COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Who Accessed or Downloaded a Confidential Document

Reading Access Trails Across Cloud Platforms, File Servers and Endpoints

A board paper reaches a journalist. A pricing model turns up at a competitor. A medical record is viewed by someone with no reason to see it. The question is always the same: who opened it, who downloaded it, when, and from where: and the answer lives in access logs that most organisations keep without knowing what they record, for retention periods measured in weeks, in formats that need interpretation before they prove anything. Cloud platforms log file access at the server; file servers log it if auditing was switched on; endpoints record what was opened locally; and none of them names a person: they name accounts, sessions and devices, which the investigation must join to a human being. This guide gives UK lawyers the method: where access evidence is recorded on each platform, what each record does and does not prove, the retention clocks that decide whether it survives, the attribution lattice from account to person, and the deployment of access findings in confidentiality, employment, data-protection and leak proceedings.

⏱ 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. Access investigations are a staple of its casework: leak inquiries, confidentiality breaches, unauthorised record viewing, and the employment and data-protection proceedings that follow: worked from platform audit logs, server audit trails and endpoint artefacts to a corroborated actor, and reported under CPR Part 35 where the access is the case.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACCESS-LOG ANALYSIS | LEAK & BREACH INVESTIGATION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01 Executive summary

02 The problem in plain English: access is logged, and logs are not names

03 Cloud platforms: what SharePoint, OneDrive, Google Drive and SaaS record

04 File servers, DMS and endpoints: the on-premises and local record

05 What each record proves: view, open, download, sync, print and share

06 Retention, licensing and the clocks that decide survival

07 From account to person: attribution and deployment

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

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: FILE ACCESS IS RECORDED AT THE PLATFORM, THE SERVER AND THE ENDPOINT, EACH NAMING AN ACCOUNT RATHER THAN A PERSON AND EACH ON ITS OWN RETENTION CLOCK: EXPORT THE LOGS FIRST, READ WHAT EACH EVENT ACTUALLY MEANS, THEN JOIN ACCOUNT TO PERSON WITH INDEPENDENT CORROBORATION

Where it is recorded (§3-§4): cloud platforms log file operations server-side: SharePoint and OneDrive through the Microsoft 365 unified audit log (accessed, downloaded, synced, shared, printed events with account, IP, client and timestamp), Google Drive through its audit and Vault reporting, SaaS applications through their own event logs of varying depth. On-premises file servers log access only where object-access auditing was enabled, in Windows security event logs with their own rotation; document-management systems keep access histories per document; endpoints record what was opened locally in artefacts (recent-file lists, shortcut files, application histories, browser downloads) that survive independently of any server. **What events mean (§5):** "accessed" is not "read"; a preview generates an access event; a sync client's download is not a human's; a share to a link is not a share to a person until the link is used: each event type's semantics are established before it is pleaded, per guide 87's field discipline. **The clocks (§6):** audit retention is licence-tiered (months by default, longer with premium licensing or export), server logs rotate on size, SaaS logs vary wildly: the export is the first act of any access inquiry because the evidence deletes itself on schedule. **Attribution (§7):** the log names an account and a session; sign-in records add device, IP and authentication context; endpoint artefacts corroborate the device; badge, calendar and physical evidence corroborate the person: the guide 96 lattice applied to a single click, with shared credentials, unlocked sessions and compromise addressed as the alternatives they are. The findings then serve confidentiality injunctions, employment proceedings, ICO breach assessments and leak inquiries, evidenced under CPR Part 35 where access is disputed.

