COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

eDisclosure or Digital Forensics?

Choosing the Correct Approach

The differences and overlap between forensic acquisition, forensic examination, eDiscovery processing and legal document review, with a decision tree showing when ordinary collection is sufficient and when forensic preservation or investigation should be considered. Written for solicitors, barristers, litigation partners, associates, paralegals, in-house counsel, disclosure lawyers, investigators and litigation-support professionals.

⏱ Estimated reading time: 28 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. Our examiners produce CPR Part 35 and CrimPR Part 19 compliant expert reports for solicitors, barristers, in-house counsel and private clients, and give evidence in the Crown Court, County Court, High Court and employment tribunals. Through our e-discovery practice at **e-discovery.uk** we also support the full disclosure lifecycle: defensible preservation, collection, processing, hosted review and production, which means we sit on both sides of the line this guide is about, and are instructed daily to advise on which side a matter belongs.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | CPR PART 35 EXPERT REPORTS | CRIMPR PART 19 EXPERT EVIDENCE | PD 57AD / DRD EXPERIENCE | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

Most disclosure exercises need **eDisclosure**: documented, metadata-preserving collection of live data, processed and reviewed at scale. A minority need **digital forensics**: device-level acquisition and expert examination directed at what happened rather than what exists. Choosing wrongly in either direction is expensive, forensically imaging every laptop in a routine contract dispute wastes six figures and drowns the team in data it cannot lawfully justify holding; running ordinary collection over a device that later needs forensic examination contaminates the very artefacts the examination would rely on.

THE HEADLINE ANSWER, WHEN DOES A DISCLOSURE MATTER ACTUALLY REQUIRE FORENSIC EXAMINATION?

When the dispute turns on a question a document population cannot answer by itself: whether a document is **authentic**, whether data was **deleted, altered or backdated**, **who** performed an action, whether files were **exfiltrated**, or what a **specific device** was used for at a specific time, or when a source is locked, damaged, volatile or already under suspicion, so that only a forensically sound acquisition will preserve its evidential value. If none of those is present, ordinary defensible collection is not the cheap option; it is the correct one.

- **Four disciplines, one supply chain.** Forensic acquisition captures data; forensic examination interprets artefacts; eDiscovery processing prepares volume for review; legal review applies judgment. They share tools and providers, but each answers a different question, and only the first two produce expert opinion evidence.
- **The choice is about the question, not the technology.** "Which of these documents must we disclose?" is eDisclosure. "What happened on this machine?" is forensics. Matters migrate from the first question to the second, so build the escalation path in from day one.
- **Preservation choices are one-way doors.** A forensic image taken today supports every later strategy, including ordinary disclosure; an ordinary collection today forecloses parts of a forensic examination tomorrow. Where suspicion is plausible, acquire forensically first and decide about examination later.
- **Proportionality cuts both ways.** Courts will not order, and UK GDPR will not comfortably accommodate, full imaging without justification; equally, a party that ignored clear forensic triggers will struggle to explain destroyed artefacts.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: two disciplines, one costly confusion

The two disciplines grew from different roots. eDisclosure descends from document discovery: its unit of work is the *document*, its habitat the review platform, its economics driven by volume. Digital forensics descends from crime-scene science: its unit of work is the *artefact*, a registry entry, a deletion trace, a USB connection record, its habitat the laboratory, its economics driven by depth. The confusion arises because both begin the same way: by copying data. From that shared first step, lawyers reasonably but wrongly infer that the disciplines are interchangeable.

The confusion costs money in one direction and evidence in the other:

- **Over-engineering:** forensic imaging of thirty custodians' devices in a dispute about invoice terms produces terabytes of unallocated space nobody will ever examine, a data-minimisation problem, and a bill that dwarfs the review budget, for no evidential gain over documented platform collection.
- **Under-engineering:** letting IT "have a look" at a suspect leaver's laptop, or exporting a mailbox from a device whose deleted content later matters, overwrites access timestamps, recycles unallocated space and breaks the chain of custody. The examination that follows can only describe the contamination.

The skill this guide teaches is **triage**: recognising, source by source and at each stage of the matter, which question you are really asking, and therefore which discipline, at which level of rigour, the source requires.

