COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Forensic Data Collection Explained for Lawyers

Repeatability, Hashes, Metadata and the Chain of Custody

Anyone can copy files. Forensic collection is something different: acquiring electronic data by a documented, repeatable method that preserves the source, captures the metadata, verifies every copy with cryptographic hashes, timestamps every step, and records an unbroken chain of custody from device to courtroom. The difference decides whether your evidence is "we have the files" or "we can prove these are the files, unaltered, and here is how". This guide explains the seven pillars of forensic collection in plain language, shows what casual copying silently destroys, and equips lawyers to instruct, question and defend collections that will face challenge.

⏱ 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. Its examiners perform forensic collections daily (computers, servers, mobile devices, cloud tenancies) under ISO 17025-aligned procedures and the NPCC digital evidence principles, with continuity of evidence maintained from seizure to court and findings reported under CPR Part 35 and CrimPR Part 19. Its eDiscovery arm, **e-discovery.uk**, applies the same discipline to disclosure-scale collections: defensibility is built, not retrofitted, and the collection stage is where it is built first.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ISO 27001-ALIGNED SECURITY | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | CPR PART 35 EXPERT REPORTS | CRIMPR PART 19 EXPERT EVIDENCE | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: COLLECTION IS AN EVIDENTIAL ACT, NOT AN IT TASK

Forensic data collection is the acquisition of electronic data by a method that is **repeatable** (documented tools, versions and settings another examiner could re-run to the same result), **audited** (contemporaneous logs of every action), **time-anchored** (original timestamps preserved, system clocks checked and offsets recorded), **verified** (cryptographic hashes computed at acquisition and re-checked at every subsequent handling), **non-destructive** (the source unaltered, or any unavoidable change recorded, justified and explained by someone competent to do so), **metadata-complete** (the dates, authors, paths and system context collected with the content, not stripped from it), and **continuous** (a chain of custody accounting for the evidence at every moment between the device and the courtroom). These seven pillars are what separate an exhibit from an attachment. They cost little when built in at the start, cannot be retrofitted afterwards, and are the entire difference between a collection that survives a hostile expert and one that becomes the case's second dispute.

- **Ordinary copying destroys evidence silently.** Drag-and-drop and email-me-the-folder change timestamps, strip metadata, miss deleted and hidden material, and leave no record: the files arrive, and the ability to prove anything about them does not.
- **The standard scales; the pillars do not.** A full forensic image and a two-hour targeted collection differ enormously in scope and cost, but both can and should be repeatable, hashed, logged and continuous: "targeted" is a scope decision, never a licence to collect casually.
- **Documentation is the product.** The acquisition log, hash schedule, exhibit record and chain-of-custody form are not paperwork around the evidence; in a challenge, they are the evidence about the evidence, and the side with them wins.
- **The framework is settled.** The NPCC digital evidence principles, ISO/IEC 27037's identification-collection-acquisition-preservation guidance, ISO 17025 laboratory discipline and (in criminal work) the statutory Forensic Science Regulator Code define what competent looks like; lawyers do not need to master them, but must know to ask for them.
- **Instruct before anyone touches anything.** Most collection failures happen in the first 48 hours, performed by well-meaning IT staff; the cheapest intervention in this guide is the sentence "do not open, copy or preview anything until the method is agreed."

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: copying is not collecting

When a dispute begins, the instinct is to gather the documents: IT copies the leaver's home drive to a share, an HR manager forwards themselves the relevant emails, someone opens the laptop "just to check what's on it". Every one of those acts feels like preservation. Each is quietly destructive:

- **Opening changes things.** Booting a computer writes hundreds of files; opening a document can update its last-accessed and sometimes its modified time; previewing generates thumbnails and cache entries. The device now says the examining party touched everything, dated after the dispute began.
- **Copying strips context.** A drag-and-drop copy typically resets file creation dates to the moment of copying, drops NTFS metadata and alternate streams, ignores deleted material entirely, and preserves nothing about where files sat or who could access them. The content arrives; its history does not.
- **Nothing is verifiable.** Without hashes computed at the point of acquisition, there is no way to demonstrate that the files reviewed, disclosed or exhibited two years later are the files taken, unaltered. "They are the same" becomes assertion, exactly where the other side will attack.
- **Nothing is recorded.** Who did it, when, with what, to which device, and what happened to the copy afterwards: in the casual version, the answers live in fading memory, and cross-examination of fading memory is a spectator sport.