- **Export before anything else:** the audit log's retention window is the investigation's first deadline.
- **Events have semantics:** preview, open, download, sync and share are different facts: pleaded as what they are.
- **Server auditing may be off:** on-premises access evidence exists only where it was configured: verified, not assumed.
- **Endpoints remember independently:** local artefacts prove what was opened on the device whatever the server logged.
- **Accounts are not people:** attribution is a corroboration exercise with alternatives addressed, or it is an assertion.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: access is logged, and logs are not names

Modern document platforms are surveillance systems by design: they log who touched what so that administrators can troubleshoot, security teams can detect intrusions, and compliance functions can answer regulators. The logs exist whether or not anyone reads them. When a confidential document leaks, the organisation discovers that it has been recording the answer for months: and that the recording is expiring on a schedule set by the licence tier, that the events need interpretation (a "FileAccessed" event fires for a thumbnail preview as readily as for a full read), and that the name in the log is an account, not a person.

The investigation therefore runs in three moves that this guide takes in turn: secure the logs before their windows close; read the events for what they actually prove; and join the account to a human being through independent evidence, because "the account opened the file" is where the argument about who did it begins, not where it ends. Each move is skippable in the panic after a leak, and each skip is discoverable by the person accused: the log that expired, the preview pleaded as a read, the shared login never examined. The discipline is the case.

§ 0 3 · THE CLOUD RECORD

Cloud platforms: what SharePoint, OneDrive, Google Drive and SaaS record

- **Microsoft 365 unified audit log:** SharePoint and OneDrive file events (accessed, downloaded, modified, synced, shared, printed, copied, moved, deleted, previewed) with the acting account, client IP, user agent, item path and timestamp: searchable through Purview audit tooling and exportable in bulk: the richest access record most organisations hold, subject to §6's tiering.
- **Google Workspace audit logs:** Drive audit events (view, download, edit, share, move, trash) with actor, IP and document identifiers, reachable through the admin console, reporting APIs and Vault: comparable coverage with its own event vocabulary and retention.
- **SaaS platforms:** CRM, HR, finance and collaboration systems log record and document access with widely varying depth: some per-view with full context, some only on export, some not at all below administrator level: each platform's logging established from its documentation and tested before it is relied on.
- **Sign-in and session records:** Entra and Google sign-in logs join the acting account to device, IP, location, authentication method and application: the second layer every attribution needs (guide 104 §6), exported alongside the file events.
- **Sharing and link artefacts:** sharing events (with whom, at what permission), anonymous and organisation-wide link creation, and link-usage records: the difference between a document shared with a person and a link that anyone could follow: guide 111-112's sharing forensics, applied to access.

§ 0 4 · THE ON-PREMISES AND LOCAL RECORD

File servers, DMS and endpoints: the on-premises and local record

- **Windows file servers:** object-access auditing, when enabled with a system access control list on the relevant folders, writes security event log entries recording account, object, access type and time: with the standing caveat that auditing is off by default, generates high volumes, and the logs rotate on size: an unconfigured server holds no access history at all.
- **NAS and other file storage:** vendor-specific audit features (some rich, some absent), often disabled for performance: established per device, with the honest finding "no access logging was configured" recorded when true.
- **Document-management systems:** iManage, NetDocuments and similar log per-document access histories (views, downloads, prints, exports) as a core function: the legal sector's best access record, exported per document or per user.
- **Endpoint artefacts:** the device that opened the file remembers: shortcut (LNK) files and jump lists naming opened documents with timestamps, recent-file registries, application most-recently-used lists, browser download histories, thumbnail caches and, for synced files, the sync client's local database: guides 97 §4 and 125's methods, proving local access independently of any server.
- **Print, screenshot and camera routes:** print-spooler and print-server logs, screenshot artefacts, and: bounded honestly: the phone camera that leaves no trace at all: the access routes enumerated with their evidential ceilings stated.

