



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Preserving Social Media Evidence Before It Changes

Posts, Profiles, Stories and Deletions: Capturing a Medium Built to Move

Social media evidence has a property no other class shares: it changes while you watch it. Posts are edited and deleted, profiles renamed, accounts locked or vanished, stories expire by design, and the platform interface between your screenshot and the server rewrites itself weekly. Yet Facebook, Instagram, X, LinkedIn, TikTok and their kin now carry evidence central to defamation, harassment, employment, family and commercial matters: what someone said, when, to what audience, and what they did about it once litigation loomed. This guide is the preservation manual: capture methods ranked by evidential weight, platform self-download archives and their contents, the account-holder versus public-view routes, what platforms retain and disclose under legal process, authentication of a medium notorious for fakes, and the race discipline that treats every relevant post as already scheduled for deletion.

🕒 Estimated reading time: 27 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. Social media preservation and authentication run through its defamation, harassment, employment and family casework: forensic capture with metadata and hash sealing, platform-archive analysis, deleted-content investigation across device and counterpart layers, and the fabrication workups that have retired manufactured posts. Its eDiscovery arm, **e-discovery.uk**, brings captured social content into disclosure-ready review.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

SOCIAL MEDIA CAPTURE & AUTHENTICATION

DELETED-CONTENT INVESTIGATION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: evidence with a half-life
- 03 The capture ladder: methods ranked by evidential weight
- 04 Platform self-download archives: the account-holder route
- 05 The public-view route: capturing what the world could see
- 06 Platforms, process and what providers hold
- 07 Authentication: proving the post was real
- 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

Executive summary

THE HEADLINE POINT: TREAT EVERY RELEVANT POST AS SCHEDULED FOR DELETION, AND CAPTURE AT THE HIGHEST EVIDENTIAL RUNG AVAILABLE TODAY

Social media evidence obeys a **capture ladder**: at the bottom, the bare screenshot: trivially fabricated, metadata-free, the weakest exhibit in modern practice (guide 63 §7's disease at its origin); above it, **forensically documented capture**: full-page acquisition with URLs, timestamps, HTTP context and hash sealing, performed by a method and operator who can give evidence; above that, **platform self-download archives**: the account holder's own data export (available on every major platform) containing posts, messages, media and account records in structured form with platform-generated metadata; and at the top, **platform records under legal process**: provider-held data with IP logs and account history: powerful, slow, jurisdiction-dependent, and for content classes often narrower than expected. The strategy is layered, not sequential: capture the public view today (it may be gone tonight), obtain the archive where any relevant account is friendly or compellable, and reserve provider process for what only providers hold: because **the medium's defining property is change**: edits, deletions, expiring stories, renamed handles, locked accounts: and every change is both a threat to evidence and, where it postdates the duty to preserve, evidence itself: the delete-after-letter pattern is social media's contribution to the conduct chronology this series builds everywhere. Two disciplines complete the method: **preservation letters that name accounts and forbid the predictable moves** (deletion, edits, privacy-setting changes, handle changes, account deletion: all standard panic responses), and **authentication built for a fabrication-rich medium**: capture pedigree, platform-archive corroboration, device-side artefacts on the poster's own equipment, and counterpart captures: because the question "is this post real" is now asked routinely, and the answer must be better than "it looks real".

- **Capture today, argue later**: the public view is preserved the day the matter opens: expiry, deletion and edits do not wait for proportionality debates.
- **The ladder decides weight**: screenshots start fights; documented captures with hashes and archive corroboration end them.
- **Self-download archives are underused gold**: structured, metadata-rich, obtainable from clients immediately and opponents by order.
- **Provider process is the top rung with caveats**: jurisdiction, speed and content-retention limits mean it supplements captures rather than replacing them.
- **Post-duty changes are conduct**: deletions, edits and privacy flips after notice join the chronology: captured-before and captured-after pairs prove them.

The problem in plain English: evidence with a half-life

A contract does not rewrite itself overnight; a server log does not delete its own worst lines. Social media does both, constantly, lawfully, at the author's whim: the medium hands every potential defendant a delete button and every potential claimant a deadline. Stories expire in twenty-four hours by design; posts are edited without always flagging it; accounts go private, get renamed, or disappear: and the platform owes your case nothing. The evidential consequence: in this class alone, the preservation step is frequently the whole case: what was captured before the change is evidence; what was not is a witness-statement argument about what a vanished post used to say.

The discipline follows: social media preservation is a day-one, same-day activity run in parallel with everything else: not a disclosure-stage task. The client interview asks for accounts and posts immediately; the capture happens that afternoon at the best rung available; the preservation letter names the accounts before the panic deletions start; and the archive requests go out while cooperation or compulsion can still reach an intact account. Everything else in this guide refines that reflex.

