



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

Can We Collect Only Relevant Data Instead of Imaging Everything?

Targeted Collection: Its Proportionality Advantages and Its Honest Risks

Yes: targeted collection is lawful, defensible and often the proportionate choice, and courts increasingly expect parties to reach for it before imaging entire estates. But narrowing what you take means deciding, in advance, what you will never have: deleted material, artefacts, and everything the selection criteria missed. This guide sets out when targeted collection is the right answer, how to design criteria that survive scrutiny, the forensic disciplines that must travel with it, the preservation backstop that makes narrow choices safe, and the risks that follow when targeting becomes triage by guesswork.

© 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. Its examiners design and execute targeted collections weekly, alongside the full imaging work that anchors contested devices, and its eDiscovery arm, **e-discovery.uk**, builds collection scope as a proportionality instrument: aggressive about noise, forensic about method, and always with the preservation backstop that keeps narrow choices reversible.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ISO 27001-ALIGNED SECURITY

ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES

TARGETED & FULL-IMAGE COLLECTION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the estate and the needle
- 03 What targeted collection is, and is not
- 04 The proportionality case for collecting less
- 05 The risk register: what narrowing costs
- 06 Designing selection criteria that survive scrutiny
- 07 The forensic disciplines that must travel with it
- 08 The preservation backstop: making narrow safe
- 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: COLLECT LESS, DECIDE MORE, PRESERVE EVERYTHING YOU MIGHT REGRET

The answer to the title is yes, with conditions. Targeted collection (taking defined custodians, folders, mailboxes, date ranges and data types rather than imaging every device) is often the proportionate, GDPR-respecting, budget-rational choice, and the disclosure regime's own logic (reasonableness under CPR 31, proportionality under PD 57AD, and the DRD's scoping machinery) points toward it. The conditions are three. **First, targeting is a scope decision, not a method discount:** whatever is taken is still collected forensically: metadata-preserving tools, hashes at acquisition, logs and custody, per guides 31 and 32. **Second, the criteria are designed and recorded:** derived from the issues, the data map and custodian interviews, stated in the protocol, and reasoned in writing, because the question a targeted collection must survive is not "did you take everything?" but "how did you decide what to take?". **Third, the backstop:** where a source is contested, deletion-prone or central, preserve it fully (a sequestered image or hold) even while collecting narrowly from it, so a narrow choice today is reversible tomorrow. Targeting without those conditions is not proportionality; it is triage by guesswork, and guesswork is what opponents litigate.

- **What targeting saves:** collection time, processing and hosting volume, review spend (the budget's real destination), business disruption, and the privacy intrusion of sweeping in what was never needed: the data-minimisation duty made operational.
- **What targeting surrenders:** deleted files and unallocated space, system artefacts (USB history, execution traces), the material outside the criteria, and the ability to answer questions nobody has asked yet. Surrender knowingly or not at all.
- **The deciding variable is contest:** the more likely a device or custodian is to be personally accused, forensically examined or suspected of deletion, the stronger the pull toward full imaging (or image-and-hold) for that source, however targeted the rest of the exercise.
- **Symmetry with the opponent:** expect and accept targeted collection from the other side too; the currency of challenge is their criteria and records, not the bare fact of narrowing.
- **The one-line discipline:** scope is a dial, method is not; turn the first freely, never the second.

The problem in plain English: the estate and the needle

A modern dispute touches perhaps eight people, three years and one project. The estate those people inhabit holds terabytes: a decade of shared drives, forty mailboxes, phones, chat platforms, cloud storage, and backups of all of it. Imaging everything is the instinct of caution, and it has real virtues: nothing is missed, every question answerable later. It also has real costs: weeks of collection, processing bills scaled to volume, review scaled to processing, a mountain of employees' personal and irrelevant data now sitting in a litigation platform, and, quite often, a proportionality argument gift-wrapped for the other side ("they copied the entire company to find twelve emails").

