



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

Recovering Historical Documents from Snapshots and Volume Shadow Copies

The Time Machine Already Running on Your Client's Systems: and How to Read It Before It Prunes

Long before anyone thought of litigation, most systems were quietly keeping history: Windows Volume Shadow Copies preserving point-in-time states of whole disks, server and NAS snapshots doing the same for shares, and file-level version histories in SharePoint, OneDrive and Google Drive recording every save. Together they answer the questions disclosure most often struggles with: what did the document say before it was edited, when did the file disappear, and what did the folder hold last March? This guide gathers the snapshot and versioning layers scattered across this series into one practical treatment: what each layer keeps and for how long, how examiners recover and difference historical states, how the same machinery exposes backdating and deletion, and why the preservation email that stops the pruning is the most valuable page in this book.

⌚ Estimated reading time: 26 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. Snapshot and version-history work threads through most of its document-dispute casework: recovering pre-edit states, dating deletions, and dismantling backdated exhibits: on instruction for claimants, defendants and, under court appointment, as neutral examiner. Its eDiscovery arm, **e-discovery.uk**, integrates recovered generations into disclosure-scale review.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES

SNAPSHOT & VERSION RECOVERY

DOCUMENT AUTHENTICITY ANALYSIS

CPR PART 35 EXPERT REPORTS

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the history nobody meant to keep
- 03 The layers: shadow copies, snapshots and version histories
- 04 Volume Shadow Copies on Windows machines
- 05 Server, NAS and hypervisor snapshots
- 06 File-level version histories in cloud platforms
- 07 Differencing: turning states into a story
- 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: THREE HISTORY LAYERS, ONE DISCIPLINE: IDENTIFY, FREEZE, DIFFERENCE

Systems keep history at three depths, and most disputes about what-a-document-used-to-say are answered at one of them. **Volume Shadow Copies (VSS)** on Windows machines preserve block-level states of whole volumes at restore points and scheduled moments: inside them, prior versions of documents, files since deleted, and system artefacts as they stood weeks or months ago: recovered by mounting each shadow copy from a forensic image and reading it like a disk of that date. **Storage-layer snapshots:** on file servers (guide 43), NAS appliances (guide 44) and hypervisors (guide 45): do the same for shares and whole machines, on schedules from hourly to weekly, with retention the owner rarely knows. **File-level version histories** in SharePoint, OneDrive, Google Drive and document-management systems record per-save generations with author and timestamp: the finest grain, tied to named accounts. Each layer prunes on its own schedule, which makes the day-one preservation email: suspend snapshot pruning, version-history trimming and shadow-copy deletion for in-scope systems: the cheapest decisive act in this corner of practice. Recovery then follows one method regardless of layer: enumerate the states that exist, freeze and collect them forensically, and **difference** them: comparing generations to show precisely what changed, appeared or vanished between dates: the technique that converts storage housekeeping into a chronology of drafting, deletion or fabrication. The same machinery cuts both ways: it resurrects what your client needs, and it exposes what your opponent's exhibit used to say: which is why version-history questions belong in every document-authenticity instruction this series drafts.

- **Ask "what history layers run?" before pleading loss:** most "deleted" and "overwritten" documents survive in at least one layer; declaring destruction without checking all three is this guide's founding error.
- **The pruning clock is real:** VSS deletes oldest-first as space demands; snapshot schedules roll; cloud version limits trim: the layers are generous but not patient.
- **Differencing is the product:** single recovered states prove existence; differenced series prove change: when the clause was inserted, when the folder emptied, when the ledger was rebuilt.
- **Authenticity work starts here:** a disputed document's version trail (or its telling absence) across shadow copies, snapshots and platform histories is the backbone of backdating and tampering analysis.
- **Collection is forensic, per layer:** shadow copies come from full images; snapshots are collected at the storage layer under guide 43-45 disciplines; platform histories are exported with metadata: each with hashes and custody, because recovered generations get challenged hardest.

