COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Forensic Image, Logical Extraction or Targeted Collection?

Choosing the Right Depth of Acquisition, Source by Source

Every collection decision is a choice of depth: a bit-for-bit forensic image capturing everything including the deleted; a logical extraction of the files and structures the operating system can see; or a targeted collection of defined mailboxes, folders and date ranges. Each is the right answer somewhere and an expensive mistake somewhere else. This guide compares the three methods honestly: what each captures and misses, what each costs through the whole disclosure chain, the risks each carries, and the decision framework that matches depth to evidential need while preserving the option to go deeper if the case turns.

⏱ 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 all three acquisition methods daily, and (more usefully) advise on which to use where: full images where a device is itself in issue, logical and targeted collections where proportionality points that way, and hybrid plans with escalation triggers where the honest answer is "it depends on what we find". Its eDiscovery arm, **e-discovery.uk**, feeds the chosen method into the disclosure pipeline, where the collection decision quietly sets most of the eventual bill.

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

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: DEPTH IS CHOSEN PER SOURCE, AND THE OPTION TO GO DEEPER IS PRESERVED

The three acquisition methods sit on a spectrum of depth. A **forensic (physical) image** copies a storage medium bit for bit: every active file, plus deleted material, unallocated space and the system artefacts that support attribution, timeline and recovery work; it is the strongest evidence and the largest, slowest, most intrusive and most expensive acquisition. A **logical extraction** copies the files and structures the operating system presents, with their metadata, but not (in general) the deleted and unallocated layers; it is faster, smaller, and the practical ceiling for many servers and cloud sources. A **targeted collection** acquires defined data (named mailboxes, folders, custodians, date ranges) by documented forensic methods; it is the smallest footprint, the cheapest through the whole disclosure chain, and the friendliest to UK GDPR minimisation. None of the three is "the forensic one": all three, done properly, honour the pillars of repeatable method, hashing, logging, metadata and custody. The choice is a per-source judgment matching depth to what the issues actually need from that source, and the professional's hedge is the hybrid: image or sequester the few contested sources completely, collect the rest at proportionate depth, and write the escalation triggers down before collection starts.

- **Depth buys the invisible layers.** Deleted files, wiping traces, USB and execution artefacts, unallocated fragments: these exist below the file system, and only imaging (or, on mobiles, the fuller extraction levels) reaches them. If the case may turn on what was deleted or done, depth is not optional.
- **Most sources do not need the invisible layers.** In the ordinary commercial dispute, the evidence is the content of known repositories: mailboxes, chat, file shares, cloud drives. Targeted and logical methods collect exactly that, verified and metadata-intact, at a fraction of the chain cost.
- **The collection decision is a budget decision.** Every gigabyte acquired multiplies through processing, hosting and review; imaging everything is the classic first step of the shocking bill, and the companion costs guide's arithmetic applies from this moment.
- **Hindsight is managed by preservation, not by over-collection.** The fear behind "image everything" is "what if we need it later?" The answer is to preserve broadly (cheap) while collecting narrowly (proportionate), with written triggers for going deeper: the option survives without the cost being incurred.
- **Method is disclosed and defended.** Whatever is chosen will be described in the DRD, questioned by opponents and possibly examined under CPR Part 35; a written per-source rationale, made at the time, is what turns "why did you not image?" from an accusation into a paragraph.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: a false binary

Instructions to collect tend to arrive in one of two broken forms. The first says *"image everything, we cannot take risks"*: fourteen laptops, three servers and a NAS, acquired in full, at full cost, most of it operating-system noise and personal data nobody needed, all of it now expanding through processing into a hosted, reviewable, GDPR-relevant mass. The second says *"just grab the mailboxes, keep it cheap"*: quick exports, no analysis of whether any source is contested, and six months later a deletion allegation lands against a laptop that was reissued to a new starter in week two.