The forensic version of the same afternoon costs modestly more and produces a different legal object: an exhibit with a birth certificate. The seven pillars that follow are that certificate's clauses, and each is explained so that a lawyer can instruct for it, check for it, and cross-examine its absence.

§ 0 3 · THE MAP

What makes a collection forensic: the seven pillars

PILLAR	IN ONE SENTENCE	WHAT ITS ABSENCE COSTS
1 · Repeatability	Method, tools, versions and settings documented so another examiner could reproduce the result	The collection becomes one person's say-so; challenge cannot be answered by re-performance
2 · Audit trail	Contemporaneous logs of every action taken, by whom, when, with what outcome	Gaps invite the inference that something happened in them
3 · Timestamps	Original file and system times preserved; collection times recorded; clock offsets checked and noted	The chronology (often the case) becomes unprovable or, worse, wrong
4 · Hash verification	Cryptographic fingerprints computed at acquisition and re-verified at every later step	No demonstrable identity between what was taken and what is produced
5 · Source preservation	The original unaltered (write-blocked, read-only methods), or unavoidable changes recorded and explicable	The best evidence is contaminated by its own collection
6 · Metadata	Dates, authors, paths, permissions and system context acquired with the content	Documents float free of the history that gives them meaning
7 · Chain of custody	An unbroken, signed record of possession, storage and transfer from acquisition to court	Admissibility friction, weight reduction, and a standing invitation to allege interference

The pillars are cumulative and cheap together: the same disciplined hour that hashes the acquisition also logs it, records the clock offset and opens the custody record. What follows takes each in turn.

§ 0 4 · PILLAR 1

Repeatability

- **The test:** could a second, independent examiner, given the documentation alone, perform the same acquisition and obtain the same verifiable result? If yes, the collection is science; if no, it is anecdote.
- **What is recorded to achieve it:** the tool and its version (imaging software, extraction platform, cloud export mechanism), the settings and options used, the source's identifiers (make, model, serial, capacity), the method (physical image, logical acquisition, targeted export), the date, time and place, and the operator. In laboratory practice this lives in the case notes and the acquisition worksheet as the work happens, not reconstructed afterwards.
- **Why courts care:** expert evidence must be capable of being tested. A repeatable collection lets the opposing expert verify rather than speculate (re-hash the image, re-run the export, confirm the result), which paradoxically is the best protection the collecting party has: verification ends arguments that suspicion would keep alive.
- **The lawyer's use:** when reviewing your own side's collection, ask for the acquisition record and check it answers the test; when attacking the other side's, ask the same question and watch what cannot be answered. "What version of the tool, and what settings?" is a devastating question to a casual collector and a trivial one to a competent laboratory.

§ 0 5 · PILLAR 2

The audit trail

- **What it is:** the contemporaneous record of everything done: the examiner's dated notes, the tool's own generated logs (imaging logs, extraction reports, export manifests), photographs of devices and their condition, and the record of anything unexpected (a drive with bad sectors, a phone that powered on, a password that failed) with how it was handled.
- **Contemporaneous is the operative word.** Notes made during the work carry evidential weight that reconstructions do not; a laboratory's habit of logging as it goes is precisely what makes its account of a contested moment believable eighteen months later.
- **Tool logs are exhibits in waiting.** Modern forensic tools generate their own audit records (start and finish times, source identifiers, hash results, errors encountered); preserving these alongside the human notes gives the court two independent accounts that corroborate each other.
- **Deviations are logged, not hidden.** Real collections meet real-world friction: the defensible response to a deviation (a live acquisition forced by encryption, a partial read from a failing drive) is a note explaining what, why and with what effect, made at the time. The indefensible response is silence, because the artefacts of the deviation will be visible to the other side's expert anyway, now unexplained.

