COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Digital Chain of Custody: A Practical Guide for Lawyers

Continuity, Transfer Records and the Documentation That Survives Court

Chain of custody is the unbroken, signed account of where evidence has been and who has touched it, from acquisition to courtroom. For digital evidence it has two strands: physical custody of devices and media, and logical custody of the data itself, proven by hash verification at every hop. This guide explains both strands, provides sample evidence-transfer records lawyers can adapt, and contrasts weak documentation with defensible documentation, side by side, so you can build the second and cross-examine the first.

⏱ Estimated reading time: 27 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Continuity of evidence, maintained from seizure to court, is a founding commitment of the laboratory: exhibit referencing, sealed storage, signed transfers and hash-verified handling are its daily routine, tested in the Crown Court, County Court, High Court and employment tribunals. Its eDiscovery arm, **e-discovery.uk**, extends the same continuity to disclosure-scale data movements between clients, platforms and parties.

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

§ CONTENTS

In this guide

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: CONTINUITY IS PROVEN, NEVER PRESUMED

Chain of custody is the answer, in writing, to the question every exhibit faces: where has this been, who has handled it, and how do we know it is unchanged? For digital evidence the answer has two strands that must run together. **Physical custody** tracks the tangible objects (devices, drives, sealed media) through exhibit references, tamper-evident sealing, secure storage, and a signed transfer record for every change of hands. **Logical custody** tracks the data itself, which is copied by design: hash values computed at acquisition and re-verified at every movement prove each copy true, so the chain follows the information as faithfully as the hardware. A chain kept from minute one costs minutes per event and makes interference allegations effectively unarguable; a chain reconstructed later is visibly a reconstruction, and every gap becomes a period the other side is entitled to populate with speculation. In civil proceedings a defective chain rarely excludes evidence outright, but it converts weight into argument at exactly the moments that decide cases, and in criminal and regulatory work the expectations are stricter still.

- **The chain starts at acquisition, or it starts compromised.** Exhibit references and custody forms opened at the point of collection are the discipline; anything begun later is memory in a form.
- **Every event is a row:** collected, sealed, stored, retrieved, copied, transferred, examined, returned, destroyed: each with date, time, persons, purpose, and hash verification where data moved. The form in §5 is deliberately boring; boring is what credibility looks like.
- **Digital custody includes systems:** which platforms held copies, who had access, what the access logs show. A perfect paper chain around an unverified network share is half a chain.
- **Breaks are managed, not hidden:** a gap discovered, documented, explained and bounded (with hashes proving no change across it) survives; a gap discovered by the other side does not.
- **Lawyers are custodians too:** exhibits couriered to counsel, USB sticks in DX pouches and review copies on firm laptops are all links in the chain, and the weakest link is usually outside the laboratory.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the question every exhibit must answer

Eighteen months after a laptop was collected, its contents are on a courtroom screen and opposing counsel rises: "Between March and November, where exactly was this device? Who could access the copy on your client's server? And how does the court know that what we are looking at is what was taken?" There are only two kinds of answer. The first is a file: a custody record showing every location, every handler, every signed transfer, with hash verifications bracketing each movement, offered to the questioner with the invitation to check. The second is testimony: people doing their best to remember, an IT manager "fairly sure" it stayed in the cabinet, a paralegal who "would have" logged the courier. The first answer ends the line of questioning; the second becomes the line of questioning.

The unfairness worth internalising is that both answers can describe identical, perfectly innocent handling. Nothing need have happened to the evidence for the second answer to damage it: the absence of the record is itself the damage, because continuity is proven, never presumed. That is the entire case for the modest paperwork this guide sets out: it is cheap, it is boring, and eighteen months later it is the difference between an exhibit and an argument.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 3 · THE TWO STRANDS