The problem in plain English: the history nobody meant to keep

None of these layers was built for lawyers. Shadow copies exist so Windows can restore itself; snapshots exist so administrators can undo mistakes; version histories exist so users can recover from their own edits. Their evidential power is a by-product, and it has a particular character: the history was written automatically, continuously and without anyone's litigation in mind: which is exactly what makes it hard to argue with. A witness can explain a document; explaining why the Tuesday snapshot disagrees with the Thursday exhibit is harder.

The corresponding hazard is ignorance on your own side. Clients declare documents lost that three layers still hold; opponents produce "originals" whose earlier states sit in their own SharePoint history; and preservation notices freeze mailboxes while shadow copies age out and snapshot schedules prune the states that would have decided the case. The lawyer's job is not to operate any of this machinery: it is to know it exists, ask the three-layer question early, send the email that stops the pruning, and instruct the differencing that turns states into a story.

The layers: shadow copies, snapshots and version histories

LAYER	WHERE IT RUNS · TYPICAL CADENCE	WHAT IT PRESERVES, AND ITS HABITS
Volume Shadow Copies	Windows PCs and servers · restore points, installs, scheduled (where enabled)	Block-level volume states: prior file versions, deleted files, historical system artefacts. Space-managed: oldest deleted automatically; count and reach vary wildly per machine.
Storage snapshots	File servers, NAS, SANs, hypervisors · hourly to weekly schedules	Share- or machine-level states; the history layer of guides 43-45. Retention set by policy; pruned on schedule; capturable and mountable at the storage layer.
Platform version histories	SharePoint/OneDrive, Google Drive, DMS · per save/edit	Per-document generations with author, timestamp, sometimes comment: the finest grain and the only layer with per-user attribution built in. Version limits and manual deletion trim it.

The layers overlap without duplicating: a document might have four platform versions today, appear in six weekly share snapshots across two months, and sit in a laptop's shadow copies in states the platform never saw. Sourcing decisions (and preservation letters) treat them as a set.

Volume Shadow Copies on Windows machines

- **What they are:** point-in-time block maps of a volume, created at restore points, before updates, and on schedule where System Protection is on: each mountable, from a forensic image, as the disk of that date: files, folders and (valuably) registry hives, event logs and the guide 41 artefact set as they then stood.
- **What examiners do with them:** enumerate the copies present (count and dates are the first report), mount each, and target: the disputed document's earlier states, the folder before it emptied, the artefact record before a clean-up ran. Historical artefacts extend timelines: a shadow copy's registry can hold USB records (guide 47) and account traces the live system no longer shows.
- **Their habits, honestly:** presence is configuration-dependent (server volumes and many corporate builds disable them; consumer machines vary); space pressure deletes oldest-first, so heavy use shortens reach; and deliberate deletion of shadow copies: a one-line command, and standing ransomware behaviour: is itself a datable act the examiner reports as conduct.
- **Collection consequence:** shadow copies live inside the volume: a full forensic image captures them; logical file copies do not: one more reason guide 32's method question is asked before anyone collects "just the documents" from a machine whose history may matter.

Server, NAS and hypervisor snapshots

- **One idea, three homes:** the storage layer preserves whole states: shares (server filers and NAS appliances, guides 43-44), and entire machines (hypervisor chains and backup restore points, guides 45 and 49). This guide's contribution is their document use: each snapshot is a generation of every file it covers.
- **Enumerate before promising:** the schedule and retention (hourly for a day, daily for a month, weekly for a year is a common ladder) define the resolution of the historical record; the first deliverable is the snapshot inventory for the shares in issue.
- **Collect at the layer:** snapshots are mounted and collected server-side under protocol: never by restoring over live data: with each generation hashed and manifested as its own collection, per guide 43's method.
- **Deletion dating as standard:** a file present in the 03:00 snapshot and absent at 03:00 the next day brackets its deletion to the day: multiplied across a folder, the pattern dates a purge: the guide 43-44 examples' engine, available wherever schedules ran.