§ 0 3 · THE LADDER

The capture ladder: methods ranked by evidential weight

RUNG	METHOD · WEIGHT · WHEN
4 · Provider records	Platform-held data under legal process: account records, IP and access logs, and content classes per platform policy: the only source for registration and access data; slow, jurisdiction-bound, content retention narrower than assumed (§6). Supplements, never substitutes.
3 · Self-download archive	The account's own structured export: posts, messages, media, metadata, account history: platform-generated, internally consistent, obtainable from clients same-day and from opponents by order (§4). The corroboration backbone.
2 · Forensic capture	Documented acquisition of the live view: full pages, URLs, timestamps, request context, hashes, operator log: repeatable methodology, statement-ready (§5). The day-one workhorse.
1 · Screenshot	A picture of a screen: no metadata, no pedigree, fabrication-trivial: better than nothing at the moment of discovery, and immediately superseded by rung 2. Never the final exhibit where anything better was available.

The working rule: capture at rung 2 the day the content is identified; pursue rung 3 for every account within reach; add rung 4 where provider-only data (attribution, access) matters. Rung 1 is what clients bring you: received gratefully, replaced promptly.

Platform self-download archives: the account-holder route

- **Every major platform provides one:** Facebook/Instagram (Meta's download tools), X's archive, LinkedIn's data export, TikTok's download, Snapchat's My Data: structured exports of posts, messages, media, connections and account events: requested from settings, delivered in hours to days.
- **Contents exceed the visible:** archives carry platform metadata (timestamps, identifiers), message threads, deleted-content classes in some cases, login and device histories, and advertising/interest data: often more than the profile ever displayed.
- **Client accounts: same-day work:** the archive request is part of matter-opening for any client whose accounts touch the issues: it preserves against later account loss, and its login-history component regularly matters (whose device posted?).
- **Opponent accounts: the ordered route:** archives are within a party's control for disclosure purposes: specific disclosure of a self-download is now a routine, proportionate order in harassment, defamation and employment matters: sought early, before account deletion makes it academic.
- **Handled forensically:** archives are received, hashed and processed like any collection: their internal structure is the authentication asset, and its integrity is preserved by not letting clients unzip, edit and re-save before handover.

The public-view route: capturing what the world could see

- **Documented capture method:** the acquisition records what was requested (URL, time), what returned (content, headers where captured), and what was sealed (hashes, operator, tooling): the difference between an exhibit and an anecdote.
- **Scope with audience in mind:** the post, its comments and reactions, the profile context, follower-visible state: because audience and reach are elements (defamation's serious harm, harassment's course of conduct), the capture preserves what a reader saw, not just what the author wrote.
- **Dynamic content needs technique:** infinite scroll, expandable threads, stories, video: captured with methods that handle the medium (scrolling captures, video acquisition, story capture inside the expiry window), not a print-to-PDF that truncates at the fold.
- **Repeat captures date changes:** the before-and-after pair: same URL, two dates: is how edits, deletions and privacy flips are proved: recapture on a schedule while the dispute is live, and always after the preservation letter lands.
- **Third-party echoes:** web archives, search caches, reposts and quote-posts: secondary captures of vanished content: located, captured themselves, and weighed honestly (they prove the echo; the original's authentication runs through §7).

Platforms, process and what providers hold

- **Account and access data:** registration details, linked emails and numbers, IP and login logs: the attribution layer only providers hold: reached by court order or platform legal-request channels, with non-UK entities adding service and jurisdiction steps (Norwich Pharmacal and its successors for anonymous-poster cases).
- **Content retention varies and shrinks:** deleted content persists provider-side for limited, platform-specific windows (and policy changes faster than guides): the request goes early or the window answers it.
- **Preservation requests:** most platforms accept law-enforcement and, variably, civil preservation requests freezing account data pending process: the holding move made the week the matter opens where provider data may matter.
- **Anonymous and pseudonymous accounts:** the unmasking sequence: capture content now, preserve provider-side now, then the disclosure application against the platform for account data: with the realistic advice that VPNs and burner registration can bound what unmasking achieves.
- **Expectations managed in writing:** provider process is the slowest rung and the least controllable: cases are built on captures and archives, with provider data as the attribution supplement: the advice letter says so before the client asks why the platform has not simply handed everything over.