The two strands: physical and logical custody

- **Physical custody** governs objects: the laptop, the phone, the evidence drive holding the image. Its tools are the exhibit reference (a unique identifier assigned at collection and used everywhere thereafter), tamper-evident bags and seals with recorded seal numbers, a secure evidence store with controlled and logged access, and the transfer record signed by releaser and receiver for every movement, courier legs included (tracking numbers and sealed-condition confirmations at both ends).
- **Logical custody** governs data: the image, the export, the production set, each of which exists in multiple lawful copies. Its tools are the hash values from guide 34: computed at acquisition, recorded in the custody file, and re-verified whenever data is copied, moved, loaded to a platform or produced. A movement whose before-and-after values match is a proven-clean hop; a chain of such hops is continuity for information.
- **The strands interlock:** the physical record says the sealed drive travelled from laboratory to chambers on 14 May; the logical record says the image on it hashed identically before dispatch and on arrival. Either alone is incomplete: pristine hardware carrying unverified data, or verified data on hardware nobody tracked. Courts and hostile experts read the two together, and so should the lawyer building or attacking a chain.
- **Access control is the third rail of both:** who could reach the evidence store, who held platform credentials, what the access logs record. Continuity claims are only as strong as the answer to "who else could have touched it?", and the defensible answer is a short named list with logs behind it.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 4 · THE LIFECYCLE

The custody lifecycle, stage by stage

STAGE	CUSTODY ACTIONS
Acquisition / seizure	Exhibit reference assigned; item photographed and described (make, model, serials, condition); custody form opened; acquisition hashes recorded; item sealed, seal number logged
Transport	Transfer record signed out by releaser, signed in by receiver; courier legs tracked; seal integrity confirmed and noted at arrival; any seal change recorded with reason
Storage	Sealed item logged into the evidence store; location recorded; access to the store controlled, logged and auditable; environmental basics (security, fire, segregation from returns) maintained
Examination	Item signed out with purpose and time; work performed on hash-verified working copies, never the master; item resealed under a new recorded seal and signed back in; examination logged in case notes
Data movements	Every copy, platform load and production hashed before and after; recipients, methods (encrypted media, secure transfer) and dates recorded; production manifests retained
Return / destruction	Final disposition recorded: signed return to owner, or certified destruction with method and date; the closing entry that completes the chain and answers UK GDPR retention duties

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 5 · THE PAPERWORK

Sample records: the forms that do the work

Exhibit record (opened at acquisition, one per exhibit)

FIELD	ENTRY (ILLUSTRATIVE)
Exhibit reference	CFL/2481/EX03
Description	Laptop, [make/model], serial [n], lid scratched lower right, powered off when received
Source and authority	Collected from [person/location] under [instruction/order reference]
Date, time, place of acquisition	14 Mar 2026, 10:42, [address]; reference clock noted
Acquired by	[Examiner name], in presence of [witness]
Acquisition method and hashes	Write-blocked image to E01; MD5 [value]; SHA-256 [value]; worksheet ref [n]
Seal	Tamper-evident bag [seal number]; photograph ref [n]

Transfer record (one row per movement, appended to the exhibit record)

DATE / TIME	FROM (SIGNED)	TO (SIGNED)	PURPOSE	SEAL / HASH CHECK
14 Mar 10:55	[Examiner]	Evidence store	Storage post-acquisition	Seal [n] intact; image SHA-256 verified
02 Apr 09:20	Evidence store	[Examiner]	Examination per instruction [ref]	Seal [n] intact; opened; working copy hashed and matched
02 Apr 16:40	[Examiner]	Evidence store	Return post-examination	Resealed [new seal n]; master untouched, verified
14 May 08:30	Evidence store	[Courier, tracking n]	Delivery to [solicitors] per [ref]	Sealed [n]; copy drive SHA-256 [value] recorded pre-dispatch
14 May 12:05	[Courier]	[Recipient, signed]	Receipt	Seal [n] confirmed intact; drive hash re-verified on arrival, matched

Adapt freely: the columns are the discipline, not the branding. The features that make these forms work are unglamorous: opened at the event, completed at the event, one row per event with no gaps between rows, signatures from both sides of every transfer, and hash checks bracketing every data movement. A form with those properties can be handed to a hostile expert with confidence; that is its entire design goal.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 6 · SIDE BY SIDE