File-level version histories in cloud platforms

- **Per-save generations with names attached:** SharePoint and OneDrive version histories, Google Drive revisions and DMS version stacks record each saved state with account and timestamp: the only layer that says *who* made the change without further correlation.
- **Export with the metadata:** versions are collected through the platform's proper export routes with authorship and timestamps intact (the cloud guides ahead give mechanics); screenshots of a version pane are not a collection.
- **Trimming and its meaning:** version limits, manual version deletion and "delete version history" actions curtail the record: the platform logs many such actions, and a history that stops the week the dispute began is a finding, not a dead end: the audit layer (guide 57 ahead) picks up where versions vanish.
- **Co-authoring nuance:** modern co-edited documents interleave authors within versions; the examiner reads version records alongside the platform's activity log before attributing a specific change: the honest grain of "who wrote this sentence" is platform-dependent, and reports say so.

Differencing: turning states into a story

- **Inventory diffs:** generation-to-generation file listings show appearances, disappearances, renames and size changes: the folder-level chronology, exhibitable as a table the court can read.
- **Content diffs:** for the documents in issue, generation pairs are compared at content level: inserted clauses, changed figures, removed paragraphs: with hashes proving identity where nothing changed and the diff proving exactly what did where it did.
- **Metadata tracks the edits:** internal timestamps, authorship fields and revision counters across generations either march coherently or betray manipulation: the backdating tells, run across the historical series rather than the single suspect file.
- **Convergence across layers:** the strongest chronologies interleave layers: platform versions give the fine grain and names, snapshots anchor independent weekly truth, shadow copies add the machine-side states: and a story consistent across all three is, in practice, unanswerable.
- **Present it as a timeline:** the deliverable is a dated series: state, change, actor where known: with method and layer per entry: the format courts absorb, and the format cross-examination struggles to shake.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never treat one history layer as the history. A document's past states may exist in: the live file's own internals (embedded revision data, tracked changes); platform version histories; share and NAS snapshots; hypervisor chains and backup generations beneath the servers (guides 45 and 49); shadow copies on every machine that held a local copy; sync-client caches and conflict copies on endpoints; counterpart copies (the version emailed out at each stage: recipients' mailboxes as an involuntary version archive); and the audit logs that record edits, deletions and version-history tampering even where the versions themselves are gone. When the primary layer is pruned, trimmed or deliberately cleared, the others: and above all the emailed-out counterpart trail: usually still carry the story.

EVIDENCE	PLATFORM VERSIONS	SNAPSHOTS (SHARE/VM)	SHADOW COPIES (ENDPOINTS)	BACKUPS	COUNTERPART COPIES (MAIL)	DELETED / RECOVERABLE
Prior document states	Y: per save, named	Y: per schedule	Y where enabled	Y: deep, sparse	Y: as-sent generations	Trimmed versions: via audit + other layers
Deletion timing	Recycle + audit records	Y: bracketed	Sometimes	Y: bracketed, coarse	n/a	Inferential
Who changed it	Y: version author	n/a (state only)	Session correlation	n/a	Sender/date context	Audit logs where enabled
Folder-level history	Partial (per-file)	Y: the natural grain	Y	Y	n/a	Varies
Tampering with history itself	Audit: version deletion events	Schedule gaps, admin logs	Deletion command traces	Catalogue gaps	Survives untouched	The act usually dates itself

Fallback strategy in one line: when one layer is silent, interleave the rest: and remember that every generation ever emailed out lives on in someone else's mailbox, beyond the reach of whoever curated the history at home.

