COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Investigating Suspected Employee Data Theft

From First Suspicion to Springboard Relief: The Forensic Investigation Done Right

The pattern is depressingly standard: a rainmaker resigns, clients follow, and someone remembers the late-night office visit or the personal Dropbox. What happens next decides everything: investigated properly, employee data theft leaves one of the richest evidence trails in digital forensics: exfiltration artefacts across USB records, cloud sync logs, personal email and printing trails, choreographed against the resignation per guide 96's timelines: investigated badly, the evidence is contaminated by the IT department's well-meant look-around, the employee is tipped off mid-copy, or the employer's own snooping breaches UK GDPR and poisons the claim. This guide gives UK lawyers and employers the investigation playbook: trigger discipline, lawful evidence gathering, the exfiltration-artefact map, attribution and quantification, interaction with employment process, and the fast route to undertakings, delivery-up and springboard relief.

⏱ Estimated reading time: 25 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. Employee-exit investigations are core laboratory work: leaver devices imaged, exfiltration artefacts read across USB, cloud, email and print layers, timelines built for injunction evidence, and the receiving side served too: examining what arrived at the new employer, and the defence work where the artefacts tell an innocent story. Reports run under CPR Part 35 at injunction speed.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | EXIT & EXFILTRATION INVESTIGATIONS | INJUNCTION-SPEED REPORTING | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: PRESERVE FIRST, INVESTIGATE LAWFULLY, BUILD THE CHOREOGRAPHY, AND MOVE FAST: DATA-THEFT CASES ARE WON BY THE QUALITY OF THE FIRST FORTNIGHT'S FORENSICS AND LOST BY THE IT DEPARTMENT'S FIRST AFTERNOON

First response (§3): on trigger (resignation plus anomaly, client-follow patterns, a tip-off), the leaver's estate is preserved before anyone investigates: devices sequestered unpowered, accounts held not purged, platform audit logs exported before rolling retention eats them, and: critically: nobody logs into the suspect's profile "for a look": the amateur hour that overwrites the very artefacts the case needs. **The artefact map (§4):** exfiltration writes across layers: USB registry records and LNK files naming what was opened from removable media; cloud sync clients and personal-account uploads in browser and platform logs (guides 51-58, 111-112); personal-email forwarding with attachments; mass downloads and report exports in audit trails (guide 105); printing and screenshots; and the anti-forensic cleanup attempts (guide 110) that are themselves evidence. **Lawful process (§5):** the investigation runs inside UK GDPR and monitoring rules: proportionate scope, documented purpose, employment procedure respected: because unlawfully obtained evidence and procedural unfairness both hand the defence its best points. **Deployment (§7):** the assembled case: guide 96's choreography timeline joining exfiltration to resignation: supports the escalation ladder: preservation letters and undertakings, delivery-up and imaging orders, springboard and confidential-information injunctions, with the new employer's estate reachable through the same machinery. Speed is structural: springboard relief protects a head start only while the head start exists.

- **Preserve before investigating:** the leaver estate frozen intact: §3's containment before anyone's curiosity.
- **The trail is multi-layer:** USB, cloud, email, print, audit logs: §4's map read together, not source by source.
- **Lawfulness is case-critical:** UK GDPR-compliant, proportionate, documented investigation: §5's frame protecting the evidence's admissibility and the employer's flank.
- **Choreography convicts:** exfiltration timed against resignation and joining dates: guide 96's build as the persuasive core.
- **Speed decides remedies:** springboard clocks run from the theft: the fortnight's forensics feeding the injunction, not the trial two years out.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: exits leave trails, and panic destroys them

Copying an employer's data is noisy. Modern estates log access, movement and egress at multiple independent layers: the platform records the download, the endpoint records the USB device, the browser records the personal-cloud upload, the mail system records the forward, the badge system records the late visit. An exiting employee harvesting the client book or the design archive writes a story across all of them, usually in a compressed period with a legible rhythm: guide 96 Example 2's choreography is the genre's standard plot.

