the members of a shared folder or deal room, their permission levels, and the history of additions and removals: who had standing access, when it was granted, and by whom.
- **External guests:** outside-the-organisation collaborators and guests, their email addresses and access history: the external reach these platforms are built for, and the confidentiality and exfiltration risk it carries.
- **Deal rooms and portals:** Box and ShareFile's structured collaboration spaces, with per-user access logs and, in some products, view-tracking and watermarking: the transaction's or matter's participants and their activity, richly recorded.
- **The sharing question answered both ways:** for the party protecting data, who reached it and how; for the party accused, whether access was sanctioned collaboration or unauthorised exfiltration: the log read for the fact and the context alike.

§ 0 6 · PRESERVATION AND COLLECTION

Preservation and collection: admin export, API and legal process

- **Where the business controls the account:** administrator holds (legal-hold features where the platform offers them), and export of content, version histories, activity logs and sharing records through admin tools and the platform API: the guide 71 reproducibility principle applied: query and scope recorded, results hashed.
- **API collection for completeness:** where admin export is limited, the platform's API enumerates files, versions, sharing and activity for targeted, documented collection: the method of choice where the complete record matters and the admin console falls short.
- **Retention beaten:** activity logs and version histories on their retention clocks (§3's caveat) exported at the earliest moment, per guide 105 §6: the platform's record preserved before it ages out.
- **Personal and uncontrolled accounts:** preservation letters, undertakings and delivery-up or imaging orders (guide 111 §6, guide 97 §7), and provider disclosure through the platform's legal-process channel where the holder will not cooperate: the account reached through law where admin access does not exist.
- **The desktop clients collected regardless:** the local sync databases and artefacts imaged from the relevant machines (guide 105 §4): the endpoint record secured whether or not the platform account is reachable, and often the only route where a personal account is denied.

§ 0 7 · DEPLOYMENT

Deployment: disclosure, exfiltration and the account nobody admits to

- **Ordinary disclosure:** the relevant content of a corporate Dropbox, Box or ShareFile collected and produced like any other source, with the sources named in the DRD and the platform's activity log corroborating completeness (guide 101 §7's discipline, for file platforms).
- **Exfiltration:** where the platform was the route out (the personal Dropbox of guide 111 Example 3, the shared folder to an outside address), the platform log and the desktop client's database supply the manifest and the destination, deployed for springboard and confidential-information relief (guide 111 §7).
- **The shadow-IT account:** the departmental or client platform nobody mapped, surfaced by desktop clients found during endpoint examination, proxy and CASB logs (guide 111 §5), and expense records: added to the data map and collected, and: where it holds relevant material never disclosed: raised against the opponent whose custodian interviews should have found it.
- **Access and sharing disputes:** the confidentiality breach, the leaked deal-room document, the collaborator who exceeded their access: the sharing and activity logs of §3 and §5 answering who reached what, deployed per guide 105.
- **The innocent explanation:** the sanctioned collaboration, the client's own portal use, the deal room's intended participants: tested against the platform's governance and the role baseline before misuse is alleged (guide 97 §6, guide 111 Example 3).

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a file-sharing platform's evidence sits in two primary records that fail independently: the platform's server-side log and version history, and the desktop client's local database on every machine that synced it. Around them lie the corroborating layers: the network's record of connections to the platform (proxy, CASB), which finds the account the data map missed; the counterparties' and collaborators' own access, on their side of every share; the platform provider's server-side history, reachable by process where the account is denied; the backups, where the business backs the platform up; and the behavioural layer, where the account is named in messages and expense records. When the platform log is thin (a low tier) or gone (retention expired, account deleted), the desktop clients still name the files and the account; when the desktop was wiped (guide 110), the platform log still records the activity; when both the party controls are silent, the provider and the collaborators hold the record. The two-record method is the platform's answer to every single-source failure.

QUESTION	PLATFORM LOG + VERSION HISTORY	DESKTOP-CLIENT DATABASE	NETWORK (PROXY/ CASB)	COLLABORATORS + COUNTERPARTS	PROVIDER RECORDS	BEHAVIOURAL + EXPENSE LAYER
What was stored	Y: files + versions	Y: local file list	Volume of transfer	Shared items	Server-side inventory	References in messages
Who accessed / downloaded	Y: activity log	Local access traces	Connection records	Their access log	Y: server-side access	n/a
What was shared, with whom	Y: links + collaborators	Share artefacts	n/a	Y: the recipient	Sharing history	Named in correspondence
What was deleted, by whom	Y: trash + deleter	Sync-state residue	n/a	n/a	Server-side deletion record	n/a
Which account, whose	User identity	Y: account in client config	Destination host	n/a	Account holder	Y: expenses, messages

