COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Microsoft Purview or Independent Forensic Collection?

Choosing the Right Collection Route for a Microsoft 365 Matter: and Defending the Choice Afterwards

Every Microsoft 365 disclosure exercise faces the same fork: collect through the tenant's own compliance machinery (Purview eDiscovery), or bring in an independent examiner with their own tooling and methods? The honest answer is that both are legitimate, each fails in predictable places, and the choice is driven by three questions: who is trusted, what structures must survive collection, and what will the output face downstream? This guide gives lawyers the decision in usable form: what Purview genuinely does well, where its export mechanics and index edges bite, what independent collection adds and costs, the hybrid patterns that dominate real practice, and the paper trail that makes whichever route you choose defensible at the CMC and beyond.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. It operates on both sides of this guide's fork: running Purview-based collections with managed export mechanics for cooperative matters, and acting as independent examiner: including under court appointment: where tenants, administrators or exports are contested. Its eDiscovery arm, **e-discovery.uk**, receives both routes' output into processing and review.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | PURVIEW & API COLLECTION | INDEPENDENT / COURT-APPOINTED EXAMINATION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01 Executive summary

02 The problem in plain English: the fork every M365 matter reaches

03 What Purview does well: and where it bites

04 What independent collection adds: and what it costs

05 The decision framework: trust, structures, downstream

06 Hybrid patterns that dominate real practice

07 Defending the choice: the record that survives the CMC

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

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: PURVIEW FOR SCOPE, INDEPENDENCE FOR TRUST, HYBRIDS FOR MOST REAL MATTERS

Purview eDiscovery is the tenant's built-in collection machinery: custodian-scoped search across workloads, integration with the holds guide 51 placed, and export with metadata reports: proportionate, fast and, for the ordinary cooperative disclosure exercise, entirely defensible. Its genuine limits sit in three places: **export mechanics** (format choices change metadata behaviour; conversation structures and complex Teams artefacts flatten; partially indexed items need deliberate handling rather than silence); **index edges** (search-based collection inherits the index's blind spots: encrypted attachments, exotic formats, corrupted items); and **operator trust** (Purview is operated by someone with tenant roles, and where the administrators, the IT provider or the organisation itself sit inside the circle of suspicion, self-collection through their own console carries exactly the credibility problem guide 32 names). Independent forensic collection answers the trust problem (an external examiner, scoped logged access, methods and records that do not depend on the party's own staff), and its API-based tooling answers several structural ones (version series, permission and sharing states, Teams structures collected with fidelity Purview's exports approximate). It costs specialist time and requires access governance: and it does not magically exceed the tenant's own retention reality: independence changes who collects and how faithfully, not what still exists. In practice most contested matters land on hybrids: Purview for the broad custodial corpus, independent collection for the contested custodians, the structural sources and the verification sampling: recorded, per guide 36, in a protocol that states which route ran where and why. The choice is rarely reversible cheaply; make it deliberately, in week two, on the three questions: **who is trusted, what structures must survive, what will the output face?**

- **Purview's core virtue is scope discipline:** custodian-and-date-bounded collection integrated with holds: the proportionality engine, and usually the right default for uncontested corpora.
- **Its exports are managed, not trusted blind:** format decisions, partially-indexed handling and metadata reports are collection decisions with review-stage consequences: made once, on the record.
- **Independence is about the operator, not the brand of tool:** the question is whether the party's own admins should be running the collection at all: guide 32's distrust factors transplanted to the cloud.
- **Structures are the quiet decider:** matters that turn on versions, permissions, sharing history or Teams architecture need collection that preserves those shapes: frequently the API route regardless of trust.
- **The record defends the route:** whichever way the fork goes, the protocol paragraph and the export manifest are what the CMC and the opposing expert actually examine.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the fork every M365 matter reaches

Once guide 51's holds are placed, someone must decide how the material actually leaves the tenant. The organisation's instinct is to use what it owns: Purview is licensed, IT knows the console, and the export button is right there. The litigator's instinct, in anything contested, is unease: the same IT team that reports to the same board whose conduct is in issue, running searches whose terms they can see, exporting through mechanics nobody in the room can explain, producing a corpus the other side is expected to take on faith. Both instincts are half right, and the resolution is not a slogan ("always independent!" is as wrong as "Purview is fine!") but a framework.