§ 0 6 · PILLAR 3

Timestamps

- **Two families to keep straight:** the timestamps *inside* the evidence (file created, modified and accessed times; email sent and received times; log entries), which forensic method preserves untouched; and the timestamps *of the collection* (when acquisition started and finished, when each transfer occurred), which the audit trail supplies. Confusing the two is a classic cross-examination trap for careless witnesses.
- **The clock check:** a device's own clock may be wrong, drifted or deliberately altered. Competent practice records the source system's clock against a reference time at acquisition and notes the offset, so every internal timestamp can later be corrected and the correction explained. Cases have turned on seven-minute DVR drifts; the examiner who recorded the offset owns that argument.
- **Time zones and normalisation:** systems store times variously in UTC and local time; processing normalises them for review. What matters legally is that the original values are preserved, the normalisation rule is documented, and displayed times can always be traced back: "what time zone is this timestamp in?" should have an instant, evidenced answer.
- **Why lawyers should care first:** chronology is usually the case: who knew what, when; which document preceded which call. Every chronology argument inherits the quality of the timestamp handling underneath it, and that quality is fixed at collection, permanently.

§ 0 7 · PILLAR 4

Hash verification

- **The concept in one paragraph:** a cryptographic hash (MD5, SHA-1, SHA-256) is an algorithm that reduces any quantity of data to a short fixed-length fingerprint. Change a single bit of the data and the fingerprint changes completely; leave it untouched and the fingerprint is identical every time it is computed, by anyone, with any conforming tool. It is the mathematics that lets a copy prove it is a true copy.
- **How it is used in collection:** at acquisition, the evidence (an image, an export, a file set) is hashed and the values recorded in the acquisition log; at every later stage (transfer to storage, delivery to a review platform, production to the other side) the hash is recomputed and matched. An unbroken chain of matching hashes is mathematical proof that the exhibit before the court is bit-for-bit what was collected.
- **Working copies, protected original:** analysis is performed on hashed working copies while the original acquisition is preserved untouched; if a working copy is ever questioned, it is re-verified or re-derived from the original, and the question ends.
- **What lawyers should know now** (a dedicated guide in this series treats hashes fully): ask for the hash values in the acquisition record; expect re-verification on every transfer; and understand that a hash proves integrity (unchanged since acquisition), not provenance (how the data came to exist on the device), which are different questions answered by different evidence.

§ 0 8 · PILLAR 5

Source preservation

- **The principle** (the first of the NPCC digital evidence principles, inherited from ACPO): no action taken should change data that may subsequently be relied upon in court. In practice: hardware or software write-blockers between the evidence drive and the examination machine; read-only acquisition methods; phones isolated from networks before extraction; cloud data exported by mechanisms that do not modify the tenancy.
- **The exception, done properly** (the second principle): where accessing original data is unavoidable (a running server that cannot be shut down, an encrypted laptop that must be imaged live, a phone that must be unlocked), the person doing so must be competent and must record and be able to explain what was done and its implications. Change is sometimes inevitable; unexplained change never is.
- **Preservation of the source after acquisition:** the original device or an unopened master copy is sealed, stored and left alone; examination happens on verified working copies. If the matter escalates, the other side's expert can be offered the original or the master image, which is both good practice and excellent tactics.
- **The lawyer's early move:** the moment litigation is contemplated, the instruction to the client is to stop touching sources: no logins to the leaver's account, no IT tidy-ups, no "quick look" at the laptop. Everything in this pillar is easiest when nobody has been helpful yet.