Targeted collection is the grown-up alternative: take the eight people, the project's folders, the relevant date span, the platforms where the story actually happened. Done well, it is faster, cheaper, kinder to data-protection duties and easier to defend in a DRD. Done badly (criteria invented at the keyboard, no record of reasoning, no preservation behind the choices, methods degraded along with the scope) it manufactures the worst outcome available: a collection that is simultaneously narrow and indefensible. The craft this guide teaches is how to get the first version and prove it is not the second.

§ 0 3 · DEFINITION

What targeted collection is, and is not

- **It is scope narrowing:** selecting custodians, sources, containers (folders, mailboxes, sites, channels), date ranges and data types before collection, so that only the selection is acquired. The selection can operate at any grain: whole mailboxes for eight people; three folders from a share; one channel from a chat platform; documents matching date bounds from a DMS.
- **It is not search-term review at the point of collection:** running keyword filters during acquisition is technically possible and occasionally agreed, but it compounds the risks (terms are untested at that stage, families fragment, and what the term missed was never taken). The stable pattern is: collect by container and date, cull by terms at processing, where results can be tested and revisited.
- **It is not a method change:** targeted collection uses forensic tooling that preserves metadata, computes hashes, and logs the exercise: guide 32's "targeted collection" method, with all of guide 31's disciplines. Copy-paste by IT is not targeted collection; it is casual copying with a smaller blast radius.
- **It sits inside the protocol:** the criteria, their rationale, the method per source and the preservation backstop are sections of guide 36's document; a targeted collection without a protocol is precisely the improvisation the approach cannot afford.

The proportionality case for collecting less

- **The regime asks for it:** civil disclosure is bounded by reasonableness and proportionality; PD 57AD's models and the DRD exist to scope exercises to the issues; and a party that images indiscriminately will fund the difference and may still be criticised. Narrow, reasoned scope is what the framework rewards.
- **The economics compound:** every gigabyte collected is processed, hosted, and (the dominant cost) reviewed. Cutting collection volume is the highest-leverage budget decision in the pipeline: culling at source is worth multiples of culling at review, which is why our eDiscovery practice treats scope design as the exercise's first cost-control, not its afterthought.
- **Data protection points the same way:** UK GDPR minimisation is a legal duty, not a preference: collecting whole estates to find a project's documents sweeps employees' personal lives into litigation platforms without necessity. Targeted scope is the compliance posture that needs no apology in a DSAR, an ICO question or an employee grievance.
- **Operations and people:** targeted collection can run without seizing machines for days, without imaging the CEO's family photographs, and without the workforce-relations cost of "they copied everything we ever wrote". These are real litigation-adjacent harms, and reducing them is part of acting well.
- **Speed is evidence too:** a targeted collection completed this week beats a full-estate collection completed next quarter, because preservation risk runs while collection waits; the fastest route to having the central material safely in hand is usually the narrow one.

The risk register: what narrowing costs

- **Deleted material and artefacts are not taken:** targeted tools collect live files; unallocated space, deletion traces, USB and execution history stay on the source. If the matter later grows a deletion or exfiltration limb, a purely targeted collection has nothing to say: the classic scenario for the §8 backstop.
- **The criteria's blind spots are permanent (unless preserved):** the folder nobody mentioned, the custodian outside the list, the project channel under an unexpected name: what selection misses, collection never has, and re-collection months later meets an estate that has moved on.
- **The reasoning becomes the target:** a full image is challenged rarely; a targeted collection is challenged at its edges ("why not that share? why this date?"), so the exercise's defensibility lives in the written rationale and the interview and data-map pedigree behind it.
- **Execution error is quieter:** a mis-scoped image announces itself by size; a targeted collection that silently excluded subfolders, skipped locked files or misapplied a date filter looks complete. Verification (counts, manifests, sampling against source) is the audit that catches it, and belongs in the protocol.
- **Repeat visits cost:** going back to sources iteratively disturbs the business each time and, for departing custodians and reissued devices, may be impossible; scope design should overshoot mildly (collect the whole mailbox, not the "relevant" folders within it) precisely to buy freedom from return trips.