Weak versus defensible: the same events, two files

WEAK DOCUMENTATION SAYS	DEFENSIBLE DOCUMENTATION SAYS
"Laptop collected from head office in March."	Exhibit CFL/2481/EX03; collected 14 Mar 2026 10:42 from [named person, address]; photographed; serials recorded; sealed [seal n]
"Imaged and kept safe by IT."	Write-blocked E01 image, tool and version stated; MD5/ SHA-256 recorded in worksheet [n]; master sealed to evidence store, location [n]
"Sent the data over to the solicitors in the spring."	Transfer row: 14 May, encrypted drive, courier [tracking], hash pre-dispatch and on-receipt matched, signatures both ends
"Various people had access as needed."	Store access limited to [three named]; access log exhibited; platform accounts listed with roles and log extract
"The device was looked at again later; nothing was changed."	Sign-out 02 Apr [purpose, instruction ref]; working copy examined; master re-verified on return; reseal [new n]
"We are confident it is the same data."	Hash chain exhibited: acquisition values re-verified at each of five events, all matched; verification offered to opposing expert
(Nothing about the gap)	"Between [dates] the exhibit remained sealed in storage; no access-log entries; seal [n] intact at next sign-out; image hash unchanged across the period"

Read the columns as a cross-examiner: every left-hand entry generates questions ("which person? which day? who checked?"), and every right-hand entry answers them before they are asked. The left file describes handling; the right file proves it: the difference is not honesty but evidence, and tribunals weigh evidence.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 7 · BREAKS

What breaks a chain, and what a break actually costs

- **The classic breaks:** the undocumented interval (evidence "somewhere in the office" between entries); the unsigned transfer; the broken or unrecorded seal; the copy nobody hashed; the platform everyone could access; the examination on the master; the courier leg with no receipt; the record written up afterwards in one sitting.
- **The legal cost, calibrated:** in civil proceedings, admissibility usually survives (relevant evidence is admitted and weighed), but the break becomes a weight submission, a cross-examination theme, and, where the affected exhibit is central, sometimes the pivot of the case. In criminal proceedings the scrutiny is sharper (continuity is a standard element of exhibit proof, and the FSR Code raises procedural expectations), and in regulatory contexts a broken chain can undermine an entire investigative narrative.
- **Managing a break you find in your own chain:** document it now, at the moment of discovery, with what is known and not known; bound it (the hash values on either side of the gap, if they match, prove the data crossed it unchanged, which converts a custody gap into a custody blemish); explain it in the evidence before the other side raises it, because candour about a bounded gap reads entirely differently from a gap excavated in cross; and fix the process so the file shows one break, not a habit.
- **Exploiting a break in theirs:** establish it precisely in correspondence (the questions in §10), assess materiality honestly (a gap around a peripheral exhibit is a point; around the central exhibit, a theme), and put the choice to them: verification (if their masters and hashes exist) or weight submissions (if they do not). The most effective deployment is usually the quietest: the schedule of their gaps, exhibited, with each gap's unanswered question printed beside it.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 8 · IN THE WILD

Worked examples

EXAMPLE 1 · THE CABINET MONTHS

In an IP theft claim, the defendant's former laptop had been collected by the employer's HR team and kept "in the HR cabinet" for five months before forensic imaging. No exhibit reference, no seal, no log; four people held cabinet keys; the office moved floors in the interim. The image, once taken, was impeccably handled, and its hash chain from that day was perfect: which is precisely what the defence emphasised, because the perfection began five months too late. The judge admitted the evidence and discounted it in terms: the artefacts said the incriminating files were copied before the defendant left, but the unaccounted months meant the court "could not exclude intervening handling", and the inference the claimant needed was not drawn. Five months of cabinet storage, documented with a one-page log and a £2 seal, would have won the point.