The framework's virtue is that it also prices the alternative honestly. Independent collection is not free: examiner time, access-governance overhead, scheduling: and in a cooperative matter about a modest custodial corpus it can be proportionality theatre. The cases that genuinely need it: conflicted administrators, structural evidence, court-appointed neutrality: need it completely, and hybrid designs let each part of a matter get the route it deserves. This guide is the fork, mapped.

§ 0 3 · THE HOUSE TOOLS

What Purview does well: and where it bites

- **Well: scoped custodial collection.** Custodians, sources, date ranges and terms defined in one place; holds honoured; iterative search refinement with statistics; export sized to the scope. For the bread-and-butter disclosure corpus, this is the proportionality machinery PD 57AD imagines.
- **Well: integration and speed.** No third-party access to arrange; collections launched in days; the audit layer logging the exercise itself: the defensible-by-default posture for cooperative matters.
- **Bites: export mechanics.** Export format choices carry metadata consequences (message formats, load-file behaviours, how conversation and attachment relationships are represented); Teams content exports as transcript-like records whose fidelity to the lived structure is approximate; and every export decision is effectively a processing decision made early: manage it with the review platform in mind, and keep the export configuration and metadata reports as exhibits.
- **Bites: the index's edges.** Search-based collection retrieves what the index reached: encrypted, corrupted and exotic items surface as "partially indexed" and are included, sampled or excluded by deliberate decision: silence here is the classic completeness challenge, cheaply avoided by enumerating and stating the handling.
- **Bites: the operator question.** Purview runs under tenant roles: fine where the organisation is a neutral custodian of its own data; structurally awkward where the operators, their managers or the organisation are adverse or suspected: not because the tool misbehaves, but because self-collection's credibility ceiling is real and arrives exactly when the stakes rise.

§ 0 4 · THE OUTSIDE EXAMINER

What independent collection adds: and what it costs

- **Adds: operator credibility.** An external examiner under instruction (or court appointment), accessing through scoped, time-bounded, logged roles, applying stated methods, producing manifests and a Part 35-ready record: the answer to every "who ran the search?" question before it is asked.
- **Adds: structural fidelity.** API-based collection can preserve what compliance export approximates: version series with authorship, permission and sharing states as data, Teams structures with their relationships, mailbox properties beyond message bodies: the difference between reviewing artefacts and reviewing a rendering of them.
- **Adds: verification capability.** Even where Purview runs the main corpus, an independent examiner can sample-verify it: re-collecting slices, comparing counts and hashes, checking the partially-indexed handling: assurance priced in days, not a parallel collection.
- **Costs: time and governance.** Access must be granted, scoped and supervised; specialist hours are real; scheduling adds days a Purview export would not: proportionate in contested matters, gratuitous in simple ones.
- **Does not add: data the tenant no longer holds.** Independence governs who collects and how faithfully: retention reality (guide 51's clocks) binds every route equally, and the architecture paths (guide 51 §8) remain the answer to genuine absence.

§ 0 5 · THE DECISION

The decision framework: trust, structures, downstream

- **Question 1 · Who is trusted?** Are the tenant's administrators (internal or outsourced) outside the circle of suspicion, and is the organisation a neutral custodian of the data in issue? Yes: Purview is available. No, or contested: the operator problem points independent, for the affected custodians at minimum. Court-ordered exercises against a hostile party point independent as a matter of course, usually under protocol.
- **Question 2 · What structures must survive?** Does the matter turn on message bodies and documents (Purview's comfortable ground), or on versions, permissions, sharing history, deletion patterns and Teams architecture (structural evidence wanting API fidelity)? Guides 53-57 flag the structure-heavy scenarios per workload.
- **Question 3 · What will the output face?** A cooperative exchange into an agreed review platform tolerates ordinary export mechanics, managed; a corpus destined for hostile expert scrutiny, authenticity challenges or criminal proceedings wants collection whose method survives that examination: which shifts the balance toward independent methods and fuller records even where trust is not in issue.
- **Score honestly, decide visibly:** the three answers, a route per source population, and a sentence of reasons each: the protocol paragraph that ends most arguments before they start.