Authentication: proving the post was real

- **Pedigree first:** the capture's own documentation: method, time, operator, hashes: is the first authentication layer: rung 2 exists precisely so this layer exists.
- **Archive corroboration:** the same post inside a platform self-download, with platform metadata and structural context: rung 3 confirming rung 2: the pairing that ends most challenges.
- **Device-side artefacts:** the poster's own devices carry app databases, caches, drafts and notification traces (guides 61, 125): posting activity provable from the posting end: decisive where the author denies authorship.
- **Counterpart and echo capture:** recipients, followers and quote-posters hold their own views: independent captures converging on content and timing: the multi-source standard of guides 63-65, social edition.
- **Fabrication signatures:** rendering inconsistencies, impossible interface states, metadata absence, no archive or device trace, no echo anywhere: the workup that has unmade manufactured posts: run whenever a screenshot arrives unaccompanied and the stakes justify it.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the profile page is one surface of a wider estate. Social media evidence also lives in: the poster's devices (app databases, caches, drafts, media); the account's self-download archive; other participants' views (recipients of messages, members of groups, followers who captured); the echo layer (reposts, quote-posts, web archives, search caches); linked accounts and cross-posting services (the Instagram post that auto-shared to Facebook); notification residue on recipients' devices; provider-held records behind legal process; and the surrounding estate: emails and chats discussing the posts, which date knowledge and intent. When the account is deleted or hostile, the map is the case: device, archive-if-obtained, echoes, counterparts and providers, in that practical order.

EVIDENCE	LIVE PLATFORM VIEW	SELF-DOWNLOAD ARCHIVE	POSTER'S DEVICES	COUNTERPARTS / ECHOES	PROVIDER (LEGAL PROCESS)	DELETED / RECOVERABLE
Public posts	Until changed: capture now	Y with metadata	App caches, drafts	Reposts, archives, captures	Limited windows	Echoes + archive + provider window
Direct messages	Account view only	Y: thread exports	App databases (FFS)	The other end: fully	Varies by platform	Counterpart is the rescue
Stories / expiring	Window-bound: race	Sometimes archived	Creation media persists	Viewer captures	Short windows	Creation-side media often survives
Profile / handle history	Current state only	Account records	n/a	Historic captures, archives	Y: registration history	Reconstructable
Login / device history	n/a	Y: the quiet asset	Session artefacts	n/a	Y: IP logs	Attribution layer

Fallback strategy in one line: when the account vanishes, run the order: poster's devices, any archive, the echo layer, counterpart captures, provider windows: and date the vanishing itself, which after notice is an exhibit.

Worked examples

EXAMPLE 1 · THE STORY THAT EXPIRED INTO A COURSE OF CONDUCT

A harassment claimant reported that her former partner was posting Instagram stories about her: each gone in twenty-four hours, each deniable. The preservation reflex made the case: same-day forensic capture caught two stories inside their windows; the respondent's phone, later examined under an order, held the creation media: fourteen videos in the camera roll and app cache, timestamped across six weeks, matching the captured pair frame for frame; and his own platform archive, ordered with the phone, listed the story posts with their platform timestamps: fourteen posts, fourteen videos, one target. Ephemerality had promised deniability; the creation side and the archive kept the record the display refused to.

EXAMPLE 2 · THE EDIT THAT THE PAIR OF CAPTURES PROVED

A defamation defendant claimed his post had "always" included the words "in my opinion": and by inspection, it did. The claimant's solicitor had captured the post at rung 2 on the morning of publication: URL, timestamp, hash: and recaptured after the letter of claim. The pair told the story: the qualifying words absent at 09:14 on publication day, present in the post-letter capture, with the platform's own edit indicator confirming a revision in between. The defendant's archive, disclosed under order, carried the edit history with its timestamp: three hours after the letter of claim was emailed. Serious-harm arguments proceeded on the unqualified original; the edit joined the aggravation narrative. Two captures, one habit: the whole issue.

EXAMPLE 3 · THE ACCOUNT DELETION THAT UNMADE ITSELF

Days after receiving a preservation letter naming his X account, a commercial defendant deleted it: "long-planned digital detox". The estate said otherwise: the claimant's rung-2 captures, taken the week before the letter, preserved the disputed thread with its URL and engagement state; a quote-post by a third party carried the key post's text verbatim with its own independent timestamp; the web-archive service had crawled the profile twice in the relevant month; and the provider, served with the preservation request the day the letter went out, confirmed a hold on the account's data pending the disclosure order that followed. The deletion achieved nothing against the record and everything against its author: the tribunal's costs language on "the destruction of a named account within days of notice" did the rest.