Both forms make the same mistake: they choose a method before analysing the sources. The right question is never "forensic or quick?" (a false binary, since every method can be forensically disciplined) but, for each source: *what could this source contribute to the issues, does that contribution live in the visible files or the invisible layers, is this source itself likely to be contested, and what does each depth cost here?* Answering that per source produces the normal professional outcome: one or two devices imaged, the email and cloud estate collected targeted, the file server acquired logically share by share, and a written plan that says why, with triggers for changing the answer. This guide equips lawyers to have exactly that conversation, and to recognise when a provider or opponent has skipped it.

§ 0 3 · TERMS OF ART

The three methods, properly defined

Forensic (physical) image

- **What it is:** a verified bit-for-bit copy of an entire storage medium (disk, SSD, phone storage where achievable), acquired write-blocked into a forensic container format (E01/Ex01 or raw) with sector-level completeness, hashed at acquisition.
- **What it uniquely captures:** deleted files and their remnants, unallocated and slack space, file-system journals, volume shadow copies, and the artefact layer (registry, event logs, link files, USB and execution traces) in its complete, analysable state: the raw material of recovery, attribution and timeline work.
- **Its natural home:** devices that are themselves in issue: the exfiltration suspect's laptop, the machine where backdating is alleged, the computer whose deletions are the story.

Logical extraction

- **What it is:** acquisition of the files, folders and structures the operating system exposes, with their metadata, into a verified container (for example a logical evidence file), by forensic tools and method. On mobile devices, "logical" and the fuller "file system" extractions are distinct levels with their own guide later in this series; the principle is the same: the visible estate, not the sectors beneath it.
- **What it captures and misses:** everything a user or administrator could see, metadata intact; not, in general, deleted material in unallocated space, and not every artefact in its richest form. Some deleted-item classes survive anyway (recycle bins, snapshots, retention holds), which is why "logical means no deleted data" is only mostly true.
- **Its natural home:** sources too large, too live or too critical to image (production servers, multi-terabyte arrays), and sources where the visible estate is the whole evidential interest.

Targeted collection

- **What it is:** forensic acquisition of defined data sets: named custodians' mailboxes, specific shares and folders, date-bounded exports from cloud platforms, particular chat channels: scoped in advance, collected by documented tools with hashing, manifests and logs.
- **What it captures and misses:** exactly what was scoped, verified and metadata-intact; nothing outside the scope, including the context, the adjacent folder, and anything whose relevance emerges later. The scope document is therefore part of the evidence, and scope errors are this method's characteristic failure.
- **Its natural home:** disclosure exercises across cooperative estates, where the issues define the repositories and proportionality (and UK GDPR minimisation) reward precision.

§ 0 4 · SIDE BY SIDE

The comparison table

	FORENSIC IMAGE	LOGICAL EXTRACTION	TARGETED COLLECTION
Captures	Everything on the medium: active, deleted, unallocated, artefacts, snapshots	The visible file estate with metadata; some recoverable classes (bins, snapshots) incidentally	The scoped data sets, verified, metadata-intact
Misses	Nothing on the medium (cloud and off-device data still separate)	Unallocated space, most deleted material, artefact depth	Everything outside scope, including later-relevant context
Volume acquired	The whole medium: maximal	The active estate: intermediate	The scoped subset: minimal
Time and intrusion	Hours per device; device out of service or acquired live	Faster; often runnable on live systems with low disruption	Fastest; frequently server-side or remote with no user impact
Downstream chain cost	Highest: maximal processing, hosting and review exposure	Intermediate	Lowest: culling done by scope at source
UK GDPR posture	Broadest personal-data capture; needs justification and handling controls	Intermediate	Most aligned with minimisation
Analytical ceiling	Full: recovery, attribution, timeline, artefact work	Content and metadata analysis; limited depth work	Content and metadata analysis within scope only
Characteristic risk	Cost, delay, over-collection, review burden	The deleted layer assumed absent when it mattered	Scope error; completeness challenge; hindsight regret
Typical cost order	£ per device: highest acquisition cost, highest chain cost	Intermediate	Lowest, often by an order of magnitude through the chain

All three rows share what the previous guide established: documented method, hashing at acquisition, contemporaneous logs, preserved metadata and chain of custody. The table compares depth, not discipline.

