COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Should Backup Systems Be Searched for Disclosure?

Preservation, Proportionality and the Cases Where the Backup Is the Only Copy Left

Backup systems occupy an awkward seat in disclosure: routinely excluded as disproportionate, yet repeatedly the only place a deleted mailbox, a departed custodian's files or a pre-dispute state of a system still exists. English procedure neither compels nor forbids searching them: it asks whether it is reasonable and proportionate on the facts, and it separately demands they be preserved while that question is decided. This guide gives lawyers the working framework: when backups must be preserved, when they should actually be searched or restored, how modern backup technology has quietly demolished the old "restoring tapes is ruinous" assumptions, what the Disclosure Review Document expects you to say about them, and how to argue the point: for access or against it: with technical accuracy.

⏱ 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. Backup work runs through both sides of the practice: targeted restorations that resurrect deleted custodians and systems for litigation, and proportionality evidence: sometimes for access, sometimes against: filed in support of DRD positions and specific disclosure applications. Its eDiscovery arm, **e-discovery.uk**, integrates restored material into disclosure-scale processing and review.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | BACKUP RESTORATION & RECOVERY | PD 57AD / DRD SUPPORT | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: PRESERVATION IS NEAR-AUTOMATIC; SEARCHING IS A REASONED, EVIDENCED CHOICE

Two questions hide inside "should we deal with backups?", and English procedure answers them differently. **Preservation:** once litigation is contemplated, the duty to preserve extends to backup media where they may hold relevant material not available elsewhere: which, concretely, means suspending recycling and overwrite schedules for in-scope periods (the routine destruction that PD 57AD's preservation duty expressly targets), documenting what exists, and telling the other side what has been done. This is cheap, immediate and near-universal: almost never the battleground. **Searching:** whether preserved backups are actually restored and reviewed is a reasonableness and proportionality question under PD 31B / PD 57AD, resolved through the DRD's machinery: and its answer has shifted with the technology. The old default ("backup tapes are a last resort") grew from a world of offsite tape rotations where restoration meant hardware archaeology at five figures per tape. Modern estates run disk- and cloud-based platforms with searchable catalogues and granular restore: a single mailbox from a nightly job in hours, not weeks: so blanket disproportionality assertions increasingly misdescribe the facts, and courts pressed with accurate technical evidence increasingly order targeted restoration. The working rule this guide defends: backups are searched when they are the **only remaining source** of material that matters (deleted custodians, purged mailboxes, pre-dispute system states, guide 45's rolled-back intervals) and the restoration can be targeted; they are left preserved-but-unsearched when live systems already cover the ground; and either position is taken in the DRD on described evidence: what platform, what catalogue, what granularity, what cost: not on folklore.

- **Day one: stop the recycling.** The preservation email (guides 43-46's, one layer down) suspends overwrite and retention-pruning for in-scope generations, and asks for the catalogue: the index of what exists, restorable without restoring anything.
- **The catalogue is the cheap first search:** modern platforms list jobs, sources, dates and often item-level content without restoration: the proportionality argument's factual foundation, obtainable in a day.
- **"Only remaining source" is the trigger:** the departed custodian whose laptop was reissued, the mailbox purged past its recycle window, the system as it stood before the amendment: backup questions become search obligations where nothing else holds the answer.
- **Target, never trawl:** restoration is scoped to custodians, systems and dates: guide 37's dial: and restored material flows into the ordinary processing, deduplication and review pipeline.
- **Legacy media are the true cost cases:** orphaned tapes without their software, formats without hardware: real disproportionality lives here, argued with a laboratory's assessment rather than an assertion.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the archive everyone hopes to ignore

Every disclosure exercise reaches the same conversation. Someone says the word "backups"; the client's IT contact sighs; a number with many zeros is floated; and both parties quietly agree that PD 31B lets them look away. Often that instinct is right: the live estate holds everything the backups hold, more accessibly, and restoring nightly copies of it would duplicate cost for nothing. But the instinct fails, expensively, in a recurring set of cases: the key custodian left eighteen months ago and their mailbox followed the leaver process into deletion; the file share was migrated and the old structure discarded; the database was "tidied"; the VM was rolled back (guide 45) or the NAS reset (guide 44). In each, the backup layer is not a duplicate: it is the last copy on earth: and a party that recycled it after the duty arose has converted a storage economy into a spoliation problem.