The trail's enemy is rarely the thief's sophistication; it is the employer's response. IT logs into the account and overwrites last-access artefacts; the laptop is reissued to a new joiner and the unallocated space overwritten; the account is deleted in the leaver process and the audit trail's subject vanishes; a manager confronts the employee mid-harvest and the personal cloud is emptied before any preservation order exists. Every one of those is standard practice somewhere: which is why §3's containment discipline is the guide's first substantive section, and why the difference between a strong claim and a shrug is usually decided before any lawyer is instructed.

§ 0 3 · THE FIRST RESPONSE

First response: triggers, containment and what not to touch

- **Trigger discipline:** resignation plus anomaly (odd hours, mass activity, client contact spikes), competitor-move intelligence, client-follow patterns, or a colleague's report: logged, assessed quickly, and escalated to a defined owner: the playbook that exists before the exit does.
- **Freeze the estate:** devices collected and held unpowered (no IT inspection, no reissue); accounts suspended-and-preserved rather than deleted: mailbox, OneDrive/Drive, chat, CRM: with litigation-hold mechanisms engaged (guides 51-58's machinery); building access and further egress closed.
- **Export the perishables:** platform audit logs (guide 105's windows), sign-in records, DLP alerts and proxy logs pulled immediately: the server-side story has rolling retention and the clock started before the suspicion did.
- **Touch nothing as the user:** no logging into the leaver's profile, no opening their files, no "quick look" at the browser history: every such act overwrites timestamps and seeds the defence's contamination argument: examination happens on images, by examiners.
- **Decide the confrontation timing with advice:** early confrontation risks destruction at the personal end (§8's counterpart problem); silence risks ongoing harm: the call made deliberately, with preservation letters ready for the moment it is made.

§ 0 4 · THE TRAIL

The exfiltration-artefact map: USB, cloud, email, print and beyond

- **Removable media:** registry device records (identities, serials, first/last connection), LNK files and shellbags showing what was opened from the stick, and volume-level copy artefacts: the classic route, still the commonest, read from the endpoint image.
- **Cloud egress:** personal sync clients installed on work machines (their local databases listing every mirrored file), browser artefacts of personal-account uploads, sharing events to external addresses in platform logs (guides 51-58, 111-112): the modern default route.
- **Email egress:** forwards to personal accounts with attachment manifests, auto-forwarding rules (guide 104's territory), and drafts-folder staging: the mail system's own records naming every item that left.
- **Volume and access anomalies:** mass downloads, report exports and repository crawls in audit trails (guide 105): the harvest visible as a statistical event against the user's own baseline: guide 95 §3's negative-space logic, inverted.
- **The peripheral routes and the cleanup:** printing trails, screenshots and phone-camera captures (bounded honestly: some routes leave little), plus the anti-forensic tail: deletion sprees, wiping tools, history clearing (guide 110): which rarely removes the multi-layer story and always darkens it.

§ 0 5 · INSIDE THE LAW

Lawful investigation: UK GDPR, monitoring rules and employment process

- **UK GDPR frames the search:** investigating employee data is processing: purpose defined and documented, scope proportionate to the suspicion (the leaver's work estate, not their life), special-category caution, and a DPIA-style record where monitoring is significant: the ICO's employment-practices expectations followed, not improvised.
- **Private material handled with care:** personal emails and files encountered on work systems filtered by protocol (search terms, examiner-only review of borderline material): relevance extracted, privacy respected, the methodology documented for the challenge that may come.
- **Covert monitoring is exceptional:** justified, necessary, time-limited and documented where used at all: the default is examination of existing records and preserved estates, which the artefact map almost always makes sufficient.
- **Employment process runs in parallel:** suspension, investigation and disciplinary fairness (Acas-consistent) alongside the forensic track: the unfair-dismissal counterclaim is the standard riposte, and procedural discipline defuses it.
- **Privilege and the investigation file:** the investigation structured with litigation in contemplation where the facts support it (guide 91's dominant-purpose lessons): instruction letters, reporting lines and the purpose file built for the privilege claim, on day one, not at disclosure.