§ 0 5 · FIT

Matching method to evidential need

- **Deletion, wiping or concealment in issue → image.** The evidence of what was deleted, when, and by what means lives in unallocated space, journals, shadow copies and artefacts: below the reach of logical and targeted methods. The same logic covers suspected backdating and manipulation, where artefact corroboration decides authenticity.
- **Attribution and conduct in issue → image.** Who was logged in, what was executed, which USB devices connected, what was opened: the artefact layer answers these, and it is captured whole only by imaging (and analysed from it).
- **Content of known repositories in issue → targeted.** Where the case is what the emails, chats and documents say (the ordinary commercial dispute), targeted collection of those repositories, custodian by custodian, is the proportionate fit, and the fastest route to review.
- **Large, live or critical infrastructure → logical or targeted, by design.** Production servers and multi-terabyte arrays are rarely imaged in full in civil matters: the disruption and volume are unjustifiable, and the evidential interest is almost always specific shares and datasets. Acquire those logically or targeted, with server logs collected alongside; the dedicated servers guide later in this series goes deeper.
- **Mobile devices → the fullest extraction the device supports,** because phone acquisition opportunities are fragile (locks, updates, remote wipes) and the marginal cost of fuller over lighter extraction is small at the moment of access and enormous afterwards. The mobile guide treats the levels properly.
- **Uncertain sources → preserve at depth, collect at proportion.** Where a source might become contested but is not yet, image or sequester it (cheap, no processing) and collect from it targeted; the depth sits in the evidence store, waiting for a trigger.

§ 0 6 · THE MONEY

Cost and proportionality: the chain consequences

- **Acquisition cost is the small difference; chain cost is the large one.** Imaging a laptop versus collecting its user folders differs by hundreds of pounds at acquisition; the difference downstream (the imaged gigabytes expanding through processing, sitting in hosting for the matter's life, and surfacing documents into review) is routinely tens of thousands. The collection method is the first term of the multiplication chain, and the companion costs guide's arithmetic starts here.
- **Images need not enter the chain.** The professional pattern that reconciles depth with cost: acquire the image, preserve it in the evidence store, and promote into processing only targeted extractions from it. Depth for the analyst, proportion for the reviewer, and the DRD describes both honestly.
- **Proportionality is argued per source, with this table.** "We imaged the two devices where deletion is alleged; we collected eleven custodians' mailboxes targeted; here is the per-source rationale and the cost of each alternative" is a DRD entry and a CMC answer that writes itself. The blanket versions ("we imaged everything to be safe" / "we kept it light to save cost") both invite the fight.
- **Minimisation is a tailwind, not an obstacle.** UK GDPR's minimisation principle points exactly where proportionality points: collect what the purpose needs. Targeted-by-default with reasoned exceptions is simultaneously the cheap posture, the defensible posture and the lawful-processing posture, which is a rare alignment worth exploiting in correspondence.

§ 0 7 · THE DECISION

The decision tree

Run per source, and record the answer against each:

Q 1
Is this source itself contested, or realistically likely to be: deletion, wiping, exfiltration, backdating, manipulation or attribution in issue?

YES → **Forensic image** (or fullest available mobile extraction), promptly, before reissue, repair or further use; analysis and targeted promotion from the image.

NO ↓

Q 2
Could deleted or below-file-system material realistically matter here, even without a current allegation?

YES → **Image and hold:** acquire or sequester at depth into the evidence store; collect targeted for review; define the trigger that would send the image to analysis.

NO ↓

Q 3
Is the source too large, live or critical to image proportionately (servers, arrays, cloud tenancies)?