§ 0 3 · DEFINITIONS

The four disciplines defined

1 · Forensic acquisition

The capture of data from a device, account or system using methods that do not alter the source and produce a verifiable copy: write-blocked imaging of drives, physical, file-system or logical extraction from mobiles, hash-verified cloud preservation. The output is an **evidence container**, a forensic image or extraction, fingerprinted with hash values, logged with device state, tool, version and operator. Acquisition is a preservation act: it commits you to nothing, and keeps every later option open, including options nobody has thought of yet. Governed operationally by NPCC digital evidence principles: no action should change data that may later be relied on, and any necessary access must be by someone competent, with a record sufficient for a third party to reproduce the result.

2 · Forensic examination

The analysis of acquired data to answer investigative questions: recovering deleted material from unallocated space and databases; interpreting operating-system artefacts (registry, event logs, link files, USB records, prefetch); authenticating documents, emails, chats, images and recordings through metadata, encoding and structural analysis; attributing actions to accounts, devices and, as far as the evidence permits, people; and reconstructing timelines across sources. Examination produces **opinion**, and in litigation that opinion is delivered as expert evidence under CPR Part 35 or CrimPR Part 19, with the expert's overriding duty to the court, methodology open to challenge, and cross-examination the proving ground. Laboratory standards (ISO 17025 alignment; in criminal work the Forensic Science Regulator's Code) exist to make that methodology defensible.

3 · eDiscovery processing

The industrial preparation of collected data for legal review: expanding containers, extracting text and metadata, de-NISTing, deduplicating, threading email, indexing, and applying culling criteria, date ranges, custodians, tested search terms, analytics. Processing answers no legal question; it makes the population reviewable and the exercise reportable (volumes in and out at each stage, exception logs for encrypted and corrupt items). Its quality determines whether the disclosure certificate can honestly be signed, and its reports are what you produce when the opponent asks what happened to the other 1.4 million documents.

4 · Legal document review

The application of legal judgment to the processed population: relevance to the issues, privilege, confidentiality, redaction, issue-coding, by human reviewers, technology-assisted review, or both, under a written protocol with quality control and sampling. Review is where lawyers own the output; it is also where forensic questions most often surface mid-matter, when a reviewer notices the gap in a thread, the contract with the impossible date, the custodian whose mailbox is suspiciously clean.

	FORENSIC ACQUISITION	FORENSIC EXAMINATION	EDISCOVERY PROCESSING	LEGAL REVIEW

Question	How do we capture this without changing it?	What happened, and is this genuine?	How do we make volume reviewable?	What is relevant and privileged?
Unit of work	Device / account / source	Artefact	Dataset	Document
Output	Verified image or extraction + custody log	Findings and expert report; testimony	Review-ready database + processing reports	Coded set, privilege log, production
Evidence type	Foundation for everything downstream	Opinion evidence (CPR 35 / CrimPR 19)	Factual audit trail of methodology	The disclosed documents themselves
Typical standards	NPCC principles; hash verification	ISO 17025 alignment; FSR Code (criminal); Part 35 / Part 19 duties	EDRM practice; PD 57AD / PD 31B expectations	Professional duties; review protocol
Cost driver	Per device / source	Per question, per hour of examiner time	Per gigabyte	Per document reviewed

§ 0 4 · THE JOINS

Where they overlap, and where they must not be substituted

The disciplines form one supply chain, and three joints in that chain cause nearly all the trouble:

Overlap 1 · Collection feeds both pipelines

A forensic acquisition can always be processed for eDisclosure, the image is opened read-only, live files are extracted, and the review proceeds as normal, with the bonus that the source remains pristine. The reverse is not true: an ordinary export cannot later be "upgraded" into a forensic image of the device it came from, because the device has moved on. This asymmetry is the single most important planning fact in the field: **where any forensic question is plausible, acquire forensically first**; the incremental cost is modest and the option value is total.

Overlap 2 · Review surfaces forensic questions

Processing and review regularly detect what they cannot explain: missing thread segments, metadata anomalies, single-session "historic" documents, encrypted containers in the exception log. The correct response is a controlled handover, stop touching the source, preserve, instruct an examiner, not an informal look by whoever is nearest. A matter that begins as pure eDisclosure should still have its escalation route agreed in advance (see §8).