The discipline is therefore sequenced: preserve reflexively, catalogue cheaply, and decide the search question deliberately, on facts about this estate's platform and this case's gaps: with the DRD as the venue and, where parties disagree, technical evidence rather than adjectives as the currency. This guide equips each step.

§ 0 3 · THE BASELINE

Preserve first, argue later: the legal baseline

- **The preservation duty reaches backups:** PD 57AD requires parties to preserve documents that might otherwise be deleted or destroyed under routine processes: backup recycling is the paradigm routine process: and to notify relevant employees and former employees. Comparable expectations operate under CPR 31 / PD 31B for cases outside the B&PCs. The practical translation: suspend overwrite for in-scope periods, hold generations that bracket key dates, and record the instruction and its confirmations.
- **Suspension is bounded, not eternal:** the hold covers relevant periods and sources, defined as tightly as honesty allows; a proportionate hold letter that names systems and dates beats an unbounded "preserve all backups" that invites both cost complaints and quiet non-compliance.
- **Disclosure duties then bite on what exists:** preserved backups are documents within a party's control; whether they must be *searched* is governed by the reasonableness factors (PD 31B's accessibility and cost factors; PD 57AD's proportionality machinery through the DRD), and whether specific restoration is ordered on application turns on the same balance with the requesting party's need in the scale.
- **Transparency is the safe harbour:** the DRD asks parties to describe backup sources and state their position on searching them. A described, reasoned exclusion survives scrutiny; a silent one, discovered later, reads as concealment: and the court's sympathy moves accordingly.
- **UK GDPR pulls the same direction as proportionality:** restoring wide historical data engages data-minimisation; targeted restoration with filtered processing is both the procedural and the data-protection answer, per this series' standing approach.

§ 0 4 · KNOW YOUR ESTATE

Know what you actually have: backup technology in 2026

GENERATION	WHAT IT LOOKS LIKE, AND WHAT RESTORATION REALLY COSTS
Modern platform (disk/ cloud)	Veeam-class software, cloud-workload backup, M365/Google native retention layers: searchable catalogues, item-level restore (a mailbox, a folder, a VM) in hours, restore-to-alternate-location as standard. Restoration cost: modest and estimable; "disproportionate" needs actual numbers to survive.
Structured tape library (current)	Managed tape with live catalogue and compatible hardware: slower and sequential, but indexed: targeted restores are routine operations, priced per tape-set and per system, not per miracle.
Legacy / orphaned media	Tapes outliving their software or hardware, formats from departed vendors, unlabelled boxes from an acquisition: restoration means environment reconstruction or specialist migration: the genuinely expensive tier, where disproportionality arguments are honest and a laboratory assessment (what exists, sample-read results, realistic cost bands) is the evidence that wins them.
Ad hoc copies	USB rotations, replica NAS units, "the old server in the cupboard": cheap to image and often evidentially rich: guides 44 and 48 territory, not really "backup systems" at all for cost purposes, and rarely a legitimate exclusion.

The single most consequential fact-finding step is identifying which tier your client (or your opponent) actually operates: the entire proportionality argument inherits from it.