§ 0 6 · THE CASE ASSEMBLED

Attribution, quantification and the choreography timeline

- **Attribution built, not assumed:** account activity joined to the person: badge and CCTV brackets, device possession, sign-in device fingerprints, the guide 105-107 disciplines: the "someone else used my login" defence answered before it is raised.
- **Quantification by manifest:** what exactly left: file lists from sync databases, attachment manifests, export logs, USB-opened items: the schedule that turns "he took data" into "these 4,117 files, listed": the injunction's Schedule 1 and the damages expert's input.
- **Sensitivity mapped:** the taken set classified: trade secrets, client data (with its own UK GDPR breach questions for the employer), commercially sensitive material: driving both remedy scope and notification obligations.
- **The choreography:** guide 96's build applied: harvest events against resignation drafting, garden-leave dates, new-employer contact and joining: the sequence that supplies intention and answers innocence: Example 2 of guide 96 is this section's method in action.
- **The innocent-explanation pass:** the artefacts tested against the defence's best case (routine home-working copies, sanctioned devices, role-consistent access): run by the examiner before the employer pleads, because the version that survives that pass is the version worth swearing.

§ 0 7 · INTO COURT

Legal deployment: undertakings, delivery-up and springboard relief

- **The preservation-and-undertakings letter:** first contact done properly: preservation demanded across personal devices, accounts and media; undertakings sought (non-use, non-disclosure, delivery-up, imaging consent); the evidence hinted sufficiently to be taken seriously: many cases end here, at letter costs.
- **Delivery-up and imaging orders:** where letters fail: orders for devices and accounts to be imaged and examined (independent-examiner structures per guide 71 §7 where proportionate), with the §6 manifest defining scope.
- **Springboard and confidential-information injunctions:** restraining use of the taken material and the unfair head start it confers: duration argued from the advantage's real life: with the choreography timeline as the persuasive core and speed as the price of admission.
- **The new employer in frame:** knowledge and receipt investigated (what arrived, who knew): joined where the evidence supports it, engaged early by letter where tactics favour it: their own preservation obligations triggered the day they learn.
- **Parallel tracks kept aligned:** employment claims, database-right and confidence claims, regulatory notifications (the employer's own breach clock where client personal data left), and: rarely but sometimes: criminal complaints: sequenced with advice so no track poisons another.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: an exit investigation reads one story across independent layers, and its gaps are covered by the map. The employer-side sources: endpoint images (USB records, LNK files, sync databases, browser artefacts), platform audit logs (downloads, shares, sign-ins per guides 51-58 and 105), mail-system records (forwards, rules, attachments), network and proxy logs, and the physical layer (badges, CCTV, printer logs): each with its own clock and tamper profile, joined by guide 96's frame. The counterpart sources: the employee's personal devices, accounts and media, and the new employer's estate: reachable through undertakings and orders (§7), and holding the received half of every transfer the employer-side artefacts show leaving. When one layer is compromised: the laptop reissued, the logs expired, the account purged by leaver process: the §8 table names the surviving routes: the transfer that vanished from the endpoint persists in the platform log; the purged account's story survives in the audit trail exported in time; the emptied personal cloud is answered by the sync database's local manifest. Redundancy is the investigator's insurance; the map is where it is written down.

EVIDENCE	ENDPOINT IMAGE	PLATFORM AUDIT LOGS	MAIL-SYSTEM RECORDS	NETWORK / PROXY	PHYSICAL LAYER	COUNTERPART ESTATES (§7 ROUTES)
What was taken	Y: sync DBs, LNK, copies	Y: download/ export lists	Attachment manifests	Transfer sizes	Print logs	Y: the received copies
How it left	Y: USB + upload artefacts	Sharing + egress events	Forwards + rules	Y: destinations	n/a	Arrival artefacts
When (the choreography)	Y: timestamps	Y: server clocks	Y	Y	Y: badges + CCTV	Receipt dates
Who (attribution)	User-context artefacts	Account + device + IP	Account	Source machine	Y: the person's body	Possession
Cleanup attempts	Y: guide 110 artefacts	Deletion events	Purged-items records	n/a	n/a	Personal-side deletions