§ 0 5 · WHAT EACH EVENT PROVES

What each record proves: view, open, download, sync, print and share

- **Accessed and previewed:** a file-accessed event fires on opens, previews, thumbnail renders and some listings: it proves the account's session touched the item, not that a human read it: pleaded as "accessed", with the client and context (browser preview, full open, search result render) distinguishing the cases where the log allows.
- **Downloaded:** a download event proves a copy was delivered to the client: the stronger fact for leak inquiries: with the client type (browser, sync client, mobile app) determining whether a human chose it or a sync process did.
- **Synced:** sync-client events are automated: a file synced to a laptop was downloaded by the client because the folder was selected, not because a person opened the document: the distinction that separates guide 97's exfiltration from routine mirroring, made from event type and client fingerprint.
- **Shared and link-followed:** a share event proves a grant; a link-usage or anonymous-access event proves consumption; the two are joined to show who actually reached the document through the share: the "I shared it internally" defence tested against who followed the link and from where.
- **Printed, exported, copied:** the events that most closely approximate intent: printing to paper, exporting to another system, copying to another location: each with its own logging coverage, and each a stronger inference than a view.

§ 0 6 · THE CLOCKS

Retention, licensing and the clocks that decide survival

- **Licence-tiered retention:** Microsoft 365 audit retention is set by licence tier (a default measured in months, extended for premium tiers and by retention policies); Google's audit retention is similarly bounded; neither pauses for a dispute: the tenant's actual configuration is the first fact established.
- **Export as preservation:** the audit log is preserved by exporting it: to a SIEM, to a compliance store, or by the investigation's own bulk export at the earliest moment: the act that converts a rolling window into a held record, per guide 97 §3 and guide 99 §3.
- **Server logs rotate:** Windows security logs overwrite on reaching size limits, sometimes within days on busy servers: the on-premises access story survives only where log forwarding or archiving was configured, or where the investigation reached the server in time.
- **SaaS windows vary:** per platform and per subscription, from days to indefinite: enumerated in the data map (guide 3) so the investigation knows which clocks are already running.
- **The preservation duty reaches logs:** PD 57AD's duty and hold notices extend to audit and access records once proceedings are contemplated: a log allowed to expire after that date is guide 95 §6's subject.

§ 0 7 · FROM ACCOUNT TO PERSON

From account to person: attribution and deployment

- **The lattice:** access event (account, time, item) joined to sign-in record (device, IP, location, method), to endpoint artefact (the same document opened on that device at that time), to physical evidence (badge, calendar, CCTV, the person's own messages): guide 96's corroboration applied to one act, with each link's independence stated.
- **Alternatives addressed:** shared or borrowed credentials, an unlocked workstation, a compromised account (guide 104 §7), an administrator's impersonation, an automated process: each considered against the session evidence and either excluded or left open in the report: the attribution's honest ceiling.
- **Pattern and anomaly:** the account's own access baseline (role-consistent items, usual hours, usual device) against the disputed access: the out-of-role, out-of-hours, new-device access that stands out: with guide 97 Example 3's warning that baselines must be built before anomalies are pleaded.
- **Deployment:** confidentiality and springboard relief (guide 97 §7), employment proceedings (with guide 97 §5's process discipline), ICO breach assessment where personal data was accessed without authority (guide 99 §6's clocks), and leak inquiries where the access population narrows the candidates: the finding drafted to the audience.
- **The receiving side:** the person accused of access: the same lattice run defensively: was it a preview, a sync, a shared login, a role-consistent act: guide 97 Example 3's innocent-explanation pass, for access.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: an access question is answered from layers that record the same act differently and fail independently. The platform audit log records the server's view: account, item, event type, client, IP. The sign-in and session layer records the authentication context. The endpoint records the local view: the shortcut, the cache, the download folder, the sync database. The physical-world layer records presence. The document's own downstream traces (the copy at the competitor, the printout, the forwarded attachment) record the consequence and sometimes carry identifying artefacts (watermarks, metadata, print-tracking dots, the guide 87 fields naming the copy's origin). And the counterpart of every share (the recipient's platform, mailbox or device) records receipt. When the primary log is gone: retention expired, auditing never enabled, the platform silent below administrator level: the table names the alternates: the endpoint proves the open; the sync database proves the download; the recipient proves the share; the downstream copy's metadata proves the lineage.