EXAMPLE 2 · THE GAP THAT WAS BOUNDED AND SURVIVED

A laboratory discovered, during pre-trial preparation, that a transfer row was missing: an evidence drive had gone to counsel's chambers and back with only the outbound record completed. The response was §7 by the book: a note made at discovery; the courier's tracking data and chambers' receipt obtained and exhibited; and, decisively, the image's SHA-256 re-verified and matched against acquisition, bracketing the gap with mathematics. The expert's report disclosed the lapse in a paragraph, explained the bounding, and offered re-verification to the other side. Cross-examination attempted the theme and abandoned it inside two questions: "the hash matched, you say?" is not a promising line. One missing signature, candidly bounded, cost nothing; concealed and discovered, it would have cost the report's credibility.

EXAMPLE 3 · THE SCHEDULE OF THEIR GAPS

Defending a fraud claim built on the claimant's own collected devices, the defence served a request under §10: exhibit references, seals, transfer records, storage access, hash schedule. The answers, assembled into a one-page table, showed: no exhibit references; imaging performed by an office manager with consumer software; no acquisition hashes; the "original" phone factory-reset and reissued after copying; and the copies held on a shared drive with forty-plus users. The table was exhibited to a weight submission, unembellished. The claimant's central WhatsApp exhibits survived as evidence but arrived at trial carrying the table, and the settlement that followed the first day reflected what both counsel could see the tribunal thinking. Nothing was alleged; the schedule merely asked the questions the file could not answer.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 9 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Starting the chain at the laboratory door,** leaving the client-side weeks (the cabinet, the IT share) undocumented: the commonest and most damaging pattern.
- **Reconstructed records:** one handwriting, one ink, one afternoon; visibly retrospective and cross-examined as such.
- **The unhashed hop:** data copied to a review platform or produced to the other side with no verification bracketing the movement.
- **Everyone-access storage:** evidence on shares and platforms whose access answer is "the team".
- **Examining the master** because making a working copy felt like delay.
- **The lawyer-side gap:** exhibits in DX pouches, counsel's unlogged USB stick, the review laptop that went home: the chain's weakest links are usually after the laboratory.
- **No closing entry:** matters end, evidence lingers unreturned and undestroyed, and the chain simply stops mid-sentence, with UK GDPR implications attached.
- **Treating a discovered break as a secret,** converting a bounded blemish into a credibility event.

Technical limitations

- **A chain proves handling, not origin:** perfect custody from acquisition says nothing about what happened to the data before collection; provenance is the metadata-and-artefact question of other guides.
- **Cloud evidence strains the model:** the "original" is a provider-side dataset nobody physically holds; custody there means documented export mechanisms, verified downloads and platform audit trails, and the cloud guides of this series carry the detail.
- **Hashes bound gaps only where masters persist:** if the original was reissued or wiped, no mathematics can bracket the interval; the chain's value is then only as good as its unbroken portion.
- **Logs are evidence too:** store access logs and platform audit records that would corroborate the chain must themselves be preserved, or the corroboration evaporates on the retention schedule.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 10 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Where has each relevant device and copy been since the dispute arose, and who has had access at each location? (The pre-laboratory chain starts with this answer.)
- Who will be our single custody point of contact, responsible for signing transfers and keeping the file current?

Ask your opponent

- For each exhibit relied on: the exhibit reference, the acquisition record, and the complete transfer history with signatures.
- Where and how has each original and master copy been stored, who has had access, and what access logs exist?
- Please provide the hash schedule and confirm each verification event; where any movement was unverified, please identify it.

Ask your eDiscovery / forensic provider

- Show us your exhibit and transfer forms, storage arrangements and access controls; who signs, and how fast is the file produced on request?
- How do you extend the chain to our side: sealed deliverables, hash confirmations, and guidance for counsel's handling?
- What is your end-of-matter routine: return, certified destruction, and the closing entries?