Designing selection criteria that survive scrutiny

- **Derive from the issues, visibly:** each issue in the case maps to custodians, systems and periods; the criteria table shows the mapping, so scope has a pedigree the DRD can quote and an opponent can test rather than merely attack.
- **Build on the data map and interviews:** custodian interviews ("where did this project live? what did you call it? who else touched it?") are where the unexpected folder and the nickname channel surface before rather than after; criteria written without interviews are guesses with formatting.
- **Prefer containers to content:** select mailboxes, folders, sites, channels and date ranges (stable, explainable, testable) over keyword-filtered collection (fragile at this stage, per §3). Take whole containers a size up from the minimum: the mailbox, not fourteen folders within it; the project site, not six libraries.
- **Date ranges with anchors and margins:** tied to pleaded events, widened by a sensible margin either side, and applied where boundary error is safe (at processing, unless collection-time filtering is genuinely reliable for that source type).
- **Name the exclusions:** what was deliberately not collected, and why: the sentence that converts absence from omission into decision, and the first thing a well-run challenge asks for.
- **Version and revisit:** criteria are dated; when review learns (new names, new systems), scope is amended through the protocol's machinery, and the amendment trail is itself the evidence of a party engaging honestly with its disclosure duty.

The forensic disciplines that must travel with it

- **Metadata-preserving acquisition:** targeted tools that maintain timestamps, paths and properties, and container formats that carry them; the drag-and-drop copy that rewrites dates is the anti-pattern, per guide 31's first example.
- **Hashes, logs, custody:** per-item or per-container hashing at acquisition, collection logs recording what ran where and when, exhibit references and transfer records: the full guide 31/34/35 apparatus, unshrunk by the smaller scope.
- **Manifests and counts:** a targeted collection's deliverable includes the manifest (what was taken, from where, item counts, sizes, hash values) reconciled against source-side counts, because completeness within the criteria is the claim being made, and it needs arithmetic behind it.
- **Verification sampling:** a proportionate sample re-checked against source (items opened, metadata compared) catches the silent execution errors of §5; the sample and its results go in the collection report.
- **The record of the criteria themselves:** the protocol section stating scope, rationale and exclusions, signed and dated: the single document that answers "how did you decide what to take?" without a meeting.

The preservation backstop: making narrow safe

- **The pattern:** preserve broad, collect narrow. Contested devices are imaged and the image sequestered (stored, hashed, unexamined) even while only targeted material is processed; cloud sources sit under legal hold while exports are scoped; backups are preserved while live systems are collected selectively. The narrow choice then risks nothing permanent: if the matter grows a limb, the sequestered layer is waiting, with acquisition-day hashes.
- **Where the backstop is mandatory in practice:** the accused custodian's devices; any source where deletion is suspected or plausible; leavers' machines ahead of reissue; single-copy sources with no organisational redundancy. Where it is unnecessary: stable corporate systems with versioning, recycle-bin machinery and audit trails, whose own resilience is the backstop.
- **Cost calibration:** a sequestered image is storage-cheap precisely because it is not processed or reviewed: the £600 insurance policy of guide 32's third example. The expensive version of caution is processing everything; the cheap version is preserving everything and processing little.
- **Say it in the DRD:** "collected on a targeted basis per the protocol; underlying devices imaged and preserved unexamined" is a sentence that disarms most scope challenges before they are made, because the opponent's real fear (that narrowing destroyed their case's evidence) is answered.

Worked examples

EXAMPLE 1 · THE TARGETED COLLECTION THAT BEAT THE DEADLINE AND THE BUDGET

A warranty dispute needed the deal team's records: six custodians, one data room, eighteen months. The protocol scoped six mailboxes, the deal share, the data-room export and two phones (messaging apps only, by consent), all collected forensically inside a week at a fifth of the full-estate quote; the two principals' laptops were imaged and sequestered as backstop. The opponent's request for "all company systems" was answered with the criteria table, the interview summaries behind it, and the sequestration note. The court's disclosure guidance hearing endorsed the scope in a sentence, and review began a month before it would otherwise have started: proportionality, functioning as designed.

