



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

Preparing a Forensic Collection Protocol

The Written Plan That Makes a Collection Defensible Before It Begins

A collection protocol is the written plan agreed before anyone touches a device: the scope, the sources, the custodians, the method per source, the handling of exclusions and privilege, the verification and custody arrangements, and who does what, when. It converts collection from a series of improvised decisions into a documented exercise that can be exchanged with opponents, annexed to orders, and defended two years later. This guide sets out the protocol's anatomy section by section, provides drafting language for each, and shows how a good protocol prevents the disputes that bad collections create.

© 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 draft and execute collection protocols weekly: single-device seizures, multi-site corporate collections, and court-ordered imaging exercises with independent supervising solicitors, each run to a written plan agreed in advance. Its eDiscovery arm, **e-discovery.uk**, holds that defensibility is built, not retrofitted; the collection protocol is where the building starts.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ISO 27001-ALIGNED SECURITY

ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES

PROTOCOL DRAFTING & EXECUTION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: collections without plans
03	What a protocol is, and when one is needed
04	The anatomy: section by section
05	Scope: custodians, sources, date ranges, method per source
06	Exclusions, privilege and personal data
07	Execution: sequence, roles, verification and custody
08	Contingencies and escalation triggers
09	Agreed and court-ordered protocols
10	Worked examples
11	Common mistakes and technical limitations
12	Questions to ask · Suggested wording
13	Checklist and red flags · When to involve a digital forensic expert
14	Frequently asked questions
15	Glossary · References · Disclaimer · How a specialist laboratory can assist

Executive summary

THE HEADLINE POINT: WRITE THE COLLECTION DOWN BEFORE IT HAPPENS

A forensic collection protocol is a short written document, agreed before collection begins, that answers every question the exercise will later be asked: **what** is being collected (custodians, sources, date ranges, data types), **how** (the method per source, from imaging to targeted export, with tools and standards), **what is not** (exclusions, privilege handling, personal-data boundaries), **by whom and in what order** (roles, sequence, site logistics), **with what proof** (hashing, logging, custody arrangements), and **what happens when reality intervenes** (contingencies for encryption, absent devices, failures, and escalation triggers for discoveries). Its value is double. Internally, it converts a stressful exercise into a checklist, so decisions are made once, calmly, by the right people, instead of repeatedly at machines by whoever is standing there. Externally, it is the defensibility instrument: exchanged with an opponent it forecloses methodology disputes; annexed to an order it becomes the measure of compliance; and produced two years later it is the contemporaneous answer to "why was it done this way?". A protocol takes hours to write and its absence takes months to litigate.

- **Proportionate to the matter:** two pages for a single-custodian employment dispute, a dozen for a multi-site fraud collection; the sections stay the same, the depth scales.
- **Drafted jointly:** lawyer (scope, privilege, legal basis), examiner (methods, contingencies, verification), client IT (access, systems, logistics): each section has an owner, and a protocol written by one discipline alone shows it.
- **Frozen, then versioned:** the protocol is dated and fixed before execution; changes during execution are amendments, logged with reasons, never silent drift.
- **The deviation log completes it:** the paired record of everything that departed from plan and why; a protocol executed with zero recorded deviations across a real estate is less credible, not more.
- **It is the DRD's raw material:** the methodology the Disclosure Review Document describes should be the protocol, summarised; writing the protocol first means the DRD is reporting rather than promising.

The problem in plain English: collections without plans

Unplanned collections fail in recognisable ways. The team arrives to find machines nobody listed and accounts nobody owns; the departing employee's phone is in a drawer nobody mentioned; someone decides at the desk to image this one and skip that one; privilege turns up mid-copy and is handled by improvisation; the client's IT lead makes scope calls under pressure; and six weeks later nobody can say why the finance share was collected but the operations share was not. Every one of those moments produces a decision, and every undocumented decision made at a machine becomes, in litigation, a decision made by nobody, for reasons nobody can state, at a time nobody recorded.

The protocol moves those decisions upstream, to a table with coffee on it, where the lawyer can weigh privilege before it is encountered, the examiner can plan for the encrypted laptop before standing at it, and the scope can be reasoned from the data map rather than the corridor. What remains for collection day is execution and the honest logging of surprises: the two things field teams are actually good at. The discipline is old and borrowed: surgeons and pilots write the plan and log the deviations, for the same reason: under pressure, people execute well and decide badly, and the paperwork remembers what the adrenaline will not.