SUGGESTED WORDING · CLIENT INSTRUCTION ESTABLISHING CUSTODY FROM DAY ONE

> "With immediate effect, all devices and media relevant to this matter are to be handled as evidence: (1) [name] is appointed custody coordinator; (2) each item is to be labelled with a unique reference, photographed, and logged (description, serial numbers, location, condition) on the attached form; (3) items are to be stored in [locked location], access restricted to [named persons] and recorded; (4) no item is to be used, examined, moved or transferred without a signed entry on its form, and no data copied without informing [provider], who will verify by hash; and (5) nothing is to be returned, reissued, repaired or disposed of without our written confirmation. These steps preserve not only the evidence but our ability to prove its integrity; they take minutes per event and cannot be recreated afterwards."

SUGGESTED WORDING · REQUEST FOR AN OPPONENT'S CUSTODY RECORDS

> "So that the continuity of the exhibits on which you rely can be assessed, please provide within [14] days, for each of [exhibits]: (1) the exhibit reference and acquisition record, including the date, method, operator and any hash values computed; (2) the complete record of transfers and handling, with signatures; (3) particulars of storage locations and access, with any access logs; (4) the dates and results of each hash verification; and (5) confirmation of whether each original source remains preserved and available for inspection. Where any of the above does not exist, please say so expressly, identifying the period or movement to which the absence relates."

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 11 · QUICK CONTROL

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

The chain-of-custody checklist

- ☐ Custody started at acquisition (or today, for existing material), never at the laboratory door
- ☐ Exhibit references assigned; items photographed, described and sealed with recorded seal numbers
- ☐ One form per exhibit; one row per event; no silent intervals between rows
- ☐ Every transfer signed by releaser and receiver; courier legs tracked and receipted both ends
- ☐ Storage locked, access restricted to named persons and logged; platform access listed with roles
- ☐ Hash verification bracketing every data movement; masters never examined, only verified working copies
- ☐ Lawyer-side handling (counsel, review copies, productions) logged to the same standard
- ☐ Discovered gaps documented at discovery, bounded by hashes where possible, disclosed candidly
- ☐ Corroborating logs (store access, platform audit) preserved alongside the chain itself
- ☐ Closing entries completed: return or certified destruction, dated and signed

Red flags

- "It was kept safe in the office" as a custody account.
- A transfer history with one signature per movement, or none.
- Evidence on an open share; storage whose access answer is "the team".
- A custody file in one handwriting and one sitting.
- Original devices reissued, reset or missing after copying.
- Hash values absent, or first computed long after acquisition.
- A chain that simply stops, months before today.

When to involve a digital forensic expert

At the start, to design the regime: forms, sealing, storage and verification points sized to the matter, plus the client instruction that starts the clock. During the matter, for every acquisition and significant movement, so the chain's hardest links are laboratory links. On discovery of a break, immediately: bounding a gap with re-verification is examiner's work, and the speed of the response is half its credibility. And against an opponent, to review their custody disclosure and report what it cannot prove: the §8 schedule of gaps is most persuasive under a CPR Part 35 / CrimPR Part 19 signature, delivered without a single adjective.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 12 · COMMON QUESTIONS

Frequently asked questions

Does a broken chain make the evidence inadmissible?

In civil proceedings, rarely by itself: relevant evidence is generally admitted and the defect goes to weight, which is where the real damage happens, because weight is exactly what contested exhibits need. In criminal proceedings continuity is policed more strictly as part of proving the exhibit, and serious defects invite exclusion arguments and abuse submissions. The practical rule for both: never litigate to find out; the paperwork costs minutes.

We already have material that was handled casually before anyone thought about custody. Is it ruined?

No: it is bounded. Start the chain today: reference, seal, log and hash everything now; reconstruct the earlier handling honestly in a witness statement (who, where, when, to the best of recollection, with any corroborating records like emails and courier receipts); and let the hashes computed today certify everything forward. The early period will carry whatever weight its reconstruction earns; the point of acting today is to stop the weak period growing another day longer.

Who should hold evidence during litigation: the client, the solicitors or the laboratory?

Contested originals and masters belong in a laboratory evidence store: purpose-built storage, restricted access, and custody handling as routine rather than exception. Working copies for review live on the provider's platform under logged access. What matters more than the address is the regime: wherever evidence sits, someone must own the file, sign the movements and run the verifications, and the honest question for each candidate holder is whether they will actually do that for eighteen months.