§ 0 9 · PILLAR 6

Metadata

- **What travels with a forensic collection:** file-system metadata (paths, sizes, timestamps, ownership and permissions), document-internal metadata (authors, companies, revision histories, edit times), email transport metadata (headers, routing, message identifiers), and system context (which account, which profile, which folder structure). Forensic acquisition captures these because it copies the container, not just the contents.
- **What casual copying loses:** creation dates reset to the copy date; ownership and permissions replaced by the copier's; folder context flattened; deleted items and previous versions ignored; and email exported to loose files shorn of headers. The loss is invisible at the time and unrecoverable later, because the evidence of what the metadata was existed only in the source state that copying overwrote.
- **Why it matters in argument:** metadata is how documents are attributed, dated, sequenced and authenticated: the questions of who wrote this, when it changed and whether it was backdated are answered from metadata or not at all. A disclosure exercise that produces content without reliable metadata has produced exhibits that cannot do evidential work.
- **Metadata has limits** (a dedicated guide treats this fully): it records what a system did, which is not always what a human intended, and some fields are alterable by the sufficiently motivated. The forensic point here is narrower: whatever the metadata proves or does not prove, collection must deliver it intact, or the analysis never gets the chance.

§ 10 · PILLAR 7

Chain of custody

- **What it is:** the documented, signed, unbroken account of the evidence's whereabouts and handlers from the moment of acquisition (or seizure) to the moment of use: exhibit references assigned at collection; sealed, labelled storage; signed transfer records for every change of hands; access logs for the evidence store; and hash re-verification marking each transition.
- **What it does legally:** continuity is what lets the court treat the exhibit as the thing collected. Breaks rarely make digital evidence inadmissible by themselves in civil proceedings, but they convert weight into argument: every gap is a period in which opposing counsel is entitled to wonder aloud what happened, and juries and judges wonder along.
- **The digital additions:** for electronic evidence the chain includes logical custody too: which systems held copies, who had platform access, and the hash trail that proves the object did not change while custody changed. A perfect paper chain around an unverified copy is theatre; the two together are continuity.
- **Kept from minute one:** custody records cannot be started retroactively without becoming reconstructions. The laboratory habit (exhibit reference and custody form opened at the point of collection, every movement signed since) is the whole discipline; a dedicated guide in this series covers the records themselves, with worked examples of weak versus defensible documentation.

§ 1 1 · THE FRAMEWORK

The standards frame: NPCC, FSR, ISO

- **NPCC digital evidence principles** (successors to the ACPO principles, and the lingua franca of UK practice): (1) no action should change data that may be relied upon; (2) where accessing original data is necessary, the person must be competent and able to explain their actions; (3) an audit trail of all processes should exist such that an independent third party could reproduce the result; (4) the person in charge of the investigation is responsible for ensuring these principles are followed. The seven pillars of this guide are these principles operationalised.
- **ISO/IEC 27037** provides international guidance for the identification, collection, acquisition and preservation of digital evidence: the vocabulary in which collection protocols are written and against which methods are judged. **ISO 17025** is the laboratory-competence standard: documented methods, validated tools, trained personnel, quality management: the reason "ISO 17025-aligned" appears in credible providers' descriptions and should appear in your instruction questions.
- **The Forensic Science Regulator Code** is statutory in England and Wales for forensic science activities in the criminal justice system: practitioners must declare compliance or non-compliance, and the declaration travels with the evidence. Civil work is not directly bound, but civil courts hear from the same experts, and the Code's expectations (validated methods, competence, quality systems) define the professional baseline everywhere.
- **The procedural overlay:** in civil disclosure, PD 57AD and CPR 31 assume preserved, intact documents (metadata included) and the disclosure certificate confirms the process; expert evidence about collections comes under CPR Part 35 or CrimPR Part 19 with its overriding duty to the court. UK GDPR runs alongside: collection is processing, minimisation applies, and the forensic discipline of documented, scoped acquisition is also the data-protection discipline.