QUESTION	PLATFORM AUDIT LOG	SIGN-IN / SESSION LAYER	ENDPOINT ARTEFACTS	PHYSICAL LAYER	DOWNSTREAM COPY + RECIPIENT	DELETED/ EXPIRED
Was it opened / previewed	Y: access events	Session brackets	Y: LNK, MRU, caches	n/a	n/a	Endpoint survives log expiry
Was it downloaded	Y: download events + client	Device context	Y: download folder, sync DB	n/a	The copy itself	Sync DB persists
Who (account)	Y: the acting account	Y: authenticated identity	User profile context	n/a	Share recipient	Permission bounds who could
Who (person)	n/a	Device + location	The device's owner	Y: badge, CCTV, calendar	n/a	n/a
Where did it go	Share + link events	n/a	Forward + upload artefacts	Print logs	Y: metadata + watermarks	Varies

Fallback strategy in one line: when the platform log has expired, the endpoint still remembers the open and the sync database the download: and the downstream copy's own metadata names the branch of the tree it fell from.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE BOARD PAPER AND THE FORTY-ONE ACCOUNTS

A confidential board paper reached the press within a day of circulation. The §3 export (run the same afternoon, inside the tenant's audit window) listed forty-one accounts with access events on the SharePoint item. The §5 reading narrowed it: twenty-nine were previews from the email notification's inline render; eight were full opens by directors and their assistants in role; three were sync-client downloads to laptops in the directors' standing sync folders; and one was a browser download at 22:47 by an assistant's account, from a sign-in on an unmanaged device at a residential IP with a new browser fingerprint. The endpoint layer could not reach the unmanaged device, but the downstream copy: the journalist's published extract: carried the platform's per-download watermark for that session. Attribution reached the account, the session and the watermark; the assistant's explanation at interview reached the rest. Forty-one accesses were one download.

EXAMPLE 2 · THE SERVER THAT WAS NEVER LISTENING

An engineering firm alleged a departed designer had accessed restricted project folders on the file server in his last week. The examiner's first finding was the honest one: object-access auditing had never been enabled on the server, so no server-side access record existed for any user, ever. The §8 alternates carried the case instead: the designer's laptop (sequestered per guide 97 §3) held LNK files and jump-list entries naming the restricted drawings with timestamps in his final three days, a sync-client database listing them among files mirrored to a personal cloud folder, and browser artefacts of the personal-cloud upload session; the VPN logs placed his session on the network at the times the LNK files recorded. The server's silence was stated in the report as a finding; the endpoint's memory did the work. The firm enabled auditing the following week.

EXAMPLE 3 · THE ACCESS THAT WAS A PREVIEW, AND THE DISCIPLINARY THAT WAS WITHDRAWN

A healthcare employer moved to dismiss a clinician for viewing a colleague's medical record without authority, on the strength of an "accessed" event in the records system's audit trail. The clinician's representative instructed an examiner. The system's event vocabulary, tested per §5, showed the "accessed" event fired on search-result rendering: the clinician had searched a common surname for a legitimate patient, the colleague's record had appeared in the results list with a summary panel, and no record-open event followed: the session moved to the correct patient eleven seconds later. The employer's own baseline data showed the pattern was routine across the department. The disciplinary was withdrawn; the employer's audit-event guidance was rewritten. An access event had been pleaded as a read; the semantics were the defence.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Export deferred:** the audit window closing while the leak was discussed internally: the evidence deleting itself on schedule.
- **Previews pleaded as reads:** Example 3's disciplinary: event semantics never tested.
- **Sync downloads read as choices:** the standing sync folder's mirror treated as deliberate exfiltration.
- **Server auditing assumed:** Example 2's silence discovered when the allegation was already made.
- **Account equated with person:** the lattice skipped; the shared-login defence left open.
- **Baselines unbuilt:** anomalies pleaded without the account's normal pattern: guide 97 Example 3's error.
- **Sharing links unexamined:** "shared internally" accepted without the link-usage events showing who followed it and from where.
- **Endpoints released:** the device that would have proved the open reissued before imaging: guide 97 §3's afternoon.