Worked examples

EXAMPLE 1 · THE CONSULTANCY AGREEMENT WITH A GROWING CLAUSE

A consultancy agreement produced in a fee dispute contained a termination-payment clause the paying party swore had never been agreed. The document lived in the producing party's SharePoint; its version history had been trimmed to a single current version: itself a flag. The layers behind it were not so tidy: the finance share's weekly snapshots held the file across five months, and differencing showed the clause absent until a snapshot three weeks after the relationship soured, then present with the document's internal edit time matching a Sunday evening; and the counterpart trail: the draft emailed to the paying party at signature: matched the clause-free generations. The audit log recorded the version-history deletion, by the producing director's account, two days before disclosure. The claim settled on receipt of the report; the costs discussion referenced the Sunday evening specifically.

EXAMPLE 2 · THE LAPTOP THAT REMEMBERED THE REAL ACCOUNTS

In a shareholder dispute, management accounts were alleged to have been rebuilt to hide diverted revenue: but the finance share had no snapshots and the platform history began after a migration. The FD's laptop image carried eleven shadow copies spanning seven months. Mounted in series, they held the working spreadsheet in nine states: and the differencing showed the revenue tab's figures unchanged for five months, then restated wholesale in a single generation whose date fell between the claimant's share-purchase enquiry and the figures being presented. The shadow copies also held the machine's execution artefacts for that day: the spreadsheet open for six hours, a calculator utility, and a file-wiping tool run that evening: which had cleaned the live disk but not the shadow copy recording it. The machine had preserved both the fabrication and the cover-up.

EXAMPLE 3 · THE PURGE DATED TO THE MAINTENANCE WINDOW

A departing team's project folder was found empty at handover; the employer alleged a leaving-day purge and sought delivery-up and damages from the team's new venture. The NAS's snapshot inventory reframed everything: the folder was intact in every nightly snapshot up to and including the team's final day: and vanished in the snapshot after a weekend during which, per the appliance's own logs, an administrator ran a "storage reclamation" script that removed dormant project folders wholesale, the departed team's among forty others. The deletion was the employer's own housekeeping, a week after departure. The snapshots restored the folder in full; the claim against the team collapsed; and the reclamation script acquired a review step.

Common mistakes and technical limitations

Common mistakes

- **Loss declared before the three-layer check:** "deleted" pleaded while snapshots hold the file: Example 3's near-miss for the employer, run in reverse daily.
- **Preservation letters that skip the layers:** mailbox holds issued while pruning schedules eat the states that mattered.
- **Logical collection from machines whose history counts:** shadow copies forfeited because nobody imaged.
- **Single-state reasoning:** one recovered version argued as the story, undifferentiated against its neighbours.
- **Version panes screenshotted, not collected:** the exhibit that dissolves under the first authenticity question.
- **Trimmed histories accepted at face value:** a one-version document treated as simple rather than curated: Example 1's flag, unread.
- **Attribution from state layers:** snapshots say what changed, not who; names imported without the platform or session evidence.
- **Restoring over live systems:** the recovery that destroys what it recovers.

Technical limitations

- **Presence is configuration:** every layer can be off, trimmed or short: the inventory step reports reality before anything is promised.
- **Resolution is the schedule:** weekly snapshots cannot separate Tuesday from Thursday; the report brackets to the grain that exists.
- **Space pressure eats VSS silently:** reach on a busy disk may be days; on an idle one, a year: per-machine facts, not assumptions.
- **Co-authored attribution has a floor:** platform version records attribute saves, not keystrokes; sentence-level claims need the platform's finer activity data or restraint.
- **History can be attacked:** shadow-copy deletion, snapshot purges and version trimming happen: usually logged, always datable in effect, but capable of taking content with them: the conduct finding then does the work the content cannot.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- For each system holding the documents in issue: what snapshot schedules, version settings and shadow-copy configuration run: and who can suspend pruning today?
- Which machines held local copies, and can we image rather than copy them?
- What was emailed out, to whom, at which stages: the counterpart version trail?