EXAMPLE 2 · THE FOLDER NOBODY MENTIONED

A targeted collection took "the project folders" from a share, as listed by the client's programme office. A year later, disclosure from the other side referenced documents that should have existed on the claimant's systems and did not appear: they lived in a personal working folder a departed engineer had kept outside the project tree, never interviewed about because he had never been asked. The folder still existed and was collected late, with an explanation and a costs consequence; the deeper repair was procedural: interviews before criteria, containers a size up, and a preservation hold on the whole share from day one, all of which the original exercise had trimmed to save a week it did not, in the end, save.

EXAMPLE 3 · THE EXFILTRATION LIMB THAT GREW

An employment dispute began as a bonus claim: targeted mailbox collection, proportionate and clean. Mid-proceedings, evidence emerged that the claimant had taken client lists on departure, and the matter grew its exfiltration limb: USB history, deletion traces, copy timestamps: none of it in mailbox exports. The respondent's fortune was one decision made at the start: the claimant's returned laptop had been imaged and sequestered before reissue, per the leaver-device backstop. The image, unexamined for nine months, yielded the device-history artefacts that decided the new limb. Same scope decisions, without the backstop, would have left the respondent proving exfiltration from correspondence: which is to say, not proving it.

Common mistakes and technical limitations

Common mistakes

- **Criteria without pedigree:** scope invented in a meeting nobody minuted, from a data map nobody made, tested against interviews nobody held.
- **Method degraded with scope:** "we're only taking folders, IT can copy them": the conflation guide 32 exists to kill.
- **Keyword-filtered acquisition** as a first resort, fragmenting families and freezing untested terms into the collection boundary.
- **No backstop on the contested source:** the accused's laptop collected lightly and reissued; the one irreversible version of narrow.
- **Exclusions unrecorded,** so every absence reads as omission and every challenge starts from suspicion.
- **No manifests or sampling,** leaving completeness-within-criteria as an assertion rather than an arithmetic.
- **Scope never revisited** as review learns, so the criteria of month one quietly misdescribe the collection of month nine.
- **Asymmetric indignation:** attacking the other side for targeting while defending your own; the challenge currency is records, and it spends both ways.

Technical limitations

- **Live-file horizon:** targeted methods see the file system's present; recovery of the deleted and the historic needs images, snapshots, versions or backups, which is a sourcing question the protocol must answer, not a tool setting.
- **Locked and open files:** some in-use items resist copying and are silently skipped by naive tools; forensic tooling handles or logs them, which is one reason the method discipline is non-negotiable.
- **Filter semantics vary by system:** a date filter may read created, modified or received depending on platform, and time zones move boundaries; criteria state which field, which zone, and the margin that absorbs the ambiguity.
- **Cloud scoping depends on the platform's export grain:** what "a channel" or "a site" includes is defined by the service's mechanisms, with limits the cloud guides of this series detail; criteria for cloud sources are written against the export's actual behaviour, not its name.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- For each issue: who worked on it, where does its material live, what was it called internally, and who has left? (The interview layer the criteria stand on.)
- Which sources could be accused, deleted or reissued? (The backstop list.)
- What is the realistic budget across collection, processing and review if we image broadly versus collect narrowly? (The economics made explicit.)

Ask your opponent

- Please state the criteria (custodians, sources, date ranges, exclusions) by which your collection was scoped, and provide the protocol section recording them.
- Please confirm what preservation stands behind sources collected on a targeted basis, and whether underlying devices or systems remain available.
- Please provide the collection manifests and any verification sampling for the targeted exercise.

Ask your eDiscovery / forensic provider

- How will the targeted acquisition preserve metadata, and what does the manifest and hash deliverable look like?
- What sampling verification do you run, and at what rate for this estate?
- Which sources on our list would you image-and-hold regardless, and what does that backstop cost?