§ 0 3 · DEFINITION

What a protocol is, and when one is needed

- **What it is:** a dated, versioned document, typically with schedules (custodian list, source list, method matrix), signed off by the instructing lawyer and the executing examiner, and, where the exercise is contested or court-ordered, agreed with the other side or annexed to the order.
- **Always, at some scale:** even a one-device collection deserves a one-page protocol: source, method, hashing, custody, contingency for encryption. The habit costs twenty minutes and standardises quality.
- **Formally, when:** multiple custodians or sites are involved; the collection will be described in a DRD or challenged by an opponent; the exercise executes a court order (search orders, imaging orders, delivery-up), where the protocol is the compliance instrument and an independent supervising solicitor may hold it; privilege or heavy personal data is expected in the sources; the client's own staff will perform parts under supervision (the hybrid model, which is only defensible with a written protocol to supervise against); or regulators, insurers or auditors will later ask how it was done.
- **What it is not:** a search-term protocol (that is a processing and review instrument, covered earlier in this series), though the two connect: the collection protocol delivers the verified sources on which terms later run.

§ 0 4 · THE SKELETON

The anatomy: section by section

SECTION	CONTENTS
1 · Purpose and authority	The matter, the legal basis (instruction, order, consent), the protocol's status and version, who approved it
2 · Scope	Custodians (Schedule A), sources (Schedule B), date ranges, data types in and out
3 · Method matrix	Per source: image / logical / targeted, tools and standards, per guide 32's tree, with the one-line rationale
4 · Exclusions and privilege	What is not collected; how privileged and personal material encountered is handled; review and quarantine routes
5 · Execution plan	Sequence, sites, dates, roles (examiner, IT, supervising lawyer), powered-on device handling per guide 33, communications and confidentiality on the day
6 · Verification and custody	Hashing standards, acquisition records, exhibit referencing, sealing, storage and transfer arrangements per guides 31 and 35
7 · Contingencies	Encryption without credentials, absent or failed devices, unexpected sources, refusals, live-system constraints: the pre-decided responses
8 · Escalation triggers	Discoveries that pause execution and refer back: suspected deletion, contested material, scope questions
9 · Deliverables and reporting	What the exercise produces: evidence schedule, hash schedule, deviation log, collection report, and to whom
10 · Amendment	How the protocol changes: written variation, logged, approved by the named owners

Scope: custodians, sources, date ranges, method per source

- **Custodians by name, tiered:** Schedule A lists each individual with their tier (collect now, preserve only) and the sources attached to them; derivation from interviews and the data map is referenced, so the list has a visible pedigree.
- **Sources by identity, not category:** "the finance share" is a category; "\\SRV02\\Finance and its archive sibling \\SRV02\\Finance_Old, per IT confirmation of [date]" is a source. Precision here is what prevents the silent miss that haunts targeted collection.
- **Date ranges per issue, stated with anchors,** and applied at collection only where safe: date-filtering at the point of collection saves volume but risks boundary errors, so the protocol states where ranges are applied (at collection, or preserved-in-full and filtered at processing) and why.
- **The method matrix is the protocol's heart:** one row per source: method, tool, who executes, expected volume, the rationale line, and the preservation position behind every light choice. It is guide 32's decision tree, frozen into a table the DRD can later quote.
- **Out-of-scope stated expressly:** personal devices not in issue, sources deferred pending triggers, systems preserved but not collected: naming what is excluded, with reasons, is what makes the inclusion list defensible rather than merely short.