Fallback strategy in one line: exfiltration writes to at least three layers; preserve them all in week one, and when one is lost, prove the transfer from the survivors: then reach the received copies through §7's machinery.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE SUNDAY HARVEST AND THE MONDAY RESIGNATION

A recruitment firm's billings director resigned on a Monday; by Wednesday two colleagues reported client calls mentioning his new venture. The §3 freeze ran that day: laptop sequestered, account held, audit logs exported. The examination assembled the §4 map: CRM report exports covering his entire desk (audit log, Sunday 19:12-20:31), a personal-cloud sync client whose local database listed 3,900 mirrored files, badge entry 18:58 and exit 20:47, and browser artefacts of a new-company domain purchase the previous month. The choreography timeline: harvest, resignation draft (20:52 Sunday), Monday delivery: anchored the preservation letter; undertakings were refused; the delivery-up and springboard application succeeded on the timeline and manifest, with his personal cloud imaged by an agreed independent examiner. The client book came back before it could be worked; the venture launched without it.

EXAMPLE 2 · THE LOOK-AROUND THAT NEARLY LOST THE CASE

An engineering firm suspected a departed designer had taken CAD libraries. Before instructing anyone, IT logged into his profile, opened the project folders "to check what was there", ran a search across his mailbox, and reimaged the laptop for a new starter: standard hygiene, catastrophic forensics: last-access artefacts overwritten, the unallocated space gone, the defence's contamination argument written for them. The case was rescued by §8's redundancy: the platform audit logs (exported, luckily, within their window) still showed the pre-departure mass downloads; the personal-email gateway logs held the forward manifests; and the USB story survived in registry hives the reimage had not touched in a preserved backup. The claim succeeded, narrower and costlier than it should have been: and the firm's leaver process gained a forensic-hold step. §3 exists because Example 2 is the default without it.

EXAMPLE 3 · THE ARTEFACTS THAT TOLD AN INNOCENT STORY

A departing consultant faced a delivery-up application built on USB records and a large pre-exit download. The §6 innocent-explanation pass: run this time by the respondent's examiner: reframed every artefact: the USB device was the firm-issued encrypted drive on the asset register, its connection history matching years of sanctioned home-working; the "mass download" was the standard project-archive export required by the firm's own engagement-closure procedure, mirrored by colleagues' accounts on comparable exits; and the personal-cloud allegation dissolved when the sync database showed only family photographs. The application was dismissed with costs on the cross-examined evidence. The example is the §6 discipline's other face: artefacts acquire meaning from baselines and procedure, and the party that tests the innocent version first: whichever side they are on: is the party the hearing believes.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The IT look-around:** Example 2's afternoon: artefacts overwritten by curiosity before preservation.
- **Leaver-process destruction:** accounts purged and laptops reissued on schedule while suspicion was already live.
- **Audit logs left to expire:** the server-side story lost to rolling retention during internal deliberation: §3's export skipped.
- **Confrontation before preservation:** the personal cloud emptied the evening of the meeting: the §3 timing call never made.
- **Disproportionate snooping:** the investigation trawling private life beyond the purpose: §5's UK GDPR frame breached, the counterclaim gifted.
- **Attribution assumed:** the account equated with the person without §6's joins: the shared-login defence left open.
- **Quantification by adjective:** "substantial confidential information" pleaded where a manifest was extractable: remedies argued without Schedule 1.
- **Slow escalation:** springboard relief sought after the head start matured: the remedy's own logic defeated by the timetable.