§ 0 6 · HOW IT ACTUALLY GOES

Hybrid patterns that dominate real practice

- **Core-plus-contested:** Purview for the broad custodial corpus; independent collection for the accused executives' accounts, run first and separately: the commonest shape in internal-wrongdoing matters.
- **Corpus-plus-structures:** Purview for mail and documents; API collection for the version histories, sharing states and Teams structures the issues turn on: guide 50's differencing fed with faithful inputs.
- **Collect-plus-verify:** the party runs Purview under an agreed specification; the independent examiner verifies by sampling and countersigns the manifest: credibility at verification cost, common in agreed protocols.
- **Neutral-examiner:** guide 32's high-distrust posture: all tenant operations through a court-appointed or jointly instructed examiner, party admins stood down for the exercise: Example 3 of guide 51, done on purpose.
- **Whatever the pattern, one custody record:** routes may differ per population; manifests, hashes and the protocol's reasons unify them: the downstream platform receives one documented corpus, not two provenance mysteries.

§ 0 7 · THE PAPER

Defending the choice: the record that survives the CMC

- **The protocol paragraph:** route per population, the three-question reasoning, operator identities and roles, export configuration: guide 36's anatomy, cloud edition.
- **The export exhibits:** search specifications, statistics, partially-indexed enumeration and handling, export settings, metadata reports, manifests with hashes: the bundle that answers completeness challenges with documents instead of adjectives.
- **The access log:** who held which role, when, doing what: from the tenant's own audit layer: the independent examiner's scoped access proving itself, or the party operator's discipline doing likewise.
- **The verification note, where used:** sampling method, comparisons run, discrepancies and their resolution: short, technical, and disproportionately persuasive.
- **Symmetry in correspondence:** the same disclosures requested of the opponent: their route, operators, export settings and handling of index edges: because the fork this guide maps was also theirs, and their answers (or silence) are evidence too.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the route decision governs collection from the tenant, but the evidence estate is wider than the tenant, and route choice interacts with it. The populations this guide scopes coexist with: endpoints and sync caches (independent device forensics regardless of tenant route, per guide 51 §7); third-party tenant backups (collectable by either route's operator, per guide 49's methods); counterpart tenants (their route decisions, requestable in correspondence); the audit and sign-in exports (secured in week one whichever route follows); mobile devices (app data outside both Purview and Graph reach); and archive or journaling platforms running beside the tenant. When the chosen route cannot reach something: Purview's index edges, API scope limits, retention-expired content: the architecture supplies the alternate path, and the protocol records the reassignment rather than the gap.

EVIDENCE	PURVIEW ROUTE	INDEPENDENT / API ROUTE	ENDPOINT FORENSICS	THIRD-PARTY BACKUP	COUNTERPART TENANTS	DELETED / RECOVERABLE
Mail and documents (bodies)	Y: the comfortable ground	Y, with fuller properties	Caches, local copies	Y where deployed	External items: Y	Hold + window bound
Versions, permissions, sharing states	Approximated in exports	Y: the structural case	n/a	Point-in-time states	Shared-item states	Guide 50 layers
Teams structures	Transcript-like renderings	Y, with relationships	App caches: partial	Sometimes	Federated copies	Policy-bound; guide 56
Index-edge items (encrypted, exotic)	Enumerated, handled deliberately	Direct collection: often	Source copies on devices	Y	Their copies	Varies
Operator conduct during collection	Audit-logged party actions	Audit-logged examiner actions	n/a	n/a	Their audit layer	The log is the record