Exclusions, privilege and personal data

- **Privilege is planned, not improvised:** the protocol states how potentially privileged material is handled: collected but quarantined for lawyer review before anyone else sees it; filtered by counsel-approved criteria (named advisers, domains) applied at processing; and, in adversarial executions (search orders, delivery-up), reviewed by the independent supervising solicitor under the order's machinery. The examiner's role is capture and quarantine, never privilege judgment.
- **Personal and private material:** collections sweep in the personal (family photographs on work laptops, personal webmail in browser caches, the BYOD phone's private life). The protocol states the minimisation posture (targeted scopes, exclusion of defined personal categories where severable), the handling rules for what is unavoidably captured (restricted access, no review beyond necessity, deletion routes), and the UK GDPR basis, which for litigation collection is typically legitimate interests or legal-claims necessity, documented rather than assumed.
- **Special categories and third parties:** health data, references to non-parties, and regulated material (client-confidential files at professional firms) get named handling rules; where a collection will foreseeably capture another organisation's confidential data, the protocol says what happens to it.
- **The quarantine mechanics:** a designated container, access limited to named lawyers, logged; releases from quarantine recorded with the decision and decider. Quarantine described in the protocol and evidenced in the logs is what turns "they hoovered up privileged material" into "privileged material was captured, sealed and never accessed, as the records show".

Execution: sequence, roles, verification and custody

- **Sequence by volatility and risk:** powered-on and contested devices first (guide 33's fleeting opportunities), leaver devices before reissue queues move, cloud exports scheduled around admin availability, bulk shares last. The order is printed, because on the day the order is the plan.
- **Roles named:** the examiner executes; client IT provides access and answers, and touches nothing evidential except under written supervision; the supervising lawyer decides scope and privilege questions live and owns amendments; a client contact handles people and rooms. One phone number for decisions, printed on page one.
- **Verification wired in:** the protocol states the hashing standard (dual, at acquisition), the acquisition-record and worksheet forms in use, and the exhibit-referencing scheme, so guides 31 and 34 happen by default rather than by memory.
- **Custody from the first exhibit:** seals, transfer forms and the evidence destination are named in advance; the courier is booked before the collection, not after it; and the day ends with a signed evidence schedule, not a car boot.
- **The day's own record:** a running log (times, machines, actions, surprises) kept as the work happens: it is the protocol's execution mirror, and with the deviation log it is what the collection report is written from.

Contingencies and escalation triggers

- **Contingencies are pre-decided responses** to the predictable frictions: the encrypted device without credentials (per guide 33: assess, hunt escrow, no password guessing, refer); the device that is absent, dead or failing (record, preserve what exists, image failing media by block-level methods); the source larger or different than mapped (collect to plan, log the delta, refer for scope decision); the custodian who refuses or is absent (record, do not force, refer to the lawyer whose problem consent is); the live system that cannot pause (the logical-plus-logs route, pre-approved).
- **Escalation triggers pause, not improvise:** discoveries that stop work on a source pending instructions: apparent deletion or wiping in progress; material suggesting criminality beyond the matter's scope; another party's privileged or heavily confidential material; anything the supervising lawyer should see before it is handled further. The trigger's response is always the same: stop, preserve the state, note the time, call the number on page one.
- **Why pre-deciding matters evidentially:** a contingency executed from the protocol is method; the same act improvised is judgment exercised by a technician at a keyboard, and will be cross-examined as such. The protocol converts the field team's hardest moments into its most defensible ones.

Agreed and court-ordered protocols

- **Agreed protocols between parties** arise where one side's expert collects from the other's systems (delivery-up compliance, agreed inspections, joint collections from third parties). The protocol then adds: confidentiality undertakings; what the collecting party may and may not view; the quarantine-and-review machinery for privilege; where the evidence is held pending review; and the reporting each side receives. Negotiating these terms in advance is cooperation at its most productive: the alternative is a dispute per decision.
- **Court-ordered executions** (search orders, imaging orders) invert the emphasis: the order and its standard machinery govern, the supervising solicitor holds the ring, and the protocol is the technical schedule the order incorporates: sources, methods, sealing, and the strict rule that imaged material is preserved unexamined pending the return date or the order's review process. The examiner's independence and the completeness of the execution record carry particular weight, because the exercise will be scrutinised at the return hearing by a respondent with every incentive to find fault.
- **In both cases, the protocol is the compliance measure:** what was done is checked against what was written, so the drafting discipline (precise sources, workable contingencies, honest method statements) is not bureaucracy but self-protection.