Fallback strategy in one line: hold the platform log and the desktop database together; when the platform record is thin or gone, the client names the files and the account; and the network and expense layers find the account nobody mapped.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DEAL ROOM AND THE COLLABORATOR WHO LINGERED

A corporate seller alleged that confidential deal-room documents had reached a rival bidder after the process closed. The Box deal room's enterprise activity log (§3) was decisive: it recorded, for each document, every view and download by user and time; it showed a junior member of one bidder's team downloading the entire financial model at 02:10 on the day the exclusivity was signed; and, more tellingly, it showed that member's access had not been removed when the bidder withdrew, and a login and bulk download from that account eleven days later, from an IP that resolved to the rival's offices. The §5 sharing record showed no further external share; the exfiltration had been a simple failure to revoke access, exploited. The seller's remedy ran on the log; the rival's "we had no access" position collapsed against the platform's own record of the access it had never lost.

EXAMPLE 2 · THE ACCOUNT NOBODY PUT IN THE DATA MAP

In a professional-negligence claim, the defendant firm's disclosure was thin on the working files behind the impugned advice. The claimant's forensic review of a produced laptop found the answer the custodian interviews had missed: a Dropbox desktop client, signed into a firm-branded account, its local database (§4) listing 12,000 working files across every matter the firm ran, none of which appeared in the disclosure. The account had been set up years earlier by a partner, paid on a personal card, and never mentioned to the firm's litigation team or its IT function: genuine shadow IT (§7). The §6 process secured the account through the firm's cooperation once its existence was undeniable; the working files it held changed the case. The desktop client had surfaced the account a data map built from interviews alone would never have found: which is why endpoint examination and proxy logs are run against every custodian list.

EXAMPLE 3 · THE SHAREFILE PORTAL AND THE SANCTIONED SHARE

An accountancy practice was accused by a former client of leaking the client's financial statements, on the basis that the statements had been "shared externally" through the practice's ShareFile portal. The §3 activity log and §5 sharing record told the innocent story: the external share had been to the client's own nominated email address, created on the day the engagement letter recorded the client requesting electronic delivery, with a password sent separately and an access log showing only the client's own IP following the link. No other external share of the statements existed; no download by any third party appeared. The §7 innocent-explanation analysis, run against the engagement terms, showed the share was the delivery the client had asked for. The allegation failed. The platform that could have proven a leak proved its absence: the two-record method clears as readily as it convicts.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The platform never mapped:** Example 2's Dropbox: custodian interviews that never asked "what else do you share files through?".
- **Platform log only, no client:** the account collected, the desktop databases that would corroborate and survive it never imaged.
- **Client only, no platform:** the local database read, the far richer server-side activity and sharing log never exported.
- **Tier assumed uniform:** enterprise-grade logging expected of a personal or small-business account that never kept it: §3's caveat ignored.
- **Sharing not distinguished from access:** a link's creation read as a third party reaching the data without the usage log that shows who did.
- **Retention missed:** the activity log aged out during deliberation: guide 105 §6's clock, per platform.
- **Sanctioned collaboration alleged as leak:** Example 3's share: the governance and engagement baseline never checked.
- **Personal accounts self-helped:** the personal Dropbox accessed without process: guide 111 §6's law bypassed.

Technical limitations

- **Logging and export vary by product and tier:** the investigable record is bounded by the subscription and the platform: established and stated per account.
- **Link-usage detail varies:** some platforms log who followed a link, some only that it exists: the "who reached it" question answered as far as the platform allows.
- **Client artefacts differ by version:** the desktop database's format and content change across product versions: parsed to the specific version, not assumed.
- **Provider disclosure is jurisdictional:** each platform's legal-process channel and data location differ: planned early where the account holder will not cooperate.
- **Shadow IT resists mapping:** unpaid-through-IT accounts appear only in endpoints, network logs and expenses: the data map is only as complete as those are searched.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which file-sharing platforms does the business use, on what tiers, and who administers each: including the accounts IT does not manage?
- What are the activity-log and version-history retention settings on each, and can they be exported now?
- Which machines run the desktop clients, and are they available for imaging?

Ask your opponent

- Please identify all file-sharing and collaboration platforms (including Dropbox, Box, ShareFile and comparable services) used in connection with [the matter], the accounts and tiers concerned, and confirm whether each was placed under hold and collected, including version histories, activity logs and sharing records.
- Please disclose the activity-log and sharing records for [documents / folders] during [period], identifying accesses, downloads, shares, links, collaborators and deletions with the acting user, timestamp and, where recorded, IP and device.
- Please confirm the retention applicable to those logs and version histories and the date on which each was preserved.

Ask your eDiscovery / forensic provider

- What does each platform's tier actually log and retain, and has it been exported before it expires?
- Do the desktop-client databases corroborate the platform record, and do they name accounts the data map missed?
- For any share in issue, does the platform log who followed the link, and what does it say?