Fallback strategy in one line: route around the chosen route's edges deliberately: index-edge items to direct or device collection, structures to the API, absent content to backups and counterparts: with each reassignment written into the protocol as method, not confessed later as gap.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE SELF-COLLECTION THAT COULD NOT CARRY THE WEIGHT

A company defending a conspiracy claim ran its entire disclosure through Purview, operated by the IT manager: who reported to the COO, one of the alleged conspirators. The collection was probably competent; it did not matter. The claimant's expert asked the structural questions: who specified the searches, who could see the terms, what the export settings were, how partially indexed items were handled: and the answers ("the IT manager", "the COO approved the scope", "default", "what are those?") did the damage no missing document needed to. The court ordered re-collection of the three contested custodians by an independent examiner under protocol, with costs. Nothing sinister was ever found in the re-collected set: the first exercise had bought a five-figure do-over purely by having the wrong operator.

EXAMPLE 2 · THE STRUCTURES PURVIEW FLATTENED

An IP dispute turned on when a design document's key section appeared and who could access the folder at that date. The producing party's Purview export contained the document: current version, clean metadata report: and none of what mattered: the version series had flattened to the latest state, and permission history was not the export's business. Instructed jointly, the laboratory collected the same library via API: seventeen versions with authors and timestamps, the permission and sharing states as structured data, and the sharing-link creation that had exposed the folder externally two days before the rival filing. The route had been chosen for the corpus; the case lived in the structures: the hybrid (corpus by Purview, structures by API) is what the protocol should have said from the start, and eventually did.

EXAMPLE 3 · THE COUNTERSIGNED MANIFEST

In a shareholder dispute where trust was frayed but budgets mattered, the parties agreed the collect-plus-verify pattern: the company ran Purview to a jointly settled specification; the laboratory, as independent examiner, held read access to the case, sampled ten per cent of the export against direct re-collection, reconciled counts and hashes, tested the partially-indexed handling, and countersigned the manifest with a two-page verification note. Total independent cost: four days. When the claimant later alleged suppression of a named email thread, the answer was the note's sampling table and the audit log: the thread was in the export, reviewed and disclosed: and the allegation died in correspondence. The pattern had bought contested-matter credibility at cooperative-matter prices.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The default default:** Purview chosen by inertia, export settings untouched, in a matter whose contest level demanded better: Example 1's shape.
- **Independence as theatre:** examiner hours spent re-collecting an uncontested corpus a Purview export would have served: proportionality inverted.
- **Structures discovered late:** the version-and-permission case collected as bodies-only: Example 2, until the re-run.
- **Partially indexed silence:** the enumeration nobody read, the handling nobody decided, the completeness challenge nobody needed.
- **Export-format regret:** settings chosen without the review platform in mind; metadata behaviours discovered at load.
- **The unlogged operator:** collection run under broad roles with no access record: credibility spent for nothing.
- **Asymmetric curiosity:** your own route documented, the opponent's never asked about.

Technical limitations

- **Neither route defeats retention:** expired is expired; the architecture paths are the recourse.
- **API scope has edges too:** some artefacts and properties are export-only or console-only; the examiner maps reachability per workload rather than promising totality.
- **Platform change is constant:** export behaviours and API surfaces move on Microsoft's schedule; method statements verify current behaviour, and old protocols are not precedents for new mechanics.
- **Verification is sampling, not omniscience:** the countersigned manifest evidences process integrity at stated confidence: which is its honest, and sufficient, claim.
- **Licence tiers gate both routes:** hold scope, audit reach and some export features step with tier (guide 51): the route decision inherits the tenant you actually have.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Who operates the tenant day to day, and is any of them: or anyone they report to: within the circle of suspicion?
- Do the issues turn on content, or on versions, permissions, sharing and structures?
- What review platform will receive the output, and who will manage export mechanics for it?