Technical limitations

- **Some routes are quiet:** phone-camera capture and reading-and-remembering leave little: scope claimed to what the artefacts support, per the standing honesty rule.
- **Personal estates need process:** the received half sits behind §7's machinery: reachable, but on legal timelines the strategy must price in.
- **Baselines decide meaning:** Example 3's lesson: without role-and-procedure baselines, artefacts over-accuse and under-accuse freely: examiners build the baseline first.
- **Encrypted personal media:** lawful-access questions on private devices and accounts are real (guide 117's territory): planned with advice, not assumed away.
- **Logs vary by licence:** audit depth differs by platform tier (guide 105's caveat): the investigable story is bounded by what the employer's stack recorded.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What has already been touched: logins, device reissue, account deletion: so contamination is known before it is discovered?
- What do the leaver and home-working procedures actually sanction: the Example 3 baseline, established before pleading?
- What did the taken material contain: and does client personal data in it start the employer's own notification clocks?

Ask your opponent (the former employee / new employer)

- Please confirm preservation of all personal devices, accounts, cloud storage and media containing or having contained our client's data, and provide undertakings in the enclosed form as to non-use, non-disclosure and delivery-up pending resolution.
- Please identify all copies made of our client's data, the devices and accounts to which they were transferred, and all persons to whom any part has been disclosed, including at [the new employer].
- (To the new employer:) Please confirm what material originating from our client has been received into your systems, the steps taken to quarantine it, and your preservation of all relevant records pending investigation.

Ask your eDiscovery / forensic provider

- Which §8 layers are preserved and which are already compromised: and what does redundancy still prove?
- Does the manifest support Schedule 1 as drafted: file-level, with sensitivity classes?
- Has the innocent-explanation pass run: and what survived it?

SUGGESTED WORDING · PRESERVATION AND UNDERTAKINGS PARAGRAPH (FIRST LETTER)

> "Our client's forensic examination of its systems evidences the transfer of confidential material to devices and accounts under your control, including [category summary], in the period [dates]. You are required immediately to: (1) preserve, without deletion, alteration or use, all devices, accounts, cloud storage and media containing or having contained such material, including [identified items]; (2) provide within [7] days the enclosed undertakings as to non-use, non-disclosure, preservation and delivery-up; and (3) identify all copies made and all persons to whom any material has been disclosed. Compliance will be verified by forensic examination on terms to be agreed, by an independent examiner if preferred. In default, our client will apply without further notice for delivery-up, imaging and injunctive relief, including springboard relief, and will rely on this letter on costs."

§ 12 · QUICK CONTROL

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

The exit-investigation checklist

- ☐ Trigger logged; owner assigned; playbook opened
- ☐ Devices sequestered unpowered; no profile logins; no reissue
- ☐ Accounts held under litigation hold, not deleted
- ☐ Audit logs, sign-ins and DLP alerts exported same week
- ☐ Investigation purpose and scope documented per UK GDPR
- ☐ Privilege structure set at instruction (§5's purpose file)
- ☐ Artefact map read across all §4 layers together
- ☐ Attribution joined; manifest built; sensitivity classified
- ☐ Innocent-explanation pass run before pleading
- ☐ Escalation ladder timed to the springboard clock

Red flags

- Mass activity in the resignation fortnight: Example 1's Sunday.
- Personal sync clients on work endpoints.
- Auto-forwarding rules to personal addresses.
- Wiping tools or history-clearing dated to the exit: guide 110's tail.
- IT "checks" already run on the leaver estate: Example 2's contamination.
- Leaver processes deleting accounts on schedule despite live suspicion.
- Client-follow patterns preceding any lawful solicitation window.

When to involve a digital forensic expert

At the trigger, before anyone touches the estate: containment advice is a same-day call and Example 2's afternoon is the alternative; through the examination, where the §4 map, §6 attribution and manifest, and the choreography timeline are built to injunction standard; at deployment, where the evidence supports letters, orders and springboard applications under CPR Part 35 at hearing speed; and on the other side, where respondents' examiners run Example 3's innocent-explanation defence. Through **cflab.uk** and **e-discovery.uk**, exit investigations run from same-week preservation to injunction evidence as one engagement: and the first week is the one that cannot be rerun.