§ 0 5 · THE DECISION

When backups should be searched: the decision framework

- **Search when the backup is the only source:** departed custodians past their leaver-deletion, purged mailboxes and chats beyond recycle windows, decommissioned or migrated systems, pre-dispute states where tampering or deletion is alleged (the guide 43-45 patterns), and the "missing period" a rollback or clean-up created. Here restoration is not an alternative to searching live systems: it is the search.
- **Search when versions-over-time are the issue:** backdating, document-evolution and altered-record cases where generational states (the file as at each month-end) are themselves the probative material: backups as a history layer, per the snapshots guide ahead.
- **Preserve but do not search when duplication is real:** live mailboxes and shares intact, custodians present, no deletion in issue: nightly copies of the same estate add cost, not documents; the DRD says so in a sentence, with the catalogue's description behind it.
- **Interrogate before excluding on cost:** the tier table above; a catalogue query and a sample restore convert guesses into numbers, and a scoped estimate ("custodian X's mailbox from the four quarter-end sets: two laboratory days") repeatedly turns "impossible" into "Tuesday".
- **Weigh the case's asymmetries:** what the material could prove, whether the requesting party can obtain it anywhere else, and who created the gap the backup would fill: a party whose own deletion (routine or otherwise) made the backup the only source argues its inaccessibility from a weak seat.

§ 0 6 · DOING IT WELL

Doing it well: targeted restoration methodology

- **Catalogue first:** export the index: jobs, sources, dates, item listings where available: and pick generations strategically: brackets around key dates, quarter-ends for evolution questions, the last set before a deletion.
- **Restore to a controlled environment:** never onto production; restored systems and mailboxes land in an isolated store or laboratory environment, hashed and logged, per guide 36's protocol disciplines: the restoration is a collection, and inherits collection's defensibility rules.
- **Preserve the metadata through the pipeline:** restoration method affects timestamps and structures; the examiner selects methods that keep original metadata (or records the mapping where the platform alters it), because the restored document's provenance will be challenged exactly like any other.
- **Deduplicate against the live collection:** restored generations overlap live data heavily; processing dedupes across them (per the processing guides ahead) so review sees the deltas: the deleted, the changed, the versions: not thousands of identical copies.
- **Document the choices:** which sets, why those, what was not restored and why: the guide 37 record, ready for the DRD, the opponent and, if it comes to it, the application.

§ 0 7 · THE ARGUMENT

Arguing the point: for access, and against it

- **Seeking restoration:** plead the gap (what is missing from live disclosure and why the backup uniquely fills it), the feasibility (their platform tier, catalogue evidence, a laboratory's scoped estimate: obtained if necessary by asking targeted DRD questions about the backup environment), and the offer (narrow custodians and dates, costs proposals where tactically wise). Courts respond to requests that sound like engineering, not fishing.
- **Resisting restoration:** evidence the duplication (live sources already searched cover the period), the tier (legacy-media assessments with sample results and cost bands), and the proportionality arithmetic against the issues: while conspicuously preserving, because "we resisted searching" is a position and "we recycled" is a problem.
- **Either way, describe accurately:** the recurring judicial irritant is discovering that "inaccessible archive tapes" were a modern platform with a search box. Technical accuracy in the DRD is both duty and strategy: the party caught overstating burden spends the rest of the case being disbelieved.
- **Expert evidence decides close calls:** a short CPR 35-compliant statement on platform capabilities, restoration scope and cost converts the hearing from adjective-trading into fact-finding: and is as available against an opponent's inflated estimate as in support of your own.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never treat "the backups" as a single object, and never assume the backup layer is the only fallback. The material a restoration would recover often coexists in: live systems' own recycle and retention layers (deleted-item retention, litigation holds, version histories); server and NAS snapshots (guides 43-44); replication targets and DR environments (whole secondary estates, often forgotten in disclosure); archive platforms (journaling and compliance archives, which are indexed and cheap to search: frequently the better first stop for mail); counterpart custodians' copies (the same email in twelve other mailboxes); endpoint copies (sync clients, local OSTs); and cloud-tenant retention (M365/Google holds and recoverable stores, per the cloud guides ahead). Conversely, when everything live is gone, the backup catalogue plus generations is the recovery plan. The DRD conversation should place backups within this map rather than debating them in a vacuum.