Ask your opponent

- Please state the collection route(s) used or proposed for your M365 sources: operators and roles, tooling, search specifications, export settings: and provide the export metadata reports and manifests.
- Please state how partially indexed and unindexed items were identified and handled, with counts.
- Where collection was performed by your own personnel, please identify their reporting lines relative to the individuals whose conduct is in issue.

Ask your eDiscovery / forensic provider

- Run the three-question framework on our matter: what does it say, population by population?
- If Purview: what export configuration for our platform, and what is the partially-indexed plan?
- If hybrid or independent: what access do you need, how is it scoped and logged, and what does verification add for what cost?

SUGGESTED WORDING · PROTOCOL CLAUSE ON COLLECTION ROUTE (ADAPT)

> "Collection from the [party] Microsoft 365 tenant shall proceed as follows: (a) the custodial corpus at Schedule A shall be collected via Purview eDiscovery by [operator], under the search specification at Schedule B, with export configured per Schedule C and the export statistics, partially-indexed enumeration and handling decisions, metadata reports and hashed manifests preserved and exchanged; (b) the sources at Schedule D (including version histories, permission and sharing states, and Teams structures) shall be collected by [independent examiner] via API-based methods under scoped, time-bounded, logged access; (c) [independent examiner] shall verify the Schedule A export by sampling at [rate], countersigning the manifest and reporting discrepancies; and (d) no other access to, search of, or export from custodian content shall occur, all tenant operations for the exercise being logged and the logs preserved."

§ 12 · QUICK CONTROL

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

The route-decision checklist

- ☐ Three questions answered on paper: trust, structures, downstream
- ☐ Route assigned per source population, with reasons, in the protocol
- ☐ Operators named; roles scoped, time-bounded, logged
- ☐ Purview exports configured for the review platform; settings preserved as exhibits
- ☐ Partially indexed items enumerated and their handling decided and stated
- ☐ Structural sources routed to methods that preserve their shape
- ☐ Verification sampling agreed where the pattern warrants it
- ☐ Manifests, hashes and metadata reports exchanged both ways
- ☐ Opponent's route interrogated with the §11 questions; answers diarised
- ☐ Reassignments around route edges recorded as method, not discovered as gaps

Red flags

- Collection operated by someone reporting to a person whose conduct is in issue.
- "Default export settings" in a matter with metadata stakes.
- No answer to the partially-indexed question.
- A version-or-permissions case served with bodies-only exports.
- Independent-examiner demands in a matter with no trust issue and a modest corpus.
- An opponent who will not say who ran their searches.
- Tenant operations during the dispute outside the protocol's log.

When to involve a digital forensic expert

At the fork itself: the three-question framework is best run with someone who has operated both routes and knows where each bites on the current platform, not last year's. For Purview matters, at export configuration and partially-indexed handling: hours of specialist input that pre-empt the standard challenges. For hybrid and independent patterns, as the examiner: scoped access, structural collection, verification sampling, countersigned manifests: Examples 2 and 3's machinery. And at the CMC and beyond, for the short Part 35 statement that explains the route chosen and answers the one your opponent chose: because in M365 matters the collection method is now litigated nearly as often as the collection's contents.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is Purview collection "forensic"?

It is defensible when managed: scoped, logged, exported deliberately, manifested: and courts accept it routinely for ordinary disclosure. What it is not is independent of the tenant's operators or faithful to every structure: the two properties the word "forensic" is usually reaching for when the question gets asked. Match the label to the need: most matters need defensible; contested ones need independent or structural too, and that is a route decision, not a tooling insult.

Will the court order independent collection if we ask?

Where you can show the operator problem (conflicted admins, self-collection by implicated teams) or demonstrated defects (Example 1's answers, export irregularities), yes: targeted orders for independent re-collection or examiner-supervised exercises are familiar territory. A bare preference for distrust without grounds fares poorly against proportionality. Build the application the way §7 builds the defence: on the record of who did what, not on adjectives.