Technical limitations

- **Logging is configuration:** what was recorded depends on licence, settings and platform: the investigable story bounded by yesterday's choices, stated per source.
- **Events are approximations:** no log records comprehension; reading, understanding and intent are inferences from access, download and downstream use.
- **Some routes are silent:** a photograph of a screen leaves no platform trace: the ceiling stated, per this series' honesty rule.
- **Unmanaged devices are opaque:** personal devices and external networks limit endpoint corroboration: the session layer and downstream artefacts carry more weight, and the report says so.
- **Platform vocabularies change:** event names and semantics move with updates: verified against current documentation per matter, per the standing rule.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What is the audit retention on each platform holding the document, and has the log been exported yet?
- Was access auditing enabled on the relevant file servers and systems, and since when?
- Which accounts had permission to reach the document, through what shares and links, and where are the devices those accounts used?

Ask your opponent

- Please disclose the audit-log entries recording access to, download of, sharing of and printing of [document] during [period], identifying for each event the acting account, event type, client, IP address and timestamp, and confirm the audit retention configuration applicable.
- Please disclose the sign-in records for [accounts] during [period], including device, location and authentication method, and the permission and sharing history of [document].
- Please confirm preservation of the devices used by [individuals] during [period] and the state of any endpoint examination.

Ask your eDiscovery / forensic provider

- Have the platform, sign-in and server logs been exported inside their windows: and which have already expired?
- What does each event in the access list actually mean on this platform: preview, open, download, sync?
- How far does the attribution lattice reach for the disputed access, and which alternatives remain open?

SUGGESTED WORDING · ACCESS-RECORD PRESERVATION AND DISCLOSURE REQUEST

> "Our client's investigation concerns access to [document] during [period]. You are required immediately to preserve, and within [14] days to disclose: (1) all audit and access log entries on [platforms / servers / systems] relating to [document], including access, preview, download, sync, share, link-usage, print and export events, with acting account, event type, client, IP address and timestamp; (2) sign-in and session records for the accounts appearing in those entries; (3) the permission and sharing history of [document]; and (4) confirmation of the audit retention settings applicable to each source and the date on which each log was exported or otherwise preserved. Please also confirm that the devices used by [individuals] have been preserved unaltered pending examination. Our client reserves its position as to any access records allowed to expire after the date of this letter."

§ 12 · QUICK CONTROL

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

The access-investigation checklist

- ☐ Audit logs exported from every platform holding the document, same day
- ☐ Sign-in and session logs exported for the relevant accounts
- ☐ Server and DMS auditing status verified; logs secured where they exist
- ☐ Permission and sharing history of the document mapped, links included
- ☐ Event semantics tested per platform before any characterisation
- ☐ Sync-client activity separated from human downloads
- ☐ Devices sequestered for endpoint corroboration
- ☐ Baselines built for each account of interest
- ☐ Attribution lattice constructed; alternatives addressed in writing
- ☐ Downstream copy examined for watermarks and lineage metadata

Red flags

- Out-of-role, out-of-hours, new-device access to sensitive items: Example 1's 22:47.
- Anonymous or organisation-wide links on confidential documents.
- Audit retention at default tier on a sensitive-data tenant.
- Servers holding restricted material with auditing off: Example 2's silence.
- Allegations resting on single "accessed" events: Example 3's preview.
- Devices reissued before imaging.
- Opposing access allegations with no sign-in or endpoint corroboration.

When to involve a digital forensic expert

The day the question arises, because §6's clocks are already running: exports first, devices sequestered, servers checked for auditing; then through the reading, where event semantics are tested (Example 3's defence) and sync separated from choice; through attribution, where the lattice is built and alternatives closed or stated (Example 1's session); and at deployment, in confidentiality, employment, breach and leak proceedings under CPR Part 35, on either side. Through **cflab.uk** and **e-discovery.uk**, access investigations run from the same-day export to the corroborated actor: and the honest finding, including "the server was never listening", is the one that survives the hearing.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can we find out who opened a document on SharePoint?