EVIDENCE	LIVE SYSTEM + RECYCLE LAYERS	SNAPSHOTS / REPLICAS	BACKUP GENERATIONS	ARCHIVE / JOURNALING	COUNTERPART COPIES	DELETED / RECOVERABLE
Departed custodian's mailbox	Only within retention windows	Sometimes	Y: the classic case	Y where journaling ran	Partially (their sent mail elsewhere)	Varies with schedules
Deleted files / folders	Recycle + versions: short reach	Y within retention	Y across generations	n/a	Possibly	Guide 43-44 methods
Pre-dispute system states	n/a	Short-range	Y: the deep reach	n/a	n/a	Generation-dependent
Document version evolution	Version history where enabled	Y, dense but short	Y, sparse but long	Sometimes	Draft copies in mail	Varies
Proof of deletion timing	Audit logs where enabled	Bracketing states	Bracketing generations	n/a	n/a	Inferential

Fallback strategy in one line: before restoring anything, sweep the cheaper layers (retention stores, archives, snapshots, counterpart copies); before conceding anything is gone, check the catalogue: the answer to "is it anywhere?" is a map, and backups are its deepest, slowest shelf.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE LEAVER PROCESS AND THE QUARTER-END TAPES

A director central to a warranty claim had left the seller two years before proceedings; the leaver process had deleted his mailbox on schedule, months before any duty arose: no spoliation, but a hole where the key custodian should be. The seller's DRD initially wrote backups off as "archived tape, disproportionate". Targeted questions established a managed library with a live catalogue; the catalogue listed his mailbox in every quarter-end set across his tenure; and a consented sample restore of one set took the laboratory a day. The court-approved compromise restored four quarter-end generations: eleven thousand unique documents after deduplication, including the email chain the claim turned on. Cost: a fraction of the hearing that avoiding it would have produced.

EXAMPLE 2 · THE HOLD THAT NEVER REACHED THE ROTATION

A defendant's solicitors issued a competent preservation notice to custodians: and nobody told the infrastructure team, whose fourteen-day NAS-to-USB rotation kept overwriting through six months of pre-action correspondence. When restoration was eventually ordered, the surviving sets began after the critical window. The gap was unbridgeable and its cause discoverable: the hold's distribution list became an exhibit, cross-examination of the IT manager established the rotation was never suspended, and the trial judge directed that the missing period be approached on adverse inferences. The documents were never seen; their absence, and its administrative cause, ran through the judgment. One additional email recipient would have prevented all of it.

EXAMPLE 3 · THE "RUINOUS" RESTORATION REPRICED

A claimant sought restoration of two years of nightly backups of an entire estate; the defendant's evidence priced compliance in six figures and the request looked doomed. Instructed for the claimant, the laboratory reframed both halves: the demand was cut to one system's month-end sets across eight months (the document-evolution question needed generations, not nights), and the defendant's own platform documentation: a modern disk-based product with granular restore: contradicted its cost evidence, which had been built on tape-era assumptions by a witness who had not checked. The order followed the reframed request; the restoration took four laboratory days; and the costs of the resistance were addressed separately, with the judge's observations on accuracy in disclosure statements attached.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The hold that misses infrastructure:** Example 2's rotation: custodian notices sent, schedules never suspended.
- **Folklore in the DRD:** tape-era cost assumptions asserted about disk-era platforms: Example 3's repricing, waiting to happen.
- **Trawl-shaped requests:** "all backups for all systems" inviting refusal where four generations would have won.
- **Restoring without dedupe strategy:** review drowned in identical nightly copies of unchanged data.
- **Restoring onto production:** overwriting live data, or contaminating the restored evidence: both, occasionally, at once.
- **Backups silently omitted from the DRD:** the described-and-reasoned exclusion abandoned for hoping nobody asks.
- **The catalogue never requested:** months of argument about what tapes "might" hold, answerable by an index export in an afternoon.
- **Cheaper layers unswept:** a restoration ordered for mail sitting in the journaling archive all along.

Technical limitations

- **Backups hold what jobs captured:** excluded paths, failed jobs and unbacked systems leave real gaps; the job history and failure logs define the ceiling, and the report states it.
- **Granularity is generational:** nightly sets show daily states, not the intra-day sequence; deletion timing brackets between generations rather than pinpointing.
- **Restoration can alter metadata:** platform-dependent; managed by method selection and mapping records, but a restored file is one step from its original and the report says so.
- **Encryption keys age:** encrypted backup sets need their keys; key rotation and departed administrators make old sets a credential hunt (guide 33) before they are a restoration.
- **Legacy media genuinely fail:** tape degradation and extinct formats defeat some recoveries at any price: the honest assessment, sampled and evidenced, is itself the proportionality answer.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What backup platform(s) run today, and what did the estate use across the relevant period: including before any migration?
- What are the retention and rotation schedules, and who can suspend them this afternoon?
- Can we have the catalogue export for [systems/custodians/period], and the job-failure history with it?