Ask your opponent

- Please preserve, and suspend all pruning, trimming and deletion of: volume shadow copies on [machines], snapshots on [shares/systems], and version histories for [documents/libraries], confirming the schedules previously in force.
- Please produce the version history of [document] as held on [platform], with authorship and timestamps, together with any audit records of version deletion or history trimming.
- Please state the snapshot inventory (dates held) for [share] and whether any snapshots have been deleted outside schedule since [date].

Ask your eDiscovery / forensic provider

- What does the three-layer inventory actually show for our systems: counts, dates, reach?
- What differencing plan fits the issues: which documents, which generation pairs, what deliverable?
- Where history has been trimmed or cleared, what do the audit and counterpart routes recover?

SUGGESTED WORDING · INSTRUCTION FOR HISTORICAL-STATE RECOVERY

"Please: (1) inventory the historical-state layers for the systems at Schedule A: volume shadow copies (per machine: count and dates), storage snapshots (per share: schedule, retention, dates held) and platform version histories (per document library: settings and depth): and report reach against the period in issue; (2) collect forensically the generations relevant to [issues], hashed and manifested per generation; (3) difference the collected series at inventory and content level for the documents at Schedule B, producing a dated timeline of changes, appearances and deletions, with the layer and method stated per entry and authorship included only where a layer attributes it; (4) examine for interference with the history layers themselves (version deletion, snapshot removal, shadow-copy clearance), dating any found; and (5) state resolution limits and configuration gaps expressly."

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

The historical-states checklist

- ☐ Three-layer question asked before any loss is pleaded or conceded
- ☐ Day-one letter suspends pruning, trimming and shadow-copy deletion, both sides
- ☐ Layer inventory obtained: counts, dates, reach, per system
- ☐ Machines with relevant local copies imaged, not logically copied
- ☐ Generations collected forensically, hashed and manifested per state
- ☐ Differencing run as a series, not a single-state argument
- ☐ Attribution taken only from layers that carry it; state layers used for states
- ☐ Trimmed or missing history treated as a finding: audit and counterpart routes engaged
- ☐ Timeline deliverable prepared with layer and method per entry
- ☐ Resolution and configuration limits stated in the report

Red flags

- A disputed document with exactly one version.
- Version history "not available" on a platform that keeps it by default.
- Snapshot schedules that pause around the key dates.
- Shadow copies cleared shortly before imaging.
- An opponent restoring systems mid-dispute "for performance".
- Chronologies built on one layer when three ran.
- "The migration lost the history" with the pre-migration source unexamined.

When to involve a digital forensic expert

At the letter stage, so the suspension wording matches how each layer actually prunes; at inventory, where reading VSS, snapshot and version reality is an examiner's afternoon and a generalist's hazard; at recovery and differencing, which are laboratory work with challenge-ready custody; and in every authenticity dispute, where the historical series is the backbone this series' backdating methods stand on. Examples 1-3 share one shape: the decisive material was already being kept, automatically, by machinery neither side controlled for litigation: the expert's role was knowing where it lived and reading it before it aged out. Reported under CPR Part 35, limits stated, both instructing positions routine.

§ 13 · COMMON QUESTIONS

Frequently asked questions

How far back do these layers really go?

Per layer, per configuration: platform version histories can span a document's whole life (subject to limits and trimming); storage snapshots follow their retention ladder: commonly weeks to a year; shadow copies are the wildcard, from days to a year depending on disk pressure; and backups (guide 49) reach deepest at the coarsest grain. The honest answer is the inventory: an afternoon's work that replaces speculation with a dated list, and the first thing to commission.

Can deleted version histories or snapshots be recovered?

Sometimes the content, usually the fact: platform audit logs record version deletions with account and date; snapshot removals log at the appliance or hypervisor; shadow-copy clearance leaves command traces. Content-wise, the other layers frequently hold the same generations (a trimmed SharePoint history rarely outruns the share snapshots and the emailed counterparts), which is the architecture table's point: history tampering tends to curate one shelf of a library while the others keep lending.