How does chain of custody work for cloud data, where there is no device to seal?

The chain attaches to the export event and everything after: the documented mechanism and date of collection, the hash of the exported set at creation, verified movements thereafter, and the platform's own audit records preserved as corroboration of the source side. What cannot be sealed is evidenced instead: the tenancy's state is the provider's record, and the export's integrity is yours. The cloud collection guides in this series treat the mechanics.

Do we really need tamper-evident seals and forms for a modest commercial dispute?

Scale the regime, keep the principles: perhaps no evidence room, but always references, a log, restricted storage, signed movements and hashes. The cost of the full discipline on a small matter is an hour and a stationery order; the cost of its absence, if the matter turns contentious about an exhibit, is Example 1. Custody is the cheapest insurance in this series, and the premium does not rise with modesty.

What should the chain say when evidence is finally returned or destroyed?

A closing entry as formal as the opening one: what was returned to whom, signed for, on what date; or what was destroyed, by what method, certified by whom, under whose authorisation, referencing the retention decision behind it. The entry completes the account (a chain that trails off invites the question of where the copies went), discharges UK GDPR minimisation duties visibly, and is the row most often missing from otherwise excellent files.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 13 · REFERENCE

Glossary

Access log
The record of who entered the evidence store or platform and when; the chain's corroboration.

Bounded gap
A custody interval bracketed by matching hash verifications, proving the data crossed it unchanged.

Closing entry
The final row: signed return or certified destruction, completing the chain.

Continuity
The unbroken accounting for evidence between acquisition and use; proven, never presumed.

Custody coordinator
The named person who owns the file, signs movements and keeps the record current.

Exhibit reference
The unique identifier assigned at acquisition and used in every subsequent record.

Logical custody
Continuity of data across lawful copies, proven by hash verification at every movement.

Master copy
The preserved acquisition, stored sealed and never examined directly.

Physical custody
Continuity of objects: devices and media, sealed, stored and transferred under signature.

Seal number
The recorded identifier of a tamper-evident seal; changed seals are logged with reasons.

Transfer record
The signed two-party entry documenting each movement of an exhibit.

Working copy
The hash-verified duplicate on which examination is performed.

Sources and authoritative references

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

- cflab.uk, digital forensics services (continuity of evidence maintained from seizure to court; full chain-of-custody documentation; CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services
- cflab.uk, the digital-evidence guide for defence lawyers (chain-of-custody best practice) and the lawyer guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection and Phase 06 · Production (verified, manifested data movements between clients, platforms and parties): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/production
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance (audit trails and continuity): college.police.uk, digital devices guidance
- Forensic Science Regulator, statutory Code of Practice: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 (preservation and custody guidance) and ISO/IEC 17025: iso.org, 27037 · iso.org, 17025
- CPR Part 35 (experts) and CrimPR Part 19: justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19
- ICO, UK GDPR guidance including storage limitation: ico.org.uk

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

DISCLAIMER

This publication provides general information about chain of custody for digital evidence in the United Kingdom as at August 2026. The sample records are illustrative templates to be adapted to the matter and the worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Rules, standards and guidance change; always check the current text. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Continuity is a founding discipline of the laboratory: exhibit referencing, tamper-evident sealing, a controlled evidence store, signed transfers and hash verification at every movement, maintained from seizure to court and produced on request as a single file. We design custody regimes for clients at matter start (forms, storage, the day-one instruction), extend the chain to solicitor and counsel handling with sealed deliverables and verification confirmations, bound and report discovered gaps at speed, and close chains properly with certified return or destruction. Against opponents, we review custody disclosure and produce the schedule of what their file cannot prove, under CPR Part 35 / CrimPR Part 19 where the matter warrants it. Through **e-discovery.uk**, the same continuity runs the disclosure pipeline: verified loads, logged platform access and manifest-and-hash productions. 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