Worked examples

EXAMPLE 1 · THE CORRIDOR DECISION

A collection team, sent without a protocol to "get everything relevant" from a subsidiary, encountered a shared drive twice the expected size and, pressed for time, took "the folders that looked relevant": a decision made by a technician, in a corridor, on filenames. Eight months later the excluded folders turned out to hold the disputed costing models; the other side's expert established the selective copy from the collection tool's own logs; and the technician's witness statement ("I used my judgment") did the damage its sentence suggests. A protocol with the standard contingency (collect to plan, log the delta, refer) would have surfaced the question to the supervising lawyer the same hour, and the eventual explanation would have had a decision-maker, a reason and a time.

EXAMPLE 2 · THE PROTOCOL ANNEXED TO THE ORDER

On an imaging order against a former director, the applicant's draft annexed a four-page protocol: named devices and accounts; imaging by an independent examiner; dual hashing; sealed storage with the supervising solicitor; no examination pending the return date; privilege quarantine machinery; and contingencies for encryption and absent devices. At the return hearing the respondent attacked execution on five fronts; each was answered by reading the protocol beside the execution log, which matched, deviation log included (one absent phone, recorded and pursued by correspondence). The judge described the exercise as "a model of how these orders should be implemented", and the substantive application proceeded on the imaged material without further continuity argument. The protocol had been drafted in an afternoon.

EXAMPLE 3 · THE HYBRID THAT STAYED DEFENSIBLE

A cost-conscious client wanted its own IT team to perform mailbox exports across forty custodians. The laboratory agreed, on protocol: written per-source method (the exact export mechanism, settings and naming), examiner-run training and a supervised first batch, hashes computed on export by provided tooling, a manifest per custodian, spot re-collection of a five per cent sample by the examiner for verification, and all deviations logged to the examiner daily. When the opponent later probed the in-house collection, the answer was the protocol, the manifests, the matching sample re-collections and the deviation log: a supervised method, verified, at a third of the cost of full external collection: which is the only version of the hybrid model that survives contact with a competent challenge.

Common mistakes and technical limitations

Common mistakes

- **No protocol**, and its cousin: a protocol written after the collection, which is a report wearing a plan's clothes.
- **Category scope**: "relevant shares and devices" instead of named sources; the silent-miss generator.
- **Single-author drafting**: the lawyer's protocol with impossible methods, or the examiner's with no privilege machinery.
- **No contingencies**, so the field team improvises exactly the decisions the document existed to pre-make.
- **Silent drift**: scope and method changed on the day without amendment entries; the plan and the execution diverge, and the divergence is discovered in cross.
- **The empty deviation log** presented as perfection; real estates produce surprises, and their absence from the record reads as non-recording.
- **Client IT unsupervised**: hybrid collection without the training, tooling, sampling and daily reporting that make it defensible.
- **The protocol never exchanged**: a methodology dispute litigated later that a two-page enclosure would have foreclosed.

Technical limitations

- **Protocols bind process, not estates**: the best plan cannot collect the source nobody disclosed; scope quality inherits the data-mapping and interview work upstream of it.
- **Precision ages**: systems migrate and custodians move between drafting and execution; the protocol carries a verification step (IT confirmation of sources within [n] days of execution) or it executes against a stale map.
- **Pre-decision has limits**: genuinely novel discoveries still require judgment; the protocol's contribution is to route that judgment to the named decision-maker with the facts preserved, not to abolish it.
- **Paper does not execute itself**: a protocol without the execution log and deviation log beside it is a promise, and promises are cross-examined; the three documents are one instrument.

§ 1 2 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Who can verify, this week and in writing, the identity and location of each source on the draft schedule?
- Who is empowered to take scope and privilege decisions live on collection day, and are they actually reachable?
- If your IT team performs any part, will they work to our written method, with training, sampling and daily deviation reporting?

Ask your opponent

- Please provide the collection protocol (or equivalent methodology record) under which your disclosure was collected, with its deviation log.
- We enclose our draft protocol for the [agreed collection]; please confirm agreement or propose amendments by [date].
- Where your collection was performed in-house, please describe the supervision, verification and sampling applied.

Ask your eDiscovery / forensic provider

- Draft the protocol with us: which sections do you own, and what do you need from the client to freeze the method matrix?
- What are your standard contingencies and escalation triggers, and where have they been tested?
- What will the deliverable set contain (evidence schedule, hash schedule, deviation log, report), and when after execution?