Can the two routes disagree about what exists?

They can differ at the edges: index-bound search versus direct enumeration, export renderings versus structural collection: which is precisely what verification sampling exists to surface and explain. Genuine content disagreement (an item one route finds and the other cannot) is rare and always informative: it points at index edges, timing, or conduct: and resolving it is exactly the examiner's job. The manifests make the comparison possible; run without them, disagreement is just fog.

We already exported everything to PSTs last year. Do we start over?

Not necessarily: assess before re-collecting. The questions: what the export captured and lost (settings, metadata report, manifest: if none exist, that is the first finding), whether the matter's issues touch what was lost, and whether the tenant still holds the sources for a better pass (holds and windows, per guide 51). Sometimes the old export serves with a supplementary structural collection; sometimes it is Example 1's do-over. An afternoon's expert assessment prices it before positions harden.

Does the choice differ for regulatory investigations or criminal matters?

The framework holds; the weights shift. Downstream scrutiny (question 3) is at its maximum: methods face expert challenge under CrimPR 19 or a regulator's own technical team: and operator independence is often effectively mandatory where the organisation's conduct is the subject. Expect independent or examiner-verified patterns as the norm, fuller method statements, and: in criminal work: the Forensic Science Regulator Code's declarations sitting over the exercise. The fork is the same; the tolerances are tighter.

What single sentence should go in every M365 protocol?

Name the operator and log the access: "All collection operations shall be performed by [named persons/ examiner] under scoped, time-bounded roles, with all tenant operations during the exercise logged and the logs preserved and disclosable." It costs nothing, it disciplines both sides, and it converts the commonest category of route dispute: who touched what, when: from allegation into lookup. Most of this guide is that sentence, expanded.

§ 14 · REFERENCE

Glossary

API collection
Graph-based programmatic collection preserving structures export approximates.

Collect-plus-verify
Party-run Purview under specification, examiner-sampled and countersigned.

Export configuration
Format and settings decisions with metadata consequences; exhibit them.

Index edge
Content the search index reached partially or not at all; enumerate and decide.

Independent examiner
External specialist collecting under scoped, logged access; the operator answer.

Manifest
The hashed inventory of what left the tenant; the comparison's foundation.

Operator problem
Self-collection by conflicted personnel; guide 32's distrust, cloud edition.

Partially indexed items
Purview's enumeration of index-edge content; handling is a decision.

Structural fidelity
Preservation of versions, permissions, sharing and relationships in collection.

Verification sampling
Independent re-collection of a slice to evidence process integrity.

Sources and authoritative references

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

- cflab.uk, digital forensics services (independent and court-appointed M365 collection, verification sampling, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection and Phase 04 · Processing (route design, export mechanics and manifest discipline; "defensibility is built, not retrofitted"): 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
- Microsoft Purview eDiscovery documentation: learn.microsoft.com, Purview eDiscovery · Microsoft Graph documentation: learn.microsoft.com, Graph
- PD 57AD and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · Forensic Science Regulator statutory Code: gov.uk/forensic-science-regulator
- ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about Microsoft 365 collection routes as at August 2026. Platform features, export behaviours and API surfaces change on Microsoft's schedule and vary by tenant and licence; verify current behaviour in the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The laboratory sits on both prongs of this guide's fork by design: Purview collections run to managed specifications with export mechanics and partially-indexed handling documented; API-based structural collection where versions, permissions and Teams architecture carry the case; independent and court-appointed examination under scoped, logged access where operators are conflicted; and the collect-plus-verify pattern: Example 3's countersigned manifest: where credibility must be bought at cooperative prices. Route advice comes first and is often the whole instruction: the three-question framework run on your matter in a scoping call. Reporting is CPR Part 35 throughout, with CrimPR 19 and FSR Code disciplines where proceedings demand them, and through **e-discovery.uk** either route's output lands in processing and review as one documented corpus. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

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