SUGGESTED WORDING · SCOPE AND BACKSTOP CLAUSES FOR THE PROTOCOL

"2.3 Collection shall be targeted in accordance with the Criteria Table (Schedule C), which records for each issue the custodians, sources, containers and date ranges selected, the derivation of each from the data map and custodian interviews, and the sources considered and excluded, with reasons. 2.4 Notwithstanding the targeted scope, the sources listed in Schedule D (contested or deletion-sensitive sources) shall be forensically imaged and the images sequestered: stored sealed, hash-verified and unexamined, pending any order or agreement for their examination. 2.5 The collection deliverables shall include per-source manifests reconciled to source-side counts and a verification sample of not less than [n] per cent re-checked against source, reported in the Collection Report."

SUGGESTED WORDING · DRD / CORRESPONDENCE DESCRIPTION

"Collection was undertaken on a targeted basis by [provider] using forensic, metadata-preserving methods: the custodians, sources and date ranges collected, and the derivation of that scope from the issues, are recorded in the collection protocol, available for inspection. Devices assessed as contested or deletion-sensitive were additionally imaged and preserved unexamined. Manifests, hash schedules and verification sampling support the completeness of the collection within its stated criteria, and the criteria remain under review as the matter develops."

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

The targeted-collection checklist

- ☐ Criteria derived from issues, data map and custodian interviews, recorded with rationale and exclusions
- ☐ Containers preferred over content filters; scope one size up from the minimum; date anchors and margins stated
- ☐ Method held forensic: metadata-preserving tools, hashes, logs, custody, unchanged by the narrower scope
- ☐ Backstop list drawn: contested, deletion-sensitive and leaver sources imaged or held in full
- ☐ Manifests reconciled to source counts; verification sample run and reported
- ☐ Protocol records the whole design; DRD summarises it; both stay consistent
- ☐ Criteria versioned and revisited as review learns; amendments logged
- ☐ Opponent's targeting tested on records (criteria, preservation, manifests), not on the fact of narrowing
- ☐ UK GDPR minimisation posture documented: what was not swept in, and why that was deliberate
- ☐ Budget model comparing broad-image versus targeted paths retained with the file

Red flags

- "We just took what looked relevant."
- Criteria that exist only in an email thread, or nowhere.
- IT copy-paste wearing the label "targeted collection".
- A contested device collected lightly and already reissued.
- Keyword-filtered acquisition of untested terms.
- No manifests, no counts, no sampling.
- A scope frozen in month one and never revisited by month twelve.

When to involve a digital forensic expert

At scope design, where the examiner's contribution is the risk register: which sources can be safely narrowed, which demand the backstop, what each path costs, and what the targeted tools will and will not capture from each system. At execution, to run the acquisition to the method disciplines and produce the manifests and sampling that make "complete within criteria" a demonstrable claim. And in challenge, both ways: defending your targeting with the records this guide requires, or testing an opponent's by asking for theirs: the CPR Part 35 report that says "on the disclosed criteria and manifests, the following cannot be established" is how narrowing without discipline is converted into weight.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Will a court criticise us for not imaging everything?

Not for narrowing; for narrowing badly. The disclosure regime expects proportionate scope, and a targeted collection with recorded criteria, forensic method, manifests and a preservation backstop is the compliant posture, not a concession. Criticism attaches to the other version: undocumented selection, degraded method, contested sources gone: which is a records failure wearing proportionality's clothes.

Is it safer to image everything if the client will pay?

Safer against the missed-source risk, yes; but it buys new exposure: cost that may be disallowed as disproportionate, months of delay, a data-protection posture that is hard to defend, and a review mountain that degrades accuracy. The optimum for most matters is the §8 pattern: broad preservation, narrow collection: which delivers full-image safety on the sources that need it at targeted-collection cost overall.

Can we use keyword filters to reduce what we collect?

Sparingly and late: prefer container-and-date scope at collection, and apply terms at processing where they can be tested, iterated and reported. Where collection-time filtering is genuinely required (a third party will only export matches; a court order specifies terms), treat the term set as a negotiated instrument, test it on a sample first, and record that families and near-misses outside the filter were never collected, so nobody later mistakes the boundary for the universe.

What if we discover mid-case that our criteria missed something?