Ask your opponent

- Please identify each backup system and archive operated in [period]: platform, media, retention, catalogue availability: and confirm recycling has been suspended for in-scope periods, stating the date of suspension.
- Please state whether [custodian/system] appears in your backup catalogues and, if so, the generations held.
- Where you assert that restoration is disproportionate, please provide the platform, the basis of the cost estimate, and whether a sample restoration has been performed.

Ask your eDiscovery / forensic provider

- From the catalogue, which generations answer our questions, and what is the scoped restoration estimate?
- How will restored material be collected, deduplicated and integrated with the live corpus?
- Will you provide a short Part 35 statement on feasibility and cost: ours, or in answer to theirs?

SUGGESTED WORDING · BACKUP LIMB FOR THE DAY-ONE PRESERVATION NOTICE

> "Your preservation obligations extend to backup and archive systems. With immediate effect, please: (1) suspend all recycling, overwriting and retention-based deletion of backup media and sets covering [systems] for [period], including offsite, cloud and replica copies; (2) preserve backup catalogues, job logs and failure records for the same scope; (3) confirm in writing the date and manner of suspension and the schedules previously in force; and (4) ensure this instruction reaches the personnel and any third-party providers who operate the relevant systems, not only document custodians. No restoration is requested at this stage; preservation of the media and catalogues is."

§ 12 · QUICK CONTROL

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

The backups-in-disclosure checklist

- ☐ Day-one notice includes the backup limb; infrastructure and providers on the distribution list
- ☐ Suspension confirmed in writing, schedules documented, confirmations filed
- ☐ Estate tiered: platform generation identified for every backup source in the period
- ☐ Catalogues exported and read before positions are taken
- ☐ Cheaper layers swept first: retention stores, archives, snapshots, counterpart copies
- ☐ Search decision made on the only-remaining-source test and recorded with reasons
- ☐ DRD describes backup sources accurately and states the position on searching
- ☐ Restorations targeted by generation and scope; restored to controlled environments; metadata handling recorded
- ☐ Restored material deduplicated into the corpus; deltas surfaced for review
- ☐ Contested points supported by scoped, sampled, Part 35-compliant evidence

Red flags

- A preservation notice with no backup limb.
- "The tapes would cost a fortune" from someone who has not named the platform.
- Rotation still running weeks into the dispute.
- Backups absent from the DRD entirely.
- A leaver-deleted key custodian and no catalogue question asked.
- Cost evidence unaccompanied by any sample restoration.
- An opponent's "inaccessible archive" that turns out to have a search box.

When to involve a digital forensic expert

At the hold, to make sure the suspension instruction reaches (and is technically apt for) the systems that matter; at tiering, where reading a backup estate accurately is an afternoon for a specialist and a hazard for anyone else; at the DRD, for the catalogue analysis and scoped estimates that let you take: or attack: positions with numbers; at restoration, which is collection work with collection's defensibility rules; and at any hearing where feasibility or cost is contested, with the short Part 35 statement that Examples 1 and 3 turned on. The recurring pattern across this guide's casework is that accurate technical facts, obtained early and cheaply, decide the backup question before it becomes expensive: the laboratory's role is supplying them.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Do we have to preserve every backup we hold, forever?

No: the duty is bounded by relevance and reasonableness: suspend recycling for the systems and periods the issues touch, hold the generations that bracket the key dates, and document the bounds you chose and why. An unbounded freeze is neither required nor wise; a reasoned, notified, recorded suspension is the standard the court will actually test you against.

Are backups "disclosable documents"?