Common mistakes and technical limitations

Common mistakes

- **Screenshot reliance:** the client's gallery as the evidence plan: rung 1 never upgraded, challenges invited.
- **Capture deferred:** the post identified Monday, captured never: edited Tuesday, deleted Thursday.
- **Archives unrequested:** the structured, metadata-rich export ignored on both sides of the case.
- **Preservation letters that forget the medium:** accounts unnamed, the predictable moves (edit, privacy flip, handle change, deletion) unforbidden.
- **The recapture never scheduled:** Example 2's pair impossible because the first capture stood alone.
- **Audience state uncaptured:** reach and visibility elements argued without evidence of who could see what.
- **Anonymous-account sequencing backwards:** unmasking applications launched while the content sat uncaptured and unpreserved provider-side.
- **Expired-content fatalism:** stories mourned while creation media sat on the poster's phone: Example 1's inverse.

Technical limitations

- **Platforms change faster than method notes:** interfaces, archive formats and retention policies shift constantly: capture tooling and provider expectations are verified per matter, not recalled.
- **Provider content windows are short and narrowing:** deleted-content recovery via process is the exception: the letter says so early.
- **Echoes authenticate weakly alone:** archives crawl selectively, reposts can themselves be fabricated: the echo layer corroborates; it rarely carries alone.
- **Private-audience content needs a lawful route:** closed groups and private profiles are reached by participants, orders or the account holder: not by investigator subterfuge, which taints what it touches.
- **Attribution ends at the account:** the account-to-hand step runs through devices and context (guide 65's ladder): provider IP logs help and VPNs bound them: pleaded to the rung reached, as ever.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Every account and post touching the issues: yours and theirs: identified today for same-day capture?
- Your own archives requested now, and your accounts frozen against "tidying" that reads as spoliation later?
- Who else saw, received or captured the content: the counterpart and echo map?

Ask your opponent

- Please preserve all social media content and account data of [accounts]: no deletion, editing, unpublishing, privacy-setting change, handle change, story expiry reliance or account deletion: and confirm within [3] days.
- Please provide the complete self-download archive for each named account, unmodified, with its generation date.
- Where content has been deleted or changed since [date]: please give particulars: what, when, by whom, and why after notice.

Ask your eDiscovery / forensic provider

- What rung is each key item captured at today, and what upgrades are available this week?
- What does the poster-side device examination add on authorship and creation?
- For the challenged exhibit: what does the full authentication stack support?

SUGGESTED WORDING · SOCIAL MEDIA LIMB FOR THE PRESERVATION LETTER

"Your client must immediately preserve all social media evidence relating to the issues, on all platforms, including: (a) all posts, stories, reels, comments, messages and media on the accounts identified in the Schedule, none of which may be deleted, edited, unpublished or restricted; (b) all account settings, which must not be changed, including privacy, audience and username settings; (c) the accounts themselves, which must not be deactivated, deleted or merged; and (d) a complete self-download archive of each account, to be generated within [7] days and preserved unmodified. Your client's attention is drawn to the fact that the accounts' public state has been forensically captured and will be recaptured: any change following this letter will be identified and relied upon."

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

The social media checklist

- ☐ Accounts and posts identified at matter-open; same-day rung-2 capture executed
- ☐ Client archives requested day one; client accounts frozen in writing
- ☐ Preservation letter names accounts and forbids the predictable moves
- ☐ Provider preservation requests lodged where provider data may matter
- ☐ Recapture schedule set; post-letter recapture always
- ☐ Audience and reach state captured, not just content
- ☐ Expiring content raced inside its windows
- ☐ Echo and counterpart layer mapped and captured
- ☐ Opponent archives sought by order early
- ☐ Contested exhibits run through the full authentication stack

Red flags

- Deletions, edits or privacy flips dated after the letter: Examples 2-3's pattern.
- A screenshot-only exhibit whose proponent resists device or archive verification.
- Handle changes or account "detox" mid-dispute.
- Stories weaponised for deniability: Example 1's design.
- Archives produced re-zipped, partial or regenerated late.
- Anonymous accounts engaging with the dispute in suspicious step with a party's knowledge.
- An echo layer that contradicts the "it never said that" account.

When to involve a digital forensic expert

At capture, where rung-2 methodology and expiring-content technique decide what exists (Example 1's same-day work); at upgrade, where archives and device-side artefacts turn captures into authenticated exhibits; at investigation, where deleted content is pursued across the §8 map and vanishings are dated (Example 3's estate); and at challenge, where the fabrication workup and the capture pedigree meet scrutiny under CPR Part 35. Through **e-discovery.uk**, captured social content is processed into review beside the estate's other channels: threaded, dated and cross-referenced per guide 70's assembly.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Are screenshots of posts admissible?