YES → **Logical or targeted acquisition** of the relevant shares, sites and datasets, with system and audit logs collected alongside and the limitation recorded.

NO ↓

Q 4
Do the issues define specific repositories, custodians and date ranges within this source?

YES → **Targeted collection** to a written scope, hashed and manifested, with the source preserved (hold, sequestration or in-place preservation) as the hindsight hedge.

NO → **Logical extraction** of the source, with culling deferred to processing where scope cannot yet be written; revisit when it can.

Two rules govern every branch. First, the answer is recorded, per source, at the time: the one-line rationale is the future defence. Second, triggers for escalation (an allegation made, a gap found, a custodian elevated) are written into the plan, because the tree is re-run when facts change, and the preserved depth is what makes re-running it possible.

§ 0 8 · HONEST LEDGER

The honest risk register of each method

Forensic image

- **Cost and delay,** at acquisition and through the chain, particularly where images are promoted wholesale into processing.
- **Over-collection:** the whole medium includes personal, privileged and irrelevant material at maximum breadth; UK GDPR and confidentiality handling must be designed, not assumed.
- **False comfort:** imaging the device does not collect the cloud, the phone or the personal account; "we imaged everything" often means "we imaged the things that were easy to image".

Logical extraction

- **The deleted layer is (mostly) absent,** and if deletion later becomes the issue, the moment to capture it has usually passed with the source's continued use.
- **Artefact depth is limited:** attribution questions may be answerable only partially, and the limitation should be stated before an opponent states it.
- **Live-system variance:** extractions from running systems capture a moving estate; the acquisition record must say what was running and when.

Targeted collection

- **Scope error is silent:** the folder not listed, the archive mailbox nobody mentioned, the date range set one quarter short: nothing in the method reveals what the scope missed.
- **Completeness challenges:** "how do you know you got everything relevant?" is the standing question; the answers are the scope's documented derivation (interviews, data maps, sampling) and the preserved source behind it.
- **Hindsight risk:** issues evolve; yesterday's proportionate scope is tomorrow's gap. The hedge, again, is preservation plus triggers, and a scope revisited at each pleading milestone.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE HYBRID THAT FITTED THE CASE

A departing sales director was suspected of taking the pricing book. The plan, written in a page: his laptop and desktop imaged in full within 48 hours (contested devices, Q1 yes); his mailbox, OneDrive and the sales share collected targeted for review; the company's remaining custodians preserved in place, collection deferred. Analysis of the images found USB connection artefacts and a cloud-upload trace in the days before resignation; the targeted collections supplied the correspondence context; the uncollected estate never needed touching. Total acquisition spend was a quarter of the "image the department" alternative, and every finding that mattered came from the two devices the tree had sent to depth.

EXAMPLE 2 · THE BLANKET INSTRUCTION

In a warranty dispute with no allegation against any device, panicked instructions ordered full images of nineteen laptops "to be safe". Nineteen images entered processing; 4.1 TB expanded, hosted for the matter's 26-month life; the review population tripled on operating-system noise and personal material; two employees raised grievances about holiday photographs in the review set; and at no point did any issue in the case require a single artefact from a single image. The eventual bill exceeded the assessed budget by a factor the firm's client did not enjoy discussing, and the DRD's honest answer to "why?" was that nobody had asked the per-source question. Depth was bought where nothing needed it; the safety it purchased was zero.