§ 13 · COMMON QUESTIONS

Frequently asked questions

We suspect a departing employee right now. What are the first three actions?

Sequester their devices unpowered, place their accounts on hold rather than deletion, and export the platform audit logs: §3's freeze, all achievable today: then instruct before anyone investigates by hand. The order matters because every layer has a clock: retention on the logs, reissue on the devices, and curiosity on the rest.

Can we search a leaver's work email and files without their consent?

Generally yes for work systems under a lawful, proportionate, documented investigation: §5's UK GDPR frame: with private material encountered on those systems handled by filtering protocol rather than free browsing. What loses cases is not examining work systems; it is disproportionate trawling and undocumented purpose: the frame is the protection.

The employee used their personal Dropbox and phone. Can we get at those?

Through process: undertakings sought by letter, then delivery-up and imaging orders, commonly via an independent examiner who reports on relevant material only (§7): the personal estate is reachable, on legal timelines, and the employer-side artefacts (sync databases, upload logs) usually prove the transfer without it. Plan the route early; do not self-help into private accounts.

What is springboard relief and why the urgency?

An injunction neutralising the unfair head start taken material confers: restraining its use (and sometimes competitive activity) for the period the advantage would last: which is precisely why it dies of delay: courts protect head starts still capable of neutralisation. The forensic fortnight feeds the application; a forensic quarter feeds a damages claim instead.

Our IT team already went through the laptop. Is the case dead?

Damaged, not dead: Example 2's rescue is the standard pattern: the platform, mail, network and physical layers (§8) carry their own copies of the story, and preserved backups often hold what the endpoint lost: an examiner maps what survives and states the contamination honestly. But stop further handling now: each additional touch narrows the rescue.

What if the artefacts have an innocent explanation?

Then finding it early is the win, whichever side you are: Example 3's dismissed application was expensive for the employer who never ran the §6 pass, and vindicating for the respondent who did: baselines (sanctioned devices, closure procedures, role-consistent access) decide what artefacts mean. The examiner's job is the supportable story; the advocate's job starts after.

§ 14 · REFERENCE

Glossary

Choreography timeline
Exfiltration events sequenced against resignation and joining.

Delivery-up
The order returning devices, accounts and copies for examination.

Exfiltration artefacts
The multi-layer traces of data leaving the estate.

Innocent-explanation pass
Testing artefacts against the defence's best case first.

Leaver hold
Suspension-with-preservation replacing deletion in exit processes.

LNK files
Windows shortcuts recording files opened, including from USB media.

Manifest
The file-level schedule of exactly what left.

Springboard relief
Injunction neutralising the head start taken material confers.

Sync database
A cloud client's local record of every mirrored file.

Undertakings
Binding promises (non-use, preservation, delivery-up) sought pre-order.

Sources and authoritative references

The exit-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 (exit investigations, exfiltration analysis, injunction-speed CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Identification and Phase 03 · Preservation (leaver holds, log export and the preservation file as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/preservation
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- ICO, employment practices and monitoring-at-work guidance, and UK GDPR resources: ico.org.uk
- PD 57AD (preservation duties): justice.gov.uk, PD 57AD · CPR Part 25 (interim remedies, including delivery-up and injunctions): justice.gov.uk, Part 25
- CPR Part 35: justice.gov.uk, Part 35 · Acas, disciplinary and investigation guidance: acas.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Exit investigations at the laboratory run the §1 sequence at the speed the remedies demand: same-day containment advice (the call that prevents Example 2), same-week preservation and log export, the §4 artefact map read across layers, attribution and the file-level manifest built to Schedule 1 standard, the choreography timeline constructed per guide 96, and the innocent-explanation pass run before anything is sworn: with CPR Part 35 reports produced on injunction timetables and independent-examiner structures offered where personal estates are imaged. The same machinery serves respondents and new employers: Example 3's defence was laboratory work too. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if the resignation landed this week, the audit logs are already ageing: preservation is today's task, the letter is this week's, and the springboard clock is not waiting for either.

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