Overlap 3 · The same providers, different hats

Many providers (this laboratory included) offer both services, which is convenient but demands role clarity. Processing staff report facts about volumes; an examiner giving Part 35 evidence owes duties to the court and must be instructed, and must document, accordingly. When one organisation wears both hats, the instruction letters should separate the roles so that privilege, independence and the expert's duties are all clean.

> WHAT MUST NEVER BE SUBSTITUTED
>
> **Processing is not examination:** a review platform showing no deleted items does not mean nothing was deleted; platforms only see what the collection gave them. **Review is not authentication:** a document reading convincingly is not evidence it is genuine; authenticity is an artefact question. **Acquisition is not analysis:** owning a forensic image proves nothing until an examiner interprets it, and budgets should separate the two, because acquisition is cheap and examination is where scope control matters.

§ 0 5 · CONSEQUENCES

Why the choice matters legally

- **Disclosure duties are method-agnostic, until challenged.** Neither PD 57AD nor CPR 31 prescribes forensic collection; they require reasonable, proportionate, documented search and preservation. But the moment completeness or integrity is disputed, the method becomes the battleground: a hash-verified, logged collection survives; "the client exported what seemed relevant" does not.
- **Authenticity is procedurally live.** Under CPR 32.19 a party is deemed to admit the authenticity of disclosed documents unless it serves notice requiring the document to be proved at trial. Serving, or receiving, such a notice converts a disclosure question into a forensic one: proving authenticity means provenance, metadata and artefact evidence, which only exists if the underlying source was properly preserved.
- **Opinion needs an expert; an expert needs a foundation.** Assertions about deletion, backdating or attribution are opinion evidence. They must come from a qualified examiner complying with CPR 35 / PD 35 (or CrimPR 19), and they collapse under cross-examination if the acquisition beneath them was informal. The examiner's first question is always "who touched this, and how, before me?"
- **Criminal and regulatory contexts raise the floor.** Where conduct may engage criminal proceedings, CPIA-standard handling, NPCC principles and the Forensic Science Regulator's Code shape what the court will accept, and an internal investigation run to civil-casual standards can compromise a later prosecution or defence.
- **Costs discipline both directions.** Judges asked to order imaging of an opponent's devices require cogent justification (it is an intrusive order, sparingly made, typically with independent-expert and privilege protocols); judges asked to excuse destroyed artefacts require an explanation of why obvious triggers were ignored. The party with a documented triage decision wins both arguments.

§ 0 6 · THE DECISION

The decision tree: ordinary collection, forensic preservation, or investigation?

Run this per source, a matter routinely mixes all three outcomes (ordinary collection for the corporate mailboxes; forensic preservation of the leaver's laptop; full examination of one disputed phone).

QUESTION 1

Does the dispute (or any pleaded issue) turn on authenticity, deletion, alteration, backdating, attribution or exfiltration?

YES

Forensic track for every implicated source: forensic acquisition now, examination scoped to the question. Go to Q5 for the remaining, unimplicated sources.

NO

Continue to Q2.

QUESTION 2

Is any source under suspicion, or likely to become contested, a departing employee's device, a custodian with an incentive to delete, a counterparty already crying forgery?

YES

Forensic **preservation**: acquire the source forensically and store the image; defer any examination until the issue crystallises. Cheap insurance, total option value.

NO

Continue to Q3.

QUESTION 3

Is the source technically volatile or inaccessible, a mobile with disappearing messages, a locked or damaged device, an account about to be decommissioned?

YES

Forensic acquisition now, by a specialist: volatility does not wait for the CMC, and locked or damaged sources need laboratory methods regardless of the legal question.

NO

Continue to Q4.

QUESTION 4

Could the matter plausibly go criminal or regulatory, fraud, computer misuse, data theft referred to police, an SFO / FCA / ICO dimension?

YES

Handle key sources to the criminal-forensic standard from the start (NPCC principles, laboratory chain of custody): a civil-casual collection can compromise the later criminal case.

NO

Continue to Q5.

QUESTION 5

None of the above applies to this source?