§ 1 2 · SCALE WITHOUT SACRIFICE

Forensic collection and proportionality

A persistent misunderstanding equates "forensic" with "everything": full images of every device, at full cost, in every case. The truth is more useful:

- **Scope is a dial; discipline is not.** The spectrum runs from full physical images (deleted-data recovery, artefact-level analysis, the strongest evidence for contested devices) through logical acquisitions to targeted collections of defined sources. Where a matter sits on that spectrum is a proportionality decision (cost, intrusiveness, what the issues need); every point on the spectrum can still be repeatable, hashed, logged, metadata-complete and continuous.
- **Targeted done forensically beats everything done casually.** A two-hour documented, hashed export of the three mailboxes that matter is better evidence than an undocumented image of the whole server, and it is cheaper, faster and kinder to UK GDPR minimisation. The choice between methods is the subject of its own guide in this series; the constant across all of them is the seven pillars.
- **Forensic triggers change the answer:** where deletion is suspected, authenticity is challenged, a device itself is the crime scene, or an employee departure smells of exfiltration, the fuller acquisition earns its cost, because the evidence lives below the file system where targeted methods do not reach. Escalation criteria belong in the collection plan before collection starts.
- **Preserve broad, collect narrow:** the cheap insurance is imaging or sequestering the contested few sources completely while collecting from the rest in a targeted way: scope can widen later only if the source still exists in its original state.

§ 1 3 · IN THE WILD

Worked examples

EXAMPLE 1 · THE HELPFUL IT DEPARTMENT

In a shareholder dispute, the company's IT manager, asked to "secure" a departed director's laptop, copied his profile to a network share, ran a malware scan "to be safe", and reinstalled the machine for a new joiner. The copy carried creation dates of the copying afternoon; the scan updated access times across the profile; the reinstall destroyed the deleted material and USB history the dispute later turned on. Nothing dishonest occurred, and the evidential damage was total: the company's expert could only report what the surviving copy could not prove, and the director's counsel spent a productive half-day on the theme of evidence handled "with all the care of a house clearance". A forensic image on day one would have cost a few hundred pounds.

EXAMPLE 2 · THE CHALLENGE THAT VERIFICATION ENDED

In a fraud claim, the defendant alleged that an incriminating spreadsheet had been planted on his imaged laptop after seizure. The laboratory's response was the file of this guide: the acquisition worksheet (tool, version, write-blocker, operator, clock offset), the image hashes computed at acquisition, the custody record showing sealed storage and two signed transfers, and matching hash re-verifications at each. The defendant's own expert was invited to re-hash the master image; the values matched; the allegation was withdrawn before it was ever put to a judge. The collection did not win the case, but it made one entire species of defence impossible.

EXAMPLE 3 · TARGETED, AND STILL FORENSIC

In an unfair dismissal claim with a £30,000 schedule of loss, full imaging of the employer's systems would have been absurd. The examiner instead performed a documented targeted collection: two mailboxes and one shared folder exported by a recorded method, hashed on export, clock context noted, custody record opened, four pages of notes. Total cost under a day's fees. When the claimant later disputed the completeness of an email chain, the export manifest and hashes answered in one letter what would otherwise have become a disclosure application. Small matter, small collection, full discipline.