EXAMPLE 3 · THE TRIGGER THAT FIRED

A fraud claim began with targeted collection across six custodians, plus one precaution: the finance manager's laptop, though uncontested at the time, was imaged and sequestered under the plan's Q2 branch, with a written trigger ("any allegation concerning deletion or alteration of accounting records"). Fourteen months later the defence alleged that a key spreadsheet had been fabricated after the event. The sequestered image went to analysis: shadow copies held four prior versions, and file-system metadata dated the sequence conclusively in the claimant's favour. The £600 imaging decision, made when nobody needed it, decided the point on which the claim turned; the nineteen-laptop version of the same instinct would have cost 300 times more and added nothing.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Method chosen before sources are analysed:** both blanket forms ("image everything" / "keep it light") applied estate-wide without the per-source question.
- **Contested devices collected lightly,** then reissued, wiped or sold: the depth destroyed exactly where it was needed, unrecoverably.
- **Images promoted wholesale into processing,** converting an evidential asset into a hosting and review liability; promote targeted extractions, hold the image.
- **No written rationale:** the method defensible at the time, indefensible two years later because nobody recorded why.
- **No escalation triggers:** the plan static while the case moves; scope gaps discovered by the opponent instead of the diary.
- **"Imaged" treated as "collected":** the cloud, phones and personal accounts forgotten because the laptops felt thorough.
- **Targeted scope written without interviews or data maps,** guaranteeing the silent miss.
- **Logical extraction of a device facing a deletion allegation,** the one pairing the table forbids.

Technical limitations

- **Modern hardware complicates "physical":** SSD wear-levelling and TRIM, encrypted volumes and soldered storage mean a bit-for-bit image is not always the archaeological trove it was on spinning disks; deleted-data expectations should be calibrated by an examiner per device, honestly.
- **Cloud sources have no medium to image:** acquisition depth there is defined by provider export mechanisms and APIs; the equivalent of "depth" is completeness of export plus audit-log collection, covered in the cloud guides of this series.
- **Live systems move:** any acquisition of a running source is a snapshot of motion; the record of when and what mitigates, but cannot remove, the variance.
- **No method collects what no longer exists:** the choice of depth operates on the source as found; preservation speed, the previous guide's subject, governs what there is to find.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which devices or accounts could plausibly become contested (departures, grievances, the individuals at the centre of the story)? Those are the depth candidates.
- What happens to leavers' devices, and can the reissue queue be paused today for the names on our list?
- Where does the estate hold the repositories the issues point at, so scope can be written from the data map rather than memory?

Ask your opponent

- Please state, per source, the acquisition method used (image, logical, targeted), the tools, and the scope definitions applied to any targeted collection.
- For devices connected to the matters in issue, please confirm whether forensic images were taken and preserved, and if not, the current state and whereabouts of the devices.
- Please provide the rationale for the method chosen for [the contested source], and confirm whether the source remains available for deeper acquisition.

Ask your eDiscovery / forensic provider

- Walk us through the tree per source: which go to image, which to logical, which to targeted, and the one-line rationale for each?
- What would each alternative cost, at acquisition and through the chain, so the DRD can state the choice as arithmetic?
- Where images are taken, what is promoted into processing, and how is the rest held?
- What escalation triggers do you recommend writing into the plan, and what does invoking one cost and take?

SUGGESTED WORDING · INSTRUCTION PARAGRAPH (METHOD PER SOURCE WITH TRIGGERS)

> "Acquisition is to proceed per the schedule: the devices at Part A are to be forensically imaged in full and the images preserved unexamined pending instructions, with targeted extractions promoted for processing as separately directed; the sources at Part B are to be collected by targeted forensic methods to the written scopes annexed, each source being preserved [by hold / sequestration / retained image] against later need; the systems at Part C are to be acquired logically to the extent described, with associated system and audit logs collected contemporaneously. For each source, please record at the time the method applied and the reason. The following events are escalation triggers requiring immediate reference back to us before any further handling: [any allegation of deletion, alteration or exfiltration concerning a source; discovery of material gaps in a collected set; elevation of any individual to custodian status]. No source is to be reissued, rebuilt, repaired or disposed of without written confirmation."