ORDINARY COLLECTION

Documented, metadata-preserving platform collection under a written protocol, hash-manifested, into standard eDiscovery processing and review. This is the correct, not the lazy, answer for most corporate sources.

BUT KEEP WATCH

Agree the mid-matter escalation route (§8) so that if review surfaces an anomaly, the source can still be preserved before anyone "has a look".

Figure 1 · Per-source triage. Note the asymmetry: answering "yes" too generously costs money; answering "no" wrongly costs evidence. Where genuinely unsure, forensic preservation (image now, examine later, or never) is the hedge that caps both risks.

§ 0 7 · ESCALATION SIGNALS

The ten forensic triggers

Commit these to memory, any one of them, appearing at any stage, means at minimum forensic preservation of the implicated source:

TRIGGER	WHY FORENSICS, NOT EDISCLOSURE
1 · A document's authenticity is disputed (or you intend to dispute one)	Authenticity lives in metadata, structure and provenance artefacts, examination territory, and CPR 32.19 notices make it procedural.
2 · Deletion is suspected or admitted	Recovery from unallocated space, databases and backups, and, equally important, expert interpretation of what deletion traces do and do not prove.
3 · A key employee is leaving or has left under a cloud	USB records, cloud-sharing logs, link files and access artefacts on their devices decay with every day of reuse; preserve before reprovisioning.
4 · Chronology anomalies: dates that cannot be right	Backdating and timeline manipulation are proven or explained through file-system, application and email-header artefacts.
5 · "It wasn't me at the keyboard"	Attribution requires logins, device artefacts and the elimination of malware / remote access, opinion evidence, not inference from documents.
6 · Mobile chat evidence is central and contested	Complete, metadata-intact extraction from handset or backup is the only answer to "the screenshots are selective / fabricated".
7 · The source is locked, encrypted, damaged or dead	Laboratory acquisition methods (and lawful-authority questions) beyond eDiscovery tooling.
8 · An opponent's disclosure smells wrong	Grounds for specific disclosure, natives-with-metadata requests, or an application for inspection / imaging, all of which need an examiner behind them.
9 · Criminal or regulatory exposure is realistic	Evidence handled below the criminal standard may be unusable exactly when the stakes rise.
10 · The court or tribunal needs an opinion	Any assertion about what happened on a device is expert evidence: CPR Part 35 / CrimPR Part 19, with a qualified examiner who can be cross-examined.

§ 0 8 · IN PRACTICE

Practical workflow: triage at the outset, escalation mid-matter

At the outset: the 48-hour triage

STEP	ACTION
1	Issue the legal hold (all sources, all custodians), the hold is common to both disciplines and buys time for triage.
2	Build the source list from client and IT interviews; mark each source against the decision tree (§6) and the ten triggers (§7).
3	Forensically acquire everything marked volatile, suspect or trigger-positive, before broader planning, before the DRD, before anyone tidies up.
4	Route the remainder into documented platform collection and standard processing.
5	Record the triage in the methodology memo: source, decision, trigger(s), date, decider. This memo is what you produce when either over- or under-engineering is later alleged.

Mid-matter: the escalation protocol

Agree this before review starts, in one paragraph of the review protocol: *any reviewer or provider who identifies a potential forensic trigger (anomalous metadata, gaps in threads, unexplained encryption, suspected fabrication) logs it and stops; the source is not accessed further; supervising counsel decides within 48 hours whether to instruct forensic preservation or examination; nobody outside the forensic instruction touches the implicated source meanwhile.* The protocol costs nothing and prevents the two classic mid-matter injuries: the IT department's "quick look", and the review team that keeps working a contaminated source for three more weeks.

FOR THE PRACTITIONER

Escalation is bidirectional. Forensic examinations also de-escalate into eDisclosure: once the examiner confirms the device is clean or the question answered, its live data joins the ordinary review population. Budget both directions: acquisition per source, examination per question, processing per gigabyte, review per document, and make each step a separate, revisitable decision.