Admissible, yes: weighty, no: a screenshot is a document, but its fabrication-triviality means challenges succeed against it alone where they would fail against a documented capture corroborated by an archive or device artefacts. The practice rule: accept screenshots as leads, upgrade the same week, and never rest a pleaded quotation on rung 1 where rungs 2-3 were available: tribunals increasingly ask why they were not taken.

A post has already been deleted. What are the realistic routes?

In practical order: the poster's devices (creation media, app caches, drafts: Example 1's rescue); any self-download archive generated before deletion, or ordered now if deleted content persists in the account's export; the echo layer (reposts, quote-posts, web archives, search caches); counterpart captures and recipients; and provider windows via preservation request and process, moving fast because they close. Plus the deletion itself: dated against notice, it may be worth more than the post.

Can we make an opponent hand over their private account content?

Where relevant and proportionate, yes: private posts and messages are documents within their control: the self-download order is the clean mechanism (complete, structured, platform-generated), with specific disclosure of identified threads the narrower alternative. Privacy objections are weighed, not dispositive: UK GDPR and proportionality shape scope and handling (redaction, confidentiality clubs), not existence of the obligation.

How do we deal with an anonymous account attacking our client?

Sequence per §6: capture everything now (rung 2, scheduled recaptures); provider preservation request immediately; then the disclosure route against the platform for account and access data (the Norwich Pharmacal line), with service and jurisdiction navigated for non-UK entities; and in parallel, the contextual investigation: who knew what the account knew, posting-time patterns, linguistic and device overlaps: which has unmasked accounts that IP logs alone could not. Expectations honest: determined anonymity sometimes holds; the capture record ensures the content is usable against whoever is eventually fixed with it.

Our client wants to "clean up" their own profile before proceedings. Advice?

In terms: once litigation is contemplated, deleting or editing relevant content is spoliation with a timestamp: the other side captures too, and Examples 2-3 show how loudly changes date themselves. The lawful path: freeze the accounts, archive them, and address bad content by evidence and submission: context, apology where wise, honest explanation: rather than deletion that converts an embarrassing post into a conduct finding. This advice, given in writing at matter-open, has saved more positions than any capture tool.

Do expiring formats (stories, view-once) beat preservation?

They compress it: the display window binds the public-view capture, so the race is real (same-day, sometimes same-hour): but the format's promise is thinner than it looks: creation media persists poster-side, archives log the posting, viewers capture, and platforms hold short windows: Example 1's fourteen videos. The advice pairing: race the window when warned in time; when not, work the creation side and the viewers: expiry defeats the casual observer, not the map.

§ 1 4 · REFERENCE

Glossary

Capture ladder

The weight-ranked hierarchy: screenshot, forensic capture, archive, provider records.

Creation media

Poster-side originals persisting after display expiry; Example 1's layer.

Echo layer

Reposts, quote-posts, web archives and caches carrying vanished content.

Forensic capture

Documented, hashed, operator-attested acquisition of the live view.

Handle change

Username alteration; a standard mid-dispute move, reconstructable.

Preservation request (provider)

The freeze lodged with the platform pending legal process.

Recapture pair

Before-and-after acquisitions proving change; Example 2's method.

Self-download archive

The platform's structured account export; the corroboration backbone.

Serious harm state

The audience/reach evidence defamation analysis needs captured.

Unmasking sequence

Capture, preserve provider-side, then disclosure against the platform.

Sources and authoritative references

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

- cflab.uk, digital forensics services (social media capture, deleted-content investigation, authentication workups, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 01 · Identification, Phase 02 · Preservation and Phase 03 · Collection (account mapping; capture into review): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Platform data-download documentation: Meta: facebook.com/help · X: help.x.com · LinkedIn: linkedin.com/help
- PD 57AD and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, 27037

DISCLAIMER

This publication provides general information about social media evidence preservation as at August 2026. Platform features, archive contents, retention policies and legal-request channels change frequently; verify the current position for the platforms in the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Social media matters at the laboratory run on the reflex this guide teaches: same-day rung-2 capture of everything identified, expiring content raced inside its windows (Example 1's stories), recapture schedules that build the pairs (Example 2's method), and provider preservation lodged while the letters go out. Archives are obtained, sealed and mined: the login histories and metadata that decide authorship: and the poster-side device work adds the creation layer when displays expire or accounts vanish (Example 3's estate). Contested exhibits meet the full authentication stack; fabricated ones meet its conclusions. Reporting is CPR Part 35 with rungs and pedigrees stated; through **e-discovery.uk**, captured content joins the estate's other channels in one reviewable record. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a relevant story is live on someone's profile right now, the capture call comes before the reading.



I N S T R U C T T H E L A B

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