SUGGESTED WORDING · DRD / CORRESPONDENCE PARAGRAPH EXPLAINING A MIXED APPROACH

> "Collection methodology was determined source by source. The two devices connected to the allegations at Issue 3 were forensically imaged in full on [dates] and the images are preserved; review material from them is promoted by targeted extraction. The mailboxes, OneDrive accounts and the [X] share of the remaining [n] custodians were collected by documented targeted methods to the scopes at Annex [n], each source remaining preserved. The [server], which cannot proportionately be imaged, was acquired logically as to the shares listed, with server logs collected alongside. Hash verification, acquisition records and chain-of-custody documentation exist for each source and can be made available to the court or to [opponent]'s expert on request."

§ 12 · QUICK CONTROL

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

The method-selection checklist

- ☐ Sources listed; the tree run and the answer recorded per source with a one-line rationale
- ☐ Contested and plausibly-contestable devices identified and sent to depth before reissue or further use
- ☐ Targeted scopes written from interviews and the data map, annexed, and dated
- ☐ Preservation in place behind every targeted and logical choice: the hindsight hedge
- ☐ Escalation triggers written, costed and diarised; the tree re-run at pleading milestones
- ☐ Images held in the evidence store; only targeted extractions promoted into processing
- ☐ Per-source costs of the alternatives obtained, so proportionality is arithmetic in the DRD
- ☐ UK GDPR posture recorded: minimisation served by scope, breadth justified where taken
- ☐ All methods executed to the seven pillars: hashed, logged, metadata-intact, custody-tracked
- ☐ Method disclosed accurately in the DRD and correspondence, matching what was actually done

Red flags

- Any estate-wide method sentence: "image everything" or "just the mailboxes".
- A contested device on the reissue pile, or already reissued.
- A targeted scope nobody interviewed for.
- Whole images sitting in hosting.
- No written rationale, no triggers, no plan revisit dates.
- An opponent who cannot say which method touched which source.
- "We imaged the laptops" offered as the complete answer in a cloud-and-phone dispute.

When to involve a digital forensic expert

At the tree, first: the per-source depth judgment is the examiner's core advisory product, cheap at planning and expensive as regret. Then wherever a Q1 answer is yes (the contested device goes to a laboratory, not an IT department), wherever hardware realities need calibrating (SSDs, encryption, mobiles, failing media), wherever servers and cloud tenancies need the logical-plus-logs design, and wherever an opponent's method choices look wrong for their facts: an examiner's short review of what a light collection cannot show about a contested source is frequently the foundation of the application that follows. The examiner also maintains the held images and the trigger machinery, so that going deeper later is a file movement, not an excavation.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is targeted collection defensible, or will we be criticised for not imaging?

Targeted collection is not merely defensible but the proportionate default in most civil disclosure, provided the discipline travels with it: a scope derived from interviews and the data map, forensic execution (hashes, manifests, logs), preservation behind it, and a recorded rationale. Criticism attaches not to the method but to its casual version: undocumented scope, no preservation, no reason. The question "why did you not image?" is answered in one sentence when the answer was written at the time.

Can we start light and upgrade to imaging later if needed?

Only if the source still exists in a meaningful state: continued use overwrites deleted material daily, and reissue or disposal ends the question. That is exactly why the framework separates preservation from collection: sequester or image the plausible-risk sources now (cheap, no processing), collect light, and the upgrade later is a decision, not a resurrection. Starting light with no preservation is the version that fails.

Do we need to image every custodian's laptop?

Almost never. In a typical matter the laptops that justify imaging are the small set connected to contested conduct; the remaining custodians' evidential contribution is their communications and documents, which live in server-side and cloud repositories reachable by targeted collection without touching the devices at all. The nineteen-laptop reflex buys volume, cost and grievances, not evidence: Example 2 is its biography.

How do phones fit this framework?

Awkwardly, which is why they get their own guide: mobile acquisition levels (logical, file system, physical where possible) are constrained by device, OS version and lock state rather than free choice, and access opportunities are fragile. The practical rule: when a phone matters and is accessible, take the fullest extraction the device supports at that moment, because the marginal cost is small and the opportunity may not recur; the depth decision is made by the device as much as the examiner.

Roughly what does each method cost?