§ 0 9 · METHOD SELECTION

Collection methods compared: cost, intrusion, evidential yield

METHOD	WHAT IT CAPTURES	WHAT IT CANNOT DO	RELATIVE COST / INTRUSION	RIGHT FOR
Platform export under protocol (Purview, Vault, APIs)	Live mail, chat, files with substantial metadata; export logs	No deleted/unallocated data; tool-specific metadata gaps; nothing device-level	Low / low	Routine corporate sources with no triggers
Targeted forensic collection	Defined folders, accounts or apps, hash-verified, metadata intact	Limited recovery of deleted material outside the target scope	Moderate / low–moderate	BYOD and mobile sources; data-minimisation-sensitive collections
Logical / file-system mobile extraction	Messages, media, app databases, much deleted-in-database content	Not full storage; some app data and unallocated space out of reach	Moderate / moderate	Chat-centric matters; most civil mobile evidence
Full forensic image (physical)	Everything, including deleted and unallocated data; maximal artefact base	Nothing, but generates maximal data-protection and cost load	High / high	Trigger-positive devices; criminal-standard handling; disputed machines
Custodian self-collection	Whatever the custodian chose to send, metadata mangled	Verification, completeness, integrity, all of it	"Free" / catastrophic	Nothing contested. Avoid.

Two rules of thumb close most method arguments. First, **match rigour to the source's risk, not the matter's glamour**: a mundane dispute can contain one radioactive laptop, and a fraud claim can contain forty entirely ordinary mailboxes. Second, **never collect below the level you may need to defend**: moving up later is impossible, moving down later (using only the live files from a forensic image) is trivial.

§ 10 · IN THE WILD

Realistic litigation examples

EXAMPLE 1 · WHERE ORDINARY COLLECTION WAS THE RIGHT CALL

A distribution dispute: twelve custodians, issues confined to what was agreed and shipped, no authenticity challenge, no leavers. The defendant's solicitors ran documented Purview collections, standard processing and a TAR-assisted review; the DRD recorded the methodology and the opponent never laid a glove on it. A forensic quote for imaging all twelve custodians' devices, six times the collection budget, was rightly declined, and the methodology memo recorded why. **Lesson:** declining forensics is a decision to document, not a corner to cut silently.

EXAMPLE 2 · WHERE FORENSICS WAS NEEDED FROM DAY ONE

A director resigned to a competitor; the company suspected the customer database had gone with him. His laptop was withdrawn from circulation and forensically imaged the same day; his phone was extracted before handback. Examination found USB connection records, link files opening the database export from external media, and cloud-sharing logs, a package that supported a springboard injunction within a fortnight. Had the laptop been reissued to a new starter first (the IT department's plan), every one of those artefacts would have been buried under new activity. **Lesson:** trigger 3 (§7) is a same-day decision.

EXAMPLE 3 · THE MID-MATTER ESCALATION

In a partnership dispute run as ordinary eDisclosure, a reviewer flagged that a pivotal side letter existed only as a scanned PDF, produced by the opponent, with no covering email anywhere in either side's population. Under the agreed escalation protocol the anomaly went to counsel within a day; a CPR 32.19 notice was served, natives and provenance were demanded, and the eventual forensic examination showed the "2019" letter's scan was created in 2023 on a device belonging to the opposing party's bookkeeper. The claim did not survive the report. **Lesson:** review teams find forensic questions; the protocol determines whether the finding is exploited or fumbled.

§ 11 · CONSTRAINTS

Proportionality, privilege and UK GDPR when forensics enters the frame

- **Data minimisation vs the full image.** A physical image is, by design, everything, including the custodian's personal life. UK GDPR (Art 5(1)(c)) and plain proportionality require that imaging be justified per source by the triggers, that examination scope be defined by questions rather than curiosity, and that targeted extraction be preferred where it answers the need, especially on BYOD devices, where the custodian is a data subject with their own rights and the practical reality is negotiation, transparency information and a documented balancing exercise.
- **Privilege inside images.** A device image will contain privileged material. Where an opponent's or third party's device is examined under court order, the standard protection is an independent examiner and a privilege protocol (keyword screens, review by the disclosing party's lawyers before anything passes across). Build the protocol into the draft order; do not improvise it afterwards.
- **Employee monitoring optics.** Forensic examination of a current employee's devices engages employment law and trust: act under clear policies, document lawful basis and necessity, and confine examination to the investigation's scope. The ICO's employment-practices guidance is the reference point.
- **Retention of images.** Forensic images are the most data-dense objects in the matter; the disposal stage (return, verified destruction, certificates) matters most here, subject to any continuing preservation duty. Agree it in the instruction letter.
- **Cross-border sources.** Imaging devices or accounts in other jurisdictions can engage local privacy, employment and blocking laws; take local advice before the acquisition, not after.