SUGGESTED WORDING · PROTOCOL CORE CLAUSES (ADAPT)

"3. Method. Each source in Schedule B shall be acquired by the method specified against it in the Method Matrix, using the tools and settings there stated, by [examiner/provider]. Dual hash values (MD5 and SHA-256) shall be computed at acquisition and recorded in the acquisition worksheet; each exhibit shall be referenced, sealed and logged in accordance with Section 6. 7. Contingencies. If a source is encrypted and credentials are not available, the examiner shall proceed per Annex 2 (assessment, escrow enquiry, no credential guessing) and refer to [named lawyer]. If material appearing to be privileged is encountered, it shall be quarantined per Section 4 without further access. If any source materially differs from Schedule B, collection shall proceed to the Schedule and the difference referred the same day. 8. Escalation. On discovery of apparent deletion, wiping or concealment, work on the affected source shall pause, its state shall be preserved and photographed, and [named lawyer] shall be contacted before any further step. 10. Amendment. This protocol may be amended only in writing by [owners]; amendments and all deviations shall be recorded in the Deviation Log, which forms part of the collection record."

SUGGESTED WORDING · COVER LETTER EXCHANGING THE PROTOCOL

"We enclose the collection protocol under which our client's electronic sources will be collected, including the method matrix, verification and custody arrangements, and privilege machinery. It is provided so that methodology is transparent and any observations can be made before execution rather than after; absent comments by [date] we will proceed on its terms. The executed protocol, together with the deviation log and hash schedule, will be available for inspection on completion."

§ 13 · QUICK CONTROL

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

The protocol checklist

- ☐ Protocol drafted jointly (lawyer, examiner, IT), dated, versioned, approved before execution
- ☐ Custodians tiered and sources named with verified identities, not categories
- ☐ Method matrix complete: method, tool, executor, rationale and preservation position per source
- ☐ Exclusions stated with reasons; privilege quarantine and personal-data handling specified
- ☐ Execution sequence, roles and the decision phone number on page one
- ☐ Hashing, acquisition records, exhibit referencing and custody arrangements wired in
- ☐ Contingencies pre-decided; escalation triggers defined with the stop-preserve-call response
- ☐ Amendment route defined; deviation log opened with the protocol and kept live
- ☐ Deliverables specified: evidence schedule, hash schedule, deviation log, collection report
- ☐ Protocol exchanged or annexed where the exercise is agreed or ordered; executed record retained as one set

Red flags

- A collection scheduled with no written plan, or a plan written afterwards.
- "Relevant material" as a scope definition.
- A method matrix with blank rationale cells.
- No named decision-maker reachable on the day.
- A deviation log with nothing in it after a forty-source collection.
- In-house collection with no supervision, sampling or tooling.
- Execution that cannot be reconciled line-by-line with the protocol.

When to involve a digital forensic expert

At drafting, always: the method matrix, contingencies and verification sections are examiner's work, and a protocol without an examiner's hand is a wish list. At execution, for everything the matrix assigns to the laboratory and for supervision of anything assigned to IT. In two-party contexts, early: agreed protocols and court-order schedules are negotiated fastest between experts, and the supervising-solicitor machinery of imaging orders assumes an independent examiner exists to name. And retrospectively, when an opponent's collection arrives protocol-less: an examiner's review of what an unplanned collection cannot demonstrate (scope reasoning, contingency handling, verification) supplies the paragraphs that turn methodology into weight.

§ 1 4 · COMMON QUESTIONS

Frequently asked questions

Is a protocol really necessary for a small, single-device matter?

At one page, yes: source, method, hashing, custody, the encryption contingency, and who decides surprises. The habit standardises quality, the page takes twenty minutes, and small matters have a way of growing: the one-page protocol from month one reads very well in the witness box of month eighteen. What scales with matter size is the document's depth, never the existence of the discipline.

Should we show our collection protocol to the other side?

Usually, and often before execution: methodology is process-plane material (per this series' cooperation guide), exchanging it forecloses later disputes cheaply, and the cover letter's "observations before execution rather than after" framing shifts the burden of silence onto them. Hold back only genuinely strategic elements (which sources you consider contested, escalation reasoning that reveals theory), which belong in a privileged annex rather than the exchanged body.