Amend and collect: scope revision on new information is the system working, and the amendment trail is evidence of good faith rather than an admission. The cost turns on two earlier decisions: whether the source was preserved (backstop or organisational resilience), and whether the original criteria were recorded, so the miss reads as a reasoned boundary honestly revised rather than a hole in an undocumented net. Example 2 is the case study, costs consequence included.

How do we challenge an opponent whose "targeted collection" looks like cherry-picking?

Ask for the records this guide would have produced: criteria and rationale, protocol section, interview basis, exclusions, manifests, sampling, preservation position. Cherry-picking and principled targeting are indistinguishable from outside and completely distinguishable on paper; a party that cannot produce the paper has answered the question. Frame relief accordingly: specific disclosure of the excluded categories, or collection from the preserved layer their answers reveal (or reveal to be missing).

Does targeted collection satisfy our preservation duty by itself?

No: preservation and collection are different duties on different timetables. The hold and its suspension of deletion mechanisms cover the estate; collection then takes what the criteria select. Targeting the collection while the hold quietly lapses elsewhere is how the §5 blind spots become permanent; the protocol should state both layers, and the DRD's preservation section should describe the hold, not the collection, as the answer to "what has been preserved?".

§ 1 4 · REFERENCE

Glossary

Backstop (sequestration)

Full imaging or hold of a source, preserved unexamined, behind a targeted collection from it.

Container scoping

Selecting mailboxes, folders, sites, channels and date ranges rather than keyword-filtered content.

Criteria table

The recorded mapping of issues to custodians, sources, ranges and exclusions, with rationale.

Data map

The inventory of systems and locations from which scope is reasoned.

Manifest

The per-source record of items collected: paths, counts, sizes, hashes, reconciled to source.

Minimisation

The UK GDPR duty to process no more personal data than the purpose requires; targeting operationalises it.

Sampling verification

Re-checking a proportion of collected items against source to catch silent execution errors.

Scope amendment

The logged revision of criteria as the matter learns; evidence of engagement, not error.

Targeted collection

Forensic acquisition of a defined subset of an estate, method undiminished.

Triage by guesswork

Selection without pedigree, records or backstop; the indefensible twin.

Sources and authoritative references

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

- cflab.uk, digital forensics services (targeted and full-image collection, sequestration, manifest and verification deliverables): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 01 · Identification and Phase 03 · Collection (scope as the first cost control: "you pay for substance, not volume"; a documented 71 per cent volume reduction case note): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- CPR Part 31 / PD 31B and PD 57AD with the Disclosure Review Document (reasonableness, proportionality and scoped collection): justice.gov.uk, [Part 31](https://justice.gov.uk) · justice.gov.uk, [PD 57AD](https://justice.gov.uk)
- NPCC / College of Policing digital evidence guidance: college.police.uk, [digital devices guidance](https://college.police.uk) · ISO/IEC 27037:2012: iso.org, [27037](https://iso.org)
- ICO, UK GDPR guidance including data minimisation: ico.org.uk · CPR Part 35: justice.gov.uk, [Part 35](https://justice.gov.uk)

DISCLAIMER

This publication provides general information about targeted collection in the United Kingdom as at August 2026. The clause wording is illustrative and the worked examples are fictional. Scope decisions are matter-specific; obtain advice on the facts. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice from a qualified lawyer or a suitably qualified forensic practitioner. Rules, standards and guidance change; always check the current text. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Targeted collection is where our forensic and eDiscovery practices meet. We design criteria with your team from interviews and the data map, write the risk register that says which sources can be narrowed and which get the backstop, and execute the acquisition with metadata-preserving tools, manifests, hashes and sampling: narrow in scope, undiminished in method. Sequestration is a standing service: contested devices imaged, sealed and stored unexamined at storage-only cost, waiting for the limb the matter may grow. Through **e-discovery.uk**, scope design runs as the pipeline's first cost control, so you pay for substance rather than volume, and the DRD describes an exercise that was engineered rather than improvised. In challenge, we defend targeting with records and test opponents' targeting by asking for theirs, under CPR Part 35 where the matter warrants. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.



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