§ 12 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The IT "quick look".** The single most destructive act in the field: logging into the suspect device, browsing folders, opening files, every action overwriting the artefacts that mattered.
- **Reissuing the leaver's laptop.** Standard IT hygiene, forensic catastrophe. The hold notice must reach IT operations, not just custodians.
- **Treating acquisition and examination as one purchase.** Parties either balk at a combined quote and preserve nothing, or sign it and fund an unscoped fishing expedition. Split them: acquire broadly, examine narrowly.
- **Screenshots as chat evidence.** Selective, metadata-free, fabricable, and increasingly said so by courts and tribunals. Extract properly or expect the challenge.
- **Asserting deletion / backdating without an expert.** Submissions do not prove artefacts. Unsupported forensic assertions damage credibility and invite adverse costs.
- **Ignoring CPR 32.19.** Failing to serve a notice to prove where authenticity is genuinely doubted, deemed admission is the price.
- **Forensic theatre.** Imaging everything to look thorough, then facing the data-protection, hosting-cost and review consequences of holding it.
- **No escalation protocol.** The anomaly is spotted in week 2 and mentioned in week 9, after the source has been reprovisioned.

Technical limitations

- **Recovery has physics.** SSD TRIM, encrypted storage and time make deletion recovery probabilistic, not guaranteed; the honest expert says so, and so should the advice to the client.
- **Absence of artefacts is weak evidence of absence.** Logs rotate, artefact sources have finite windows, and "no trace found" supports limited inferences, a point that cuts for and against you.
- **Attribution has a ceiling.** Examination attributes actions to accounts and devices robustly; attributing them to a human being is inference, contestable by shared-credential, malware and remote-access alternatives. Frame pleadings accordingly.
- **Cloud evidence depends on providers.** Audit-log depth, retention windows and export fidelity vary by platform and licence tier; some questions are answerable only within a provider's log-retention window, another reason speed matters.
- **Locked devices are not always openable.** Lawful-access capability varies by device, OS version and state; no reputable laboratory guarantees access in advance.

§ 13 · INTERROGATORIES

Questions to ask

Ask your client

- Is any part of this dispute really about whether something is genuine, complete, or was deleted, now or foreseeably?
- Who had motive and opportunity to delete or fabricate? Where are their devices and accounts now?
- Have any implicated devices been reissued, repaired, reset or "looked at" since the dispute arose? By whom, exactly?
- Which sources are volatile: mobiles, disappearing-message apps, accounts scheduled for deletion, backup rotations?
- Could this plausibly become a police, SFO, FCA or ICO matter?
- What is the realistic budget split between preserving everything relevant and examining what is actually in question?

Ask your opponent

- For each source: collection method, tool, operator, date, and whether any source was accessed outside that method.
- Are hash values available for the collections and for pivotal documents? Will natives with metadata be produced?
- Were any devices central to the issues reissued, reset or disposed of after the dispute arose? On whose instruction?
- Where authenticity is challenged: what provenance evidence supports the document, and who will give it?
- Was any forensic work done? By whom, to what standard, and will the reports and images be disclosed?

Ask a forensic / eDisclosure provider

- Which service am I buying, acquisition, examination, processing, review support, and where does each start and stop?
- For acquisition: method per source type, what it captures and omits, and turnaround for volatile sources.
- For examination: who examines, their qualifications and court experience, and how scope and hours are controlled per question.
- How are the roles separated if you provide both eDiscovery and expert services on the same matter?
- What standards apply, NPCC principles, ISO 17025 alignment, FSR Code where criminal, and how is chain of custody documented?
- What happens to images and data at the end: retention, return, verified destruction?