Is a document recovered from a shadow copy or snapshot admissible like the original?

It is disclosed and proved like any electronic document, with its provenance stated: which layer, which dated state, collected how, hashed when. Properly collected, its evidential position is strong precisely because the preserving system acted automatically and before the dispute; the challenges that succeed target sloppy recovery (restored over live data, unhashed, undocumented), not the concept. Hence the laboratory-collection discipline throughout this guide.

The other side's disclosure shows only final versions. What should we ask for?

The §11 requests: version histories with authorship for the named documents; audit records of version deletion or trimming; snapshot inventories for the hosting shares; and confirmation of suspension. Then read the answers as evidence: platforms keep versions by default, so absence has causes: settings, trimming, migration: each checkable, each with its own audit trail, and each more informative than the silence it replaces.

Do Macs and non-Windows systems have equivalents?

Yes: APFS local snapshots and Time Machine series on Macs (guide 42's structure-not-carving point), ZFS/Btrfs snapshots on the appliances and servers guides 43-44 cover, and the same platform version histories wherever the documents live in cloud services. The three-layer question is asked identically; only the tool names change: and the preservation email adapts its verbs, not its logic.

What single habit should our team adopt from this guide?

Make "what history layers run, and when do they prune?" a standard early question in every document dispute: alongside the custodian list, before the preservation letter goes out. It costs one conversation with IT, it shapes the letter's most valuable paragraph, and in a meaningful fraction of cases it is the difference between arguing about what a document says and proving what it said: the entire trade of this guide, available for the price of asking.

§ 1 4 · REFERENCE

Glossary

Differencing

Comparing generations to show exactly what changed between dated states.

Generation

One preserved state of a file, share or volume at one moment.

Inventory (layer)

The enumerated list of states each layer holds: counts, dates, reach.

Pruning / trimming

Scheduled or manual removal of old states; the clock preservation must stop.

Restore point

A Windows-created shadow copy moment; also guide 49's backup unit.

Shadow copy (VSS)

Windows block-level volume state; mountable as the disk of its date.

Snapshot ladder

Tiered retention (hourly/daily/weekly) defining historical resolution.

Version history

Per-save document generations with author and time on platforms and DMS.

Version trimming

Deletion of history entries; logged by most platforms, datable in effect.

Counterpart trail

As-sent generations preserved in recipients' mailboxes; the involuntary archive.

Sources and authoritative references

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

- cflab.uk, digital forensics services (snapshot and shadow-copy recovery, version-history analysis, document authenticity, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (layer-aware preservation and generation collection; "defensibility is built, not retrofitted"): 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
- NPCC / College of Policing digital evidence guidance: [college.police.uk, digital devices guidance](https://college.police.uk/digital-devices-guidance) · ISO/IEC 27037:2012: [iso.org, 27037](https://iso.org/27037)
- PD 57AD (preservation of documents that would otherwise be deleted under routine processes) and CPR Part 35: [justice.gov.uk, PD 57AD](https://justice.gov.uk/pd-57ad) · [justice.gov.uk, Part 35](https://justice.gov.uk/part-35)
- ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about snapshot, shadow-copy and version-history recovery as at August 2026. Layer behaviour varies by platform, version and configuration, and 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

Historical-state work is core laboratory practice: the three-layer inventory delivered in days; suspension wording for the day-one letter matched to how each layer actually prunes; forensic collection of shadow copies (from full images), snapshots (at the storage layer) and platform versions (with metadata); differencing series into the dated timelines Examples 1-3 turned on; and interference analysis where the history itself was attacked: reported under CPR Part 35 with resolution and configuration limits stated. Authenticity instructions: is this document what it claims to be?: run on this machinery as standard. Through **e-discovery.uk**, recovered generations deduplicate into disclosure-scale review so the deltas, not the duplicates, reach reviewers. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a pruning schedule is running against you today, the suspension email outranks this brochure.



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