Orders of magnitude, honestly: imaging a single computer typically runs from several hundred pounds to low four figures including verification and handling; logical and targeted collections often less per source, with server and cloud collections priced by scope and logistics. But acquisition prices mislead: the dominant difference is downstream, where an imaged-and-promoted estate can cost ten times a targeted one through processing, hosting and review. Price the chain per method, per source, and the comparison becomes real; the companion costs guide supplies the arithmetic.

What should we do when the other side chose the wrong method for a contested source?

Establish it in correspondence (method, tools, scope, whether the source survives), then act on what remains: if the device exists, seek preservation and deeper acquisition by agreement or application, promptly, before further use degrades it; if it was reissued or wiped after the dispute arose, the questions become preservation-duty questions, and the artefacts of the destruction itself may be examinable. Either way, an examiner's statement of what the chosen method cannot show about the contested issue converts a methodological quibble into a submission with teeth.

§ 14 · REFERENCE

Glossary

Artefact layer
System records (registry, logs, link files, execution traces) supporting attribution and timeline work; captured whole by imaging.

E01 / Ex01
Standard forensic image container formats with built-in integrity verification.

Escalation trigger
A pre-written event that sends a source from light collection to deeper acquisition or analysis.

Forensic (physical) image
A verified bit-for-bit copy of an entire storage medium, including deleted and unallocated content.

Hybrid plan
Depth for contested sources, proportion for the rest, preservation and triggers behind both.

Logical extraction
Forensic acquisition of the file estate the operating system exposes, metadata intact, without unallocated space.

Promotion
Moving acquired data into processing and hosting; held images are deliberately not promoted wholesale.

Scope document
The written definition of a targeted collection: custodians, repositories, ranges; part of the evidence.

Sequestration
Removing a source from use and holding it unaltered, with or without immediate acquisition.

Targeted collection
Forensic acquisition of defined data sets to a written scope, hashed and manifested.

TRIM / wear-levelling
SSD behaviours that erode deleted-data recovery; a reason imaging expectations are calibrated per device.

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

Sources and authoritative references

The method-selection 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 imaging, logical and targeted acquisition of computers, servers and mobile devices under NPCC principles, with preserved masters and CPR Part 35 reporting): cflab.uk/digital-forensics-services
- cflab.uk, mobile phone forensics (extraction levels and the fullest-available principle) and the lawyer guides library: cflab.uk/mobile-phone-forensics · cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection (targeted, documented collection as the proportionate default at disclosure scale) and Phase 02 · Preservation (the hold-and-trigger machinery behind light collection): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/preservation
- e-discovery.uk, practice principles ("you pay for substance, not volume") and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance
- ISO/IEC 27037:2012 (collection and acquisition guidance) and ISO/IEC 17025: iso.org, 27037 · iso.org, 17025
- CPR 31.7 / PD 31B (reasonable search, accessibility and expense factors) and PD 57AD (proportionate disclosure and the DRD): justice.gov.uk, PD 31B · justice.gov.uk, PD 57AD
- CPR Part 35 (experts): justice.gov.uk, Part 35 · ICO, UK GDPR guidance including data minimisation: ico.org.uk

DISCLAIMER

This publication provides general information about digital evidence acquisition methods 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

Method selection is the conversation we most like to have early, because it is where cases are made cheaper and stronger at the same time. Our examiners run the per-source tree with you, image the contested few under full laboratory discipline, design and execute targeted and logical collections to written scopes with hashes, manifests and custody records, and hold preserved depth (sealed images, sequestered devices) behind every light choice with the escalation triggers costed in advance. Through **e-discovery.uk**, targeted collections flow straight into culled processing so the proportionality argument and the budget tell the same story, and the DRD's methodology sections are drafted from what was actually done. Where an opponent's method does not fit their facts, we review their acquisition records and state, under CPR Part 35 / CrimPR Part 19 where needed, precisely what their chosen depth cannot show. 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