§ 14 · DRAFTING AIDS

Suggested wording for instructions

FORENSIC PRESERVATION (IMAGE NOW, EXAMINE LATER)

"We instruct you to take forensic acquisitions of the devices and accounts listed in Schedule 1, using write-protected, hash-verified methods appropriate to each source, documenting device state, tools, versions and operators, and maintaining chain-of-custody records throughout. No examination or analysis is instructed at this stage. Images and extractions are to be securely stored [in the UK] pending further instructions, and no person is to access them without our written authority. Please confirm acquisition and provide the custody log and hash manifest within [x] days."

SCOPED FORENSIC EXAMINATION

"Further to the preserved acquisitions, we instruct you to examine [source(s)] for the purpose of addressing the following questions only: [e.g. (1) whether the document at Exhibit A was created, modified or backdated, and when; (2) whether files from the folder 'X' were copied to external media or cloud accounts between [dates], and if so the detail of each transfer]. Please report findings, methodology and limitations in a form compliant with CPR Part 35 and Practice Direction 35 [/ CrimPR Part 19], including the required expert's declaration, and identify any further questions the evidence raises before undertaking work beyond this scope."

ESCALATION PARAGRAPH FOR A REVIEW PROTOCOL

"Any reviewer identifying material suggesting deletion, fabrication, alteration, backdating, unauthorised transfer or other integrity concern shall code the document [FORENSIC-FLAG], record the concern in the escalation log, and take no further investigative step. Supervising counsel will determine within 48 hours whether forensic preservation or examination is required. Pending that determination, no person shall access the implicated source device or account."

§ 15 · QUICK CONTROL

Checklist and red flags

The triage checklist

- ☐ Every source run through the decision tree, with the outcome and trigger(s) recorded per source
- ☐ Trigger-positive and volatile sources forensically acquired before any other handling
- ☐ IT operations (not just custodians) on notice: no reissue, reset, repair or disposal of implicated devices
- ☐ Acquisition and examination instructed and budgeted separately; examination scoped by written questions
- ☐ Escalation paragraph in the review protocol; forensic-flag code live in the platform
- ☐ CPR 32.19 position considered for every pivotal opposing document
- ☐ Privilege protocol agreed before any examination of shared or opposing-party sources
- ☐ Data-protection record: justification per image, targeted extraction where sufficient, BYOD handled with custodian transparency
- ☐ Expert independence and Part 35 / Part 19 compliance confirmed where opinion evidence is foreseeable
- ☐ Image retention and destruction terms agreed in the instruction letter

Red flags: forensics is (or was) needed

- A pivotal document exists only as a scan or image-PDF, with no native, no covering email, no metadata.
- Devices central to the issues were reissued, reset or "repaired" after the dispute arose.
- Chat evidence arrives as screenshots, with gaps at the interesting moments.
- The opponent's collection was performed by an interested party, the accused employee, the family member, "our IT guy", with no logs.
- Timeline impossibilities: documents referencing events post-dating their own dates; ledgers with uniform authoring sessions.
- An internal investigation has already "checked the laptop" informally.
- Sudden hash or metadata unavailability for exactly the contested documents.
- A witness's account depends entirely on what a device would show, and the device has not been preserved.

§ 16 · COMMON QUESTIONS

Frequently asked questions

When does a disclosure matter actually require forensic examination?

When an issue turns on authenticity, deletion, alteration, backdating, attribution, exfiltration or device usage, questions about what *happened* rather than what *exists*, or when a source is volatile, locked, damaged or under suspicion, so that only forensic acquisition preserves its evidential value. Absent those features, a documented, metadata-preserving ordinary collection is the correct approach, and the decision to proceed without forensics should simply be recorded with reasons.

Can we start with ordinary collection and go forensic later if something emerges?

Only partially. The review population can always be re-examined, but the source devices keep living: artefacts are overwritten, logs rotate, handsets are replaced. That is why the hedge for uncertain sources is forensic *preservation* now, an image on a shelf, with examination deferred until (and unless) a question crystallises.

Is a forensic image always better, then?

No. Imaging every source is disproportionate, collides with data minimisation, and multiplies hosting and disposal obligations for no gain on untriggered sources. The image is better *for trigger-positive and uncertain sources*; the documented platform collection is better for the rest. Triage, per source, is the discipline.

Our IT team already looked at the laptop. Is it ruined?