§ 14 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The first 48 hours problem:** IT staff or managers opening, copying and tidying before anyone with forensic training is consulted; the single largest source of spoiled evidence in civil disputes.
- **Drag-and-drop "preservation":** content saved, provability destroyed, silently.
- **No hashes at acquisition:** integrity becomes assertion, permanently, because the moment to compute the baseline cannot be revisited.
- **Reconstructed records:** custody forms and notes written up weeks later; visibly retrospective, and cross-examined as such.
- **Examining the only copy:** analysis performed directly on the acquisition with no preserved master, so every analytical act is also a handling of the best evidence.
- **Clock assumptions:** device times taken at face value, offsets unrecorded, chronologies built on sand.
- **Metadata-blind exports:** emails saved as loose files without headers, documents printed to PDF "for convenience", cloud data downloaded through a browser.
- **Casual transport and storage:** evidence drives in desk drawers, couriered unsealed, copied to personal laptops; each a chain-of-custody gap wearing a lanyard.
- **Forensic-everything reflex:** full images of forty devices where the issues needed three, burning budget and goodwill and inviting the proportionality fight from the other direction.

Technical limitations

- **Some change is unavoidable:** live systems, encrypted devices and cloud platforms cannot always be acquired with zero alteration; the standard is not magic stillness but competent action, recorded and explicable (the NPCC second principle exists for exactly this).
- **Collection preserves what exists:** it cannot resurrect what routine retention deleted before anyone acted, which is why preservation instructions precede collection in every competent plan.
- **Hashes prove integrity, not meaning:** a verified image of a device proves the device's contents are before the court unaltered; what those contents establish (who typed, who knew, who intended) is analysis, a different discipline with its own limits.
- **Cloud sources shift the ground:** provider-side data is acquired through export mechanisms whose behaviour is the provider's, not the examiner's; competent practice documents the mechanism and its known characteristics, and a later guide in this series covers cloud collection in depth.

§ 15 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Who has touched the relevant devices and accounts since the dispute arose, and what exactly did they do? (Asked without blame; the answer shapes everything.)
- Where are the devices now, who controls the credentials, and can we sequester them today?
- Is anything auto-deleting while we speak (retention policies, chat expiry, leaver processes)?

Ask your opponent

- Please describe the method of collection of the disclosed material: tools and versions, operators, dates, and whether acquisition hashes were computed and retained.
- Please confirm whether original sources were preserved and remain available for verification, and provide the chain-of-custody records for the exhibits relied upon.
- Please confirm the time-zone handling and any clock offsets recorded at acquisition.

Ask your eDiscovery / forensic provider

- What method do you propose per source, and why is it proportionate; what are the escalation triggers to fuller acquisition?
- What will the acquisition record contain, and can we see a template of your worksheet, custody form and hash schedule?
- What standards do you work to (NPCC principles, ISO 17025 alignment, ISO/IEC 27037), and who would sign a CPR Part 35 report if this is challenged?
- How will originals or master copies be preserved, stored and made available to the other side's expert if required?

SUGGESTED WORDING · INSTRUCTION PARAGRAPH FOR A FORENSIC COLLECTION

> "You are instructed to collect the sources listed in Schedule 1 in a forensically sound manner, namely: by documented, repeatable methods appropriate to each source; preserving original data unaltered so far as practicable, with any unavoidable changes recorded and explained; computing and recording cryptographic hash values at acquisition and verifying them on each subsequent transfer; preserving all associated metadata; recording the source system clock against reference time; maintaining contemporaneous notes and tool logs; and opening and maintaining chain-of-custody records for each exhibit from the point of acquisition. Original devices or sealed master copies are to be preserved unexamined and stored securely. Please confirm the proposed method per source, with costs, before acquisition begins, and flag immediately any source at risk of alteration or loss in the interim."

SUGGESTED WORDING · THE STANDSTILL EMAIL TO THE CLIENT (SEND FIRST, TODAY)

> "Until collection is arranged, please ensure that nobody opens, copies, previews, scans, tidies, reinstalls or logs into any of the devices or accounts we discussed, including IT support acting helpfully. Do not forward yourself documents. Suspend any automatic deletion you can (we will confirm the list). The devices and accounts should simply be left alone and kept secure. This preserves both the evidence and our ability to prove it is the evidence; an hour of well-meant tidying can undo both."