Usually, within the audit retention window: the unified audit log records access, download, share and related events with the acting account, client and IP (§3): Example 1's forty-one accounts came from one search. The account is then joined to a person through §7's lattice, and the event type read for what it proves (§5): a preview is not a read.

How long do access logs last?

Months by default on the major platforms, longer with premium licensing or retention policies, days on busy on-premises servers, and anything from days to indefinite on SaaS systems (§6): the tenant's actual configuration is the first fact, and export is the first act. Logs allowed to expire after proceedings are contemplated are a preservation failure.

The file server has no access logs. Is the trail cold?

The server's trail never existed if auditing was off (Example 2), but the endpoint's did: shortcut files, recent-file lists, sync databases and browser artefacts on the device that opened the file prove local access independently (§4, §8). Sequester the device before it is reissued; the trail is on it.

The log says my client's account accessed the record. Is that the end of it?

No: the event's semantics may be a preview or a search render (Example 3), the download may be a sync client's, and the account may have been used by someone else: the defensive lattice of §7 tests each. Access allegations built on a single log line without semantics, baseline or corroboration are the ones that fail at the hearing.

Can access to a document be proved after it was deleted?

Access events are recorded independently of the item's survival, so the audit log holds the history of a deleted document for its retention period; endpoint artefacts likewise persist (§8). The document's content may need guide 95 or 102's recovery; its access history is a separate, often longer-lived record.

Someone photographed the screen. Can that be traced?

Not from the platform: a camera leaves no access event beyond the open itself. The investigation narrows the population to accounts that had the document displayed at the relevant time (§5's open events), joins sessions to devices and rooms (§7), and examines the downstream image for screen artefacts, reflections and the platform's on-screen watermarks where deployed: bounded honestly, and sometimes sufficient.

§ 14 · REFERENCE

Glossary

Access event
A platform log entry recording that a session touched an item.

Attribution lattice
The independent-source chain from account to person.

Audit retention
The licence- and policy-bound period a platform keeps its logs.

Baseline
An account's normal access pattern, against which anomalies are read.

Event semantics
What a specific event type proves on a specific platform.

Link-usage event
The record that a sharing link was followed, by whom, from where.

LNK / jump list
Windows artefacts recording documents opened on a device.

Object-access auditing
Windows server logging of file access, off by default.

Sync event
An automated client download, distinct from a human's.

Unified audit log
Microsoft 365's cross-service record of user and admin activity.

Sources and authoritative references

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

- cflab.uk, digital forensics services (access-log analysis, endpoint examination, attribution, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 07 · Analysis (log export, retention mapping and access analysis as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft Learn, audit log activities and retention: learn.microsoft.com, audit activities · learn.microsoft.com, audit retention · Google Workspace Admin Help, Drive audit log: support.google.com, Drive audit
- PD 57AD: justice.gov.uk, PD 57AD · CPR Part 25 (interim remedies): justice.gov.uk, Part 25 · CPR Part 35: justice.gov.uk, Part 35
- ICO, UK GDPR guidance and employment monitoring: ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Access work at the laboratory begins with the clocks: platform, sign-in and server logs exported the day of instruction, devices sequestered, auditing status established (Example 2's honest first finding); continues with the reading: event semantics tested per platform so previews, syncs and downloads are pleaded as what they are (Example 3's defence); and closes with the lattice: account to session to device to person, alternatives addressed, baselines built, downstream copies examined for the watermark that ends the argument (Example 1's session). Reports serve confidentiality, employment, breach and leak proceedings under CPR Part 35, on whichever side the evidence favours. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a leak surfaced this week, the audit log is on its retention clock now: export today, argue later.

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