What is the difference between the collection protocol and the DRD's methodology sections?

Sequence and status: the protocol is the operational instrument, written first, at full technical depth, and executed against; the DRD summarises it for the court at the level PD 57AD requires. Writing the protocol first means the DRD reports a designed exercise rather than promising an undesigned one, and when the DRD is questioned, the protocol and its execution record are the annexes that answer.

Can the client's IT team execute parts of the protocol to save cost?

Yes, under the hybrid conditions of Example 3: examiner-written per-source methods, training and a supervised first run, provided verification tooling, manifests, sample re-collection, and daily deviation reporting. Without those, in-house collection is the cheapest way to buy the most expensive problem; with them, it is a legitimate proportionality tool the protocol makes visible and defensible.

What happens when execution has to depart from the protocol?

It departs, in the open: the deviation is logged (what, why, who decided, when), material departures are made as amendments approved by the named owners, and the collection report reconciles plan against execution including every delta. Deviations are expected and survivable; drift is not: the difference is whether the departure has an entry, a decider and a reason, or is discovered by comparison two years later.

Who signs off the protocol, and does the client need to?

The instructing lawyer (scope, privilege, legal basis) and the executing examiner (method, feasibility) must; the client signs where its people perform steps, where business disruption is authorised, or where the protocol embodies its UK GDPR decisions, which in corporate collections it usually does. Signature blocks are not ceremony: they are the answer, two years on, to "who approved this?", and the protocol exists to make that answer boring.

§ 1 5 · REFERENCE

Glossary

Amendment

A written, approved change to the frozen protocol, logged with reasons.

Collection report

The post-execution reconciliation of plan against performance, with deliverables listed.

Contingency

A pre-decided response to predictable friction: encryption, absence, failure, refusal.

Deviation log

The live record of departures from plan; part of the collection record, not an embarrassment.

Escalation trigger

A discovery that pauses work on a source pending instructions: stop, preserve, call.

Execution log

The running record of collection day: times, machines, actions, surprises.

Hybrid collection

Client IT executing examiner-written methods under training, supervision, sampling and verification.

Method matrix

The per-source table: method, tool, executor, rationale, preservation position.

Protocol

The dated, versioned written plan governing a collection, approved before execution.

Quarantine

The sealed, access-logged container for privileged or sensitive material pending lawyer review.

Supervising solicitor

The independent solicitor holding the ring on search-order and imaging-order executions.

Verification step

IT confirmation of source identities shortly before execution, against map drift.

Sources and authoritative references

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

- cflab.uk, digital forensics services (protocol drafting and execution, court-ordered imaging support, hybrid-collection supervision, CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection ("defensibility is built, not retrofitted"; documented, verified collection at disclosure scale): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance: [college.police.uk, digital devices guidance](https://college.police.uk/digital-devices-guidance) · Forensic Science Regulator Code: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 and ISO/IEC 17025: iso.org, [27037](https://iso.org) · iso.org, [17025](https://iso.org)
- CPR Part 31 / PD 31B and PD 57AD (methodology description and the DRD) and CPR Part 25 / PD 25A (interim remedies including search orders): justice.gov.uk, [PD 57AD](https://justice.gov.uk) · justice.gov.uk, [Part 25](https://justice.gov.uk)
- CPR Part 35 (experts): justice.gov.uk, [Part 35](https://justice.gov.uk) · ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about forensic collection protocols in the United Kingdom as at August 2026. The clause wording is illustrative and must be adapted to the matter; 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. 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

Protocol work bookends our collections. Before: we draft the method matrix, contingencies, verification and custody sections with your team, verify source identities with client IT, and freeze a document sized to the matter, from one page to the schedule annexed to an imaging order. During: our examiners execute to the protocol, keep the execution and deviation logs live, supervise hybrid steps with training, tooling and sample re-collection, and staff the decision line. After: the collection report reconciles plan against performance, and the executed set (protocol, logs, evidence and hash schedules) is delivered exchange-ready and, where needed, supported under CPR Part 35 / CrimPR Part 19. Through **e-discovery.uk**, the protocol's outputs flow directly into processing and the DRD, so the methodology the court reads is the methodology that happened. 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