§ 16 · QUICK CONTROL

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

The forensic collection checklist

- ☐ Standstill instruction issued before anyone touches sources; auto-deletion suspended
- ☐ Method chosen per source, proportionate, with escalation triggers recorded
- ☐ Tools, versions, settings and operators documented; acquisition worksheet completed contemporaneously
- ☐ Source clock checked against reference time; offset recorded; time-zone handling documented
- ☐ Hashes computed at acquisition, recorded, and re-verified on every transfer
- ☐ Originals or sealed masters preserved unexamined; analysis on verified working copies only
- ☐ Metadata acquired with content; no browser downloads, loose-file exports or convenience PDFs
- ☐ Exhibit references assigned and chain-of-custody records opened at acquisition, signed at every movement
- ☐ Deviations and incidents logged at the time with explanation
- ☐ Acquisition records, tool logs and custody forms filed as a set, ready for exchange or Part 35 exhibit

Red flags

- "IT have already taken a copy."
- A collection with no hash values, or hashes computed for the first time long after acquisition.
- Custody records in one handwriting, one ink, one sitting.
- Originals reformatted, reissued or "returned to the pool".
- Timestamps that cluster on the collection date.
- An opponent who cannot say what tool collected their disclosure.
- Any account of the collection that changes between letters.

When to involve a digital forensic expert

Immediately, for the method decision: the choice between imaging, logical acquisition and targeted export, and the escalation triggers between them, is exactly the judgment an examiner supplies cheaply at the start and expensively as a rescue. Involve the laboratory as of course where a device or account is itself contested (deletion, planting, backdating alleged), where the collection will face a hostile expert, where sources are technically awkward (encryption, live servers, failing media, cloud tenancies), and where criminal proceedings are possible, since the Forensic Science Regulator Code's expectations then attach and compliance declarations must accompany the work. And involve them defensively when the other side's collection looks casual: a short expert review of their acquisition records (or the absence of any) often produces the most cost-effective paragraphs in your next letter.

§ 17 · COMMON QUESTIONS

Frequently asked questions

Is evidence collected non-forensically inadmissible?

Not automatically: civil courts admit relevant evidence and weigh it, and plenty of cases proceed on imperfectly collected material. The cost is weight and vulnerability: every gap becomes a submission for the other side, authenticity challenges cannot be conclusively answered, and where the collection's flaws touch the very documents in dispute, the evidence may be effectively neutralised. Forensic collection is not an admissibility ticket; it is the difference between evidence that withstands attack and evidence that invites it.

Our IT team is competent. Why can they not do the collection?

Sometimes, for genuinely routine sources under examiner supervision and to a written protocol, they can, and a good laboratory will design exactly that hybrid to save cost. What IT teams lack is not skill but forensic method and independence: their tools are administrative rather than evidential, their notes are rarely contemporaneous, and as employees of a party their handling is an easy target. The question the court will ask is not "were they clever?" but "can this be verified, and by whom?"

Does forensic collection mean imaging everything, at huge cost?

No: that is the most common misconception in instructions. Scope (image, logical, targeted) is a proportionality decision made source by source; the forensic pillars (repeatability, hashing, logging, metadata, custody) apply at every scope and add modestly to cost. A targeted collection done forensically is routinely the right answer in civil matters, with full imaging reserved for the contested few sources where deleted data and artefact-level analysis may matter.

What does forensic collection actually cost?

Ranges, honestly stated: a straightforward single-device image or a targeted mailbox collection is typically hundreds to low thousands of pounds; multi-source corporate collections scale with source count and logistics rather than drama. The comparison that matters is with the alternative: one authenticity challenge that cannot be answered, or one re-collection ordered because the first was casual, costs more than the forensic version of the entire exercise would have.

The other side collected their disclosure casually. What do we do with that?