SUGGESTED WORDING · FILE-PLATFORM PARAGRAPH FOR THE DRD / PROTOCOL

> "File-sharing and collaboration platforms (including Dropbox, Box, ShareFile and comparable services), whether administered by the party's IT function or otherwise, are data sources for the purposes of disclosure. Each party shall identify such platforms and accounts by reference to administrator records, endpoint examination of desktop-client artefacts, and network and expense records; shall place relevant accounts under hold; and shall collect content, version histories, activity and audit logs, and sharing and link records, recording the tier and retention applicable to each. Where an account is personal or otherwise outside the party's administrative control, the party shall identify it and the relevant content, and the parties shall address access to it by undertakings, order or provider disclosure. Desktop-client sync databases on relevant devices shall be preserved and collected as corroborating sources."

§ 12 · QUICK CONTROL

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

The file-platform checklist

- ☐ All file-sharing platforms and accounts identified, IT-managed and not
- ☐ Endpoints examined and proxy/expense records searched for shadow-IT accounts
- ☐ Tier and retention established per account; logs exported before expiry
- ☐ Platform record collected: content, versions, activity, sharing
- ☐ Desktop-client databases imaged from relevant machines
- ☐ Sharing distinguished from access; link-usage logs read where available
- ☐ Deletions and restores attributed from the platform trash and log
- ☐ Personal and uncontrolled accounts reached by process, not self-help
- ☐ Governance and engagement baseline checked before misuse alleged
- ☐ Completeness reconciled and recorded for the certificate

Red flags

- Desktop clients on endpoints with no corresponding account in the data map: Example 2.
- Collaborators or guests whose access was never revoked: Example 1's lingerer.
- External shares of whole folders or deal rooms.
- Accounts paid on personal or departmental cards outside IT.
- Activity logs at personal-tier depth on business-critical data.
- Disclosure thin on working files a shared platform would hold.
- Leak allegations made without the sharing and usage logs: Example 3's failure.

When to involve a digital forensic expert

At scoping, where the platforms and accounts: including the shadow-IT ones: are found from endpoints, network logs and expenses, not just interviews (Example 2); at collection, where the platform record and the desktop clients are gathered together and reconciled; at analysis, where sharing is distinguished from access and the deal-room log read for who reached what (Example 1); at assessment, where sanctioned collaboration is separated from leak (Example 3); and at deployment, under CPR Part 35 for disclosure, exfiltration and confidentiality proceedings. Through **e-discovery.uk**, file-platform collection runs the two-record method as standard: the platform proves what happened, and the client corroborates it where the account is denied, deleted or never admitted.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Do Dropbox, Box and ShareFile 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 whatever 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 endpoint 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 OneDrive 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.

§ 14 · REFERENCE

Glossary

Activity log
A platform's record of user events with timestamps and context.

Box Drive
Box's desktop client, leaving local sync artefacts.

Collaborator
A user granted standing access to a shared folder.

Deal room
A structured collaboration space with per-user access logging.

Enterprise tier
The subscription level with the richest logging and export.

Link usage log
The record of who followed a shared link, where the platform keeps it.

Local sync database
A desktop client's record of files mirrored to a machine.

Shadow IT
Platforms used outside the IT function's knowledge or control.

Shared link
A URL granting access to a file or folder, optionally secured.

Two-record method
Collecting platform log and desktop client together.

Sources and authoritative references

The file-platform 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 (file-platform mapping, admin and API collection, desktop-client corroboration as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- cflab.uk, digital forensics services (sync-client artefact analysis, sharing and access investigation, 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
- Dropbox Help, admin activity and content management: help.dropbox.com · Box, enterprise events and admin: support.box.com · ShareFile, activity logs and reporting: docs.sharefile.com
- PD 57AD: justice.gov.uk, PD 57AD · CPR Part 31 (r.31.17): justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

File-platform work at **e-discovery.uk** runs the two-record method across Dropbox, Box, ShareFile and their peers: the platforms and accounts found from endpoints, network logs and expenses rather than interviews alone (Example 2's shadow-IT Dropbox); the platform record collected by admin export and API with tier and retention established and beaten; the desktop-client databases imaged to corroborate the server side and survive a denied or deleted account; sharing distinguished from access and the deal-room log read for who reached what (Example 1); and the governance baseline checked before misuse is alleged (Example 3). Personal and uncontrolled accounts are reached by undertaking, order or provider process, never self-help. Reports run under CPR Part 35 for disclosure, exfiltration and confidentiality proceedings. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a matter touches a file-sharing platform, the first question is the one the data map forgot: what else do they share files through?

INSTRUCT THE LAB

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