Not necessarily ruined, but changed. Much artefact evidence survives casual access; what is lost is mainly last-access states and some volatile data, and what is created is post-incident noise an examiner must now explain around. Stop further access immediately, record exactly who did what and when, and let the examiner assess. The candid access log materially limits the damage in court.

Can we make the other side hand over their devices for imaging?

Sometimes, with cogent justification: courts can order inspection or imaging where disclosure appears deficient or integrity is genuinely in issue, but the order is intrusive and exceptional, and almost always comes wrapped in protections, an independent examiner, a privilege and confidentiality protocol, defined search scope. Build that architecture into the application; a bare "hand over the laptops" request fails.

Who should give the evidence, the provider who processed our disclosure?

The processing team can give factual evidence about what was done. Opinion about authenticity, deletion or attribution needs an expert instructed under CPR Part 35 / CrimPR Part 19, with the overriding duty to the court and the declaration to match. Where one organisation does both, insist the roles and instruction letters are separated, it protects the expert's independence and your client's position.

§ 17 · REFERENCE

Glossary

Artefact
A trace recorded by a system about activity: registry entries, log records, link files, deletion traces, connection records.

Attribution
Linking an action to an account, device and, as far as evidence permits, a person.

Chain of custody
The documented, unbroken record of who has held evidence and what was done to it.

Exfiltration
Unauthorised transfer of data out of an organisation, by USB, cloud sharing, personal email or otherwise.

Forensic acquisition
Capture of data by methods that do not alter the source and produce a hash-verified, reproducible copy.

Forensic image
A verified bit-for-bit copy of a storage device, including deleted and unallocated data.

Hash (MD5 / SHA-256)
A cryptographic fingerprint used to verify integrity and prove copies identical.

Link (LNK) files
Windows shortcut artefacts recording files opened, including from external media.

Logical / file-system extraction
Mobile acquisition levels capturing accessible files and app databases short of full physical storage.

NPCC principles
The national digital-evidence principles (successor to the ACPO principles) governing handling of electronic evidence.

Notice to prove (CPR 32.19)
The notice displacing deemed admission of a disclosed document's authenticity, requiring it to be proved at trial.

Processing
Industrial preparation of collected data for review: extraction, deduplication, indexing, threading, culling.

TAR / CAL
Technology-assisted review / continuous active learning, machine-learning prioritisation of review.

Unallocated space
Disk areas not assigned to live files, where deleted material may persist until overwritten.

Write blocker
Hardware or software preventing any write to a source device during acquisition.

Authoritative UK references

- CPR Part 35, Experts and Assessors (and PD 35): justice.gov.uk/courts/procedure-rules/civil/rules/part35
- CPR Part 32.19, notice to prove authenticity: justice.gov.uk/courts/procedure-rules/civil/rules/part32
- Practice Direction 57AD and the Disclosure Review Document: justice.gov.uk, PD 57AD
- CPR Part 31 and PD 31B, Disclosure of Electronic Documents: justice.gov.uk, PD 31B
- Criminal Procedure Rules Part 19, Expert Evidence: gov.uk, Criminal Procedure Rules
- Criminal Procedure and Investigations Act 1996: legislation.gov.uk/ukpga/1996/25
- Attorney General's Guidelines on Disclosure (rev. 2024): gov.uk, AG's Guidelines
- Forensic Science Regulator, Code of Practice: gov.uk, FSR Code
- ICO, employment practices and data protection guidance: ico.org.uk
- Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12 · Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/21

DISCLAIMER

This publication provides general information about digital forensics and electronic disclosure practice in the United Kingdom as at August 2026. It 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, guidance and legislation 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

Because we operate both a digital forensics laboratory and an e-discovery practice (**e-discovery.uk**), we are routinely instructed at exactly the decision point this guide describes, and we advise candidly in both directions, including when forensic work is not warranted. Our examiners provide same-day forensic preservation of volatile sources, laboratory acquisition from locked and damaged devices, scoped examinations reported under CPR Part 35 / CrimPR Part 19, and independent-examiner appointments under privilege protocols; our e-discovery team provides the documented collection, processing, hosted review and production that the untriggered majority of every matter needs, with a single chain-of-custody discipline across both. 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