Ask the questions in §15 in correspondence: method, tools, hashes, custody, clock handling. If the answers are absent or embarrassing, the options escalate: requiring re-collection or verification of specific contested exhibits, an expert-review protocol, adverse submissions on weight, and in serious cases an application concerning the integrity of their disclosure. Calibrate to materiality: casual collection of peripheral documents is a point; casual collection of the document the case turns on is a theme.

How long should collected evidence and its records be kept?

Until the proceedings and any realistic appeal are exhausted, and in regulated or criminal-adjacent contexts for the period the applicable rules require; agree the retention and eventual destruction or return in writing with the laboratory at the outset. The custody record should close the loop: the entry recording certified destruction or return is the chain's final link, and UK GDPR minimisation is the reason indefinite retention is not the safe default it appears.

§ 18 · REFERENCE

Glossary

Acquisition
The forensic act of obtaining data from a source into a verifiable evidential form.

Acquisition worksheet
The contemporaneous record of an acquisition: source, tool, settings, operator, times, hashes, incidents.

Audit trail
The combined human notes and tool logs recording every action taken on the evidence.

Chain of custody
The unbroken signed record of possession, storage and transfer from acquisition to court.

Clock offset
The recorded difference between a source system's clock and reference time at acquisition.

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

Hash value
A cryptographic fingerprint (MD5, SHA-1, SHA-256) proving data identity and integrity.

Logical acquisition
Collection of the files and structures visible to the operating system, without unallocated space.

Master copy
The preserved, unexamined acquisition from which verified working copies are derived.

Targeted collection
Documented forensic collection of defined sources or data sets rather than whole devices.

Working copy
A hash-verified duplicate on which analysis is performed, protecting the master.

Write blocker
Hardware or software preventing any write to an evidence source during acquisition.

Sources and authoritative references

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

- cflab.uk, digital forensics services (forensic acquisition of computers, servers, mobile devices and cloud sources under NPCC principles and ISO 17025-aligned procedures, with chain-of-custody documentation and CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services
- cflab.uk, mobile phone forensics (extraction methodology and preservation practice for handsets and messaging data) and the lawyer guides library of which this series forms part: cflab.uk/mobile-phone-forensics · cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (defensible, documented collection at disclosure scale; "defensibility is built, not retrofitted"): 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 (successor to the ACPO Good Practice Guide for Digital Evidence): college.police.uk, digital devices guidance
- Forensic Science Regulator, statutory Code of Practice (Forensic Science Regulator Act 2021): gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 (identification, collection, acquisition and preservation of digital evidence) and ISO/IEC 17025 (laboratory competence): iso.org, 27037 · iso.org, 17025
- CPR Part 31 / PD 31B and Practice Direction 57AD (preservation and disclosure of electronic documents, including metadata): justice.gov.uk, PD 31B · justice.gov.uk, PD 57AD
- CPR Part 35 (experts) and CrimPR Part 19: justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19

- ICO, UK GDPR guidance including data minimisation: ico.org.uk

DISCLAIMER

This publication provides general information about forensic data collection in the United Kingdom as at August 2026. The worked examples are fictional illustrations and all figures are illustrative. 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

Forensic collection is the laboratory's core trade. Our examiners acquire computers, servers, NAS devices, mobile handsets, email systems and cloud tenancies by documented, repeatable methods under the NPCC principles and ISO 17025-aligned procedures: write-blocked imaging where the matter needs depth, targeted and hybrid collections where proportionality points that way, always hashed at acquisition, logged contemporaneously, and held under chain-of-custody records that have been tested in the Crown Court, County Court, High Court and employment tribunals. Through **e-discovery.uk** the same discipline scales to disclosure exercises: collection planned source by source with escalation triggers, feeding culled, verified data into processing and review so defensibility and proportionality arrive together. We design standstill and preservation instructions, supervise or train in-house IT for hybrid collections, review opposing parties' acquisition records, and report under CPR Part 35 / CrimPR Part 19 with Forensic Science Regulator Code compliance declared where criminal-justice work requires it. 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