The material on them is: backup copies of documents within your control are within your control, and the DRD expects them described. Whether they must be searched is the separate proportionality question this guide frames: and describing them accurately while declining to search, with reasons, is a legitimate and commonly correct position. Silence about them is neither.

Our key custodian's mailbox was deleted before the dispute. Is that spoliation?

Routine deletion before any preservation duty arose is not spoliation: leaver processes are lawful housekeeping. The consequences are practical: the backup and archive layers become the custodian's only remains, the catalogue question becomes urgent (retention there is also finite), and if generations exist, the only-remaining-source test points firmly at restoration. Deletion *after* the duty arose is a different conversation, and Example 2 shows where it goes.

How much does targeted restoration actually cost now?

On modern platforms: typically laboratory days, not months: a mailbox or file-set from catalogued disk-based sets is hours-to-days including processing; a handful of generations for evolution questions, low single-digit days. Managed tape multiplies handling but stays estimable. The open-ended numbers belong to legacy and orphaned media, where honest assessment (sample reads, environment reconstruction scoping) is the product. Any figure offered without naming the platform tier is a guess wearing a suit.

Can we get access to the other side's backups directly?

Orders for restoration and disclosure of the results are the norm; direct access to an opponent's backup environment is rare and reserved for guide-32-style distrust scenarios, usually via an independent examiner under protocol rather than party access. The productive route is almost always: catalogue disclosure, targeted restoration by them (or an agreed neutral), and the output into ordinary disclosure: sought with the engineering specificity that Example 3's reframed request modelled.

Cloud services back everything up anyway, don't they?

Partially and differently: SaaS platforms run retention, recycle and version layers (excellent short-to-medium reach, per the cloud guides ahead) and providers keep their own resilience copies you generally cannot reach; many tenants add third-party backup products that behave like this guide's modern tier. The practical rule transfers intact: map the layers, read the retention windows, suspend what your side controls, and ask the catalogue question of whatever backup product the tenant runs: "it's in the cloud" is the beginning of the analysis, not its answer.

§ 14 · REFERENCE

Glossary

Catalogue
The backup platform's index of jobs, sources, dates and items; the cheap first search.

Generation
One backup set at one time; the unit restorations are scoped in.

Granular restore
Item-level recovery (a mailbox, a folder) without rebuilding whole systems.

Journaling archive
Compliance capture of mail at send/receipt; indexed, and often the better first stop.

Leaver process
Routine deletion of departed staff's data; lawful pre-duty, decisive for sourcing.

Only-remaining-source test
This guide's trigger: search backups where nothing else holds the material.

Orphaned media
Backup media outliving their software or hardware; the true-cost tier.

Recycling / rotation
Scheduled overwriting of backup media; the routine destruction holds must stop.

Restore-to-alternate
Restoration into a controlled environment, not production; the defensible route.

Sample restoration
A test restore evidencing feasibility and cost; the proportionality exhibit.

Sources and authoritative references

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

- cflab.uk, digital forensics services (backup restoration and recovery, legacy-media assessment, proportionality evidence, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation, Phase 03 · Collection and Phase 04 · Processing (restored generations deduplicated into review; "you pay for substance, not volume"): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- PD 57AD (preservation duties; DRD) and CPR Part 31 / PD 31B (reasonable search; accessibility factors): justice.gov.uk, PD 57AD · justice.gov.uk, PD 31B
- CPR Part 35: justice.gov.uk, Part 35 · ICO, UK GDPR guidance (data minimisation): ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Backup questions arrive at the laboratory in both directions: making restoration happen, and pricing whether it should. We tier estates and read catalogues in a day; draft the infrastructure-reaching hold limb; run sample restorations that convert proportionality arguments into numbers; execute targeted restorations to controlled environments with metadata handling recorded; assess legacy and orphaned media honestly, sample reads included; and file the short CPR Part 35 statements that decide contested feasibility: Example 3's repricing is standing work. Through **e-discovery.uk**, restored generations are deduplicated into the live corpus so review sees deltas, not noise. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a rotation is overwriting evidence while positions are being drafted, the suspension call comes first.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace