COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Remote Forensic Collection: When Can It Be Defensible?

Secure Agents, Remote Access and the Disciplines That Replace Physical Presence

Distributed workforces, international custodians and time-critical matters have made remote collection routine: forensic agents deployed over the network, acquisitions run through secure channels, evidence streamed to the laboratory without an examiner in the room. Done properly, remote collection is as defensible as attendance: the hashes are the same mathematics, the logs the same record, the method the same method. Done casually, it inherits every risk of distance: unverified endpoints, interrupted transfers, custodian interference, and a chain of custody that starts on a machine nobody controlled. This guide explains the models, the verification and integrity disciplines, the bandwidth and interruption realities, the custodian-cooperation problem, and when the flight is still worth booking.

⏱ Estimated reading time: 27 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its examiners run remote acquisitions across the UK and internationally (agent-based endpoint collection, supervised custodian sessions, cloud and server acquisition over secure channels) alongside laboratory and on-site work, with the same hashing, logging and custody standards regardless of where the examiner sits. Its eDiscovery arm, **e-discovery.uk**, coordinates remote collection at disclosure scale across distributed custodian populations.

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

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: DEFENSIBILITY FOLLOWS METHOD, NOT GEOGRAPHY

Remote forensic collection is defensible when it reproduces, over the wire, everything that makes attended collection defensible: a controlled acquisition process, verification by hashing at source before transfer, encrypted transport, complete logging, and a custody record that starts at the endpoint rather than at the laboratory door. The mathematics does not care where the examiner sits: an agent that images or collects on the device, hashes locally, and streams verified data through an encrypted channel produces evidence identical in integrity to an acquisition performed at the desk. What distance changes is everything around the mathematics: the examiner cannot see the room, verify the machine's identity, prevent custodian interference, or handle the surprises of guide 33 in person; connections fail mid-acquisition; and cross-border endpoints import data-transfer and local-law questions. The defensible remote collection therefore adds compensating controls (endpoint verification, session recording or supervision, resumable and re-verified transfers, and a written remote protocol) and reserves attendance for the cases distance cannot serve: contested devices, powered-on encrypted machines, hostile custodians and anything a court ordered to be done under supervision.

- **The core equivalence:** hash-at-source before transfer means transmission cannot silently corrupt or alter: the value computed on the endpoint is the value verified at the laboratory, or the transfer is re-run. Integrity is proven the same way it always is.
- **The core deficit:** the examiner's eyes. Everything attendance gives (machine identity, room control, state assessment, the at-the-machine decisions of guide 33) must be replaced by controls or accepted as risk, explicitly, in the plan.
- **Custodian-executed steps are the weak joint:** anything the custodian does (plugging in a drive, launching a collector, staying logged in) is a step the other side can attribute to the person with the incentive; supervision, recording and minimisation of custodian involvement are the answers.
- **Remote is a spectrum, not a switch:** from fully agent-based enterprise collection (strongest) through supervised custodian sessions (workable) to posted self-collection kits (weakest, and only for uncontested sources); pick the point on the spectrum per source, in the protocol.
- **Time zones and speed are the quiet advantages:** remote collection can start tonight, across twelve custodians in four countries, while flights are still being priced: for preservation-critical matters, immediacy is itself an evidential virtue.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the examiner is not in the room

Attended collection buys certainty by presence: the examiner sees the actual laptop, checks its serial number against the schedule, watches nobody touch it, makes the guide 33 decisions at the machine, and carries the sealed evidence out. Remote collection buys reach by absence: the examiner works through software and someone else's hands. Between the two sits every question that matters: Is the machine on the other end the machine on the schedule? Who else is in that room? What happened to the laptop in the hour before the session? If the custodian is the person under investigation, what exactly are we trusting them to do and not do?

None of these questions is unanswerable; each is answered by a control. Endpoint identity is verified technically (hardware identifiers, serials read by the agent, cross-checked against asset records) rather than visually. The room is replaced by session supervision and recording. The custodian's hands are minimised to launching a collector, or removed entirely by IT-deployed agents. The pre-session hour is bounded the way custody gaps always are: by artefacts and hashes. The point of this guide is that remote collection is not attended collection minus rigour; it is a different rigour, designed for distance, and the file must show that design.

§ 0 3 · THE MODELS

The remote-collection models

MODEL	HOW IT WORKS	STRENGTH AND PROPER DOMAIN
Enterprise agent	Forensic agent deployed by IT (or pre-installed via endpoint management) collects on the device: targeted files, artefacts, or full images; hashes at source; streams encrypted to the laboratory or collector server	Strongest: no custodian involvement, silent where lawfully appropriate, scalable across estates; the default for corporate endpoints under organisational control
Supervised remote session	Examiner connects by remote-access session; custodian or local IT provides physical access; examiner drives the acquisition live, session recorded, screen and actions logged	Workable where no agent infrastructure exists; the recording substitutes for the room; suits cooperative custodians and one-off devices
Custodian-assisted kit	Pre-configured collector (shipped drive or download) launched by the custodian per written script, sometimes on a supervised video call; results hashed by the tool and returned or uploaded	Weakest link is the custodian's hands; acceptable for uncontested, cooperative sources with supervision; never for the accused
Server / cloud remote	Acquisition of servers, VMs and cloud tenancies through administrative channels and APIs; no user endpoint involved	Standard practice: these sources are always collected "remotely" in truth; the disciplines are the cloud and server guides of this series

§ 0 4 · THE DISCIPLINES

What makes remote defensible: the five disciplines

- **1 · Endpoint verification:** the agent or session records what machine this actually is: hardware serials, disk identifiers, hostnames, logged-in user, OS and encryption state, cross-checked against the asset schedule and the protocol. The identity question is answered by the machine itself, in the log.
- **2 · Hash at source, verify on receipt:** values computed on the endpoint before transmission, recomputed at the laboratory after: matching values prove the wire added and lost nothing; mismatches trigger re-transfer, automatically and loggedly. Transfer is thereby removed from the list of things anyone need trust.
- **3 · Encrypted, authenticated transport:** the channel (agent tunnel, VPN, secure transfer platform) encrypts in transit and authenticates both ends, so interception and substitution are cryptographic non-starters; the channel's configuration is part of the method record.
- **4 · Complete session logging:** everything the remote process did, timestamped: deployment, commands, scope applied, files enumerated and collected, errors, interruptions, resumptions, teardown. Where a human session ran, the recording is retained as an exhibit. This log is the remote substitute for the attending examiner's contemporaneous notes, and is held to the same standard.
- **5 · A remote protocol and custody from the endpoint:** guide 36's document, with the remote specifics: model per source, custodian involvement minimised and scripted, supervision arrangements, interruption handling, and the custody record opening at the endpoint (what was collected from which verified machine, when) rather than at the laboratory's receiving dock.

§ 0 5 · PHYSICS

Bandwidth, interruption and the physics of distance

- **Volume against the wire:** a full disk image is hundreds of gigabytes; over a domestic connection that is days, not hours. Remote strategy therefore leans targeted (guide 37's scope discipline earns its keep here) or stages: collect the priority set over the wire now, image locally to an encrypted drive for courier where fullness is required.
- **Interruption is normal, so resumption is designed:** connections drop, laptops sleep, custodians go to lunch. Defensible tooling checkpoints and resumes with integrity intact (block-level verification across the seam), and the log shows each interruption and resumption; a transfer that silently restarted is a transfer that must be re-verified end to end.
- **The endpoint must survive the session:** long acquisitions need power, disabled sleep, and a custodian instructed not to "help": the pre-session script covers all three, because the commonest remote failure is not attack but a closed lid at 40 per cent.
- **Local staging with hygiene:** where collection stages to a local encrypted container before upload (bandwidth strategy), the container is hashed at creation, and its custody (whose machine, how long, who could touch it) is part of the record: staging is a custody location, not a technicality.
- **Couriered media as the fallback bandwidth:** for big estates, an encrypted drive in a tracked pouch is often the fastest network available; the hybrid (wire for urgency, courier for bulk) is standard and should be planned, not improvised.

§ 0 6 · THE HUMAN ENDPOINT

The custodian problem: cooperation, interference and supervision

- **Grade the custodian before choosing the model:** a cooperative employee under company instruction, a neutral third party, and the individual under investigation are three different risk postures; the model (agent, supervised session, kit) is chosen per custodian, and the accused gets agents or attendance, never kits.
- **Minimise the hands:** every custodian-executed step is a challengeable step; good remote design reduces custodian involvement to physical acts (plug in, power on, click run) performed on a recorded call, with the examiner driving everything evidential.
- **Supervision that means something:** a live video session showing the machine, the screen and the acts; the recording retained; identity confirmed at session start; the machine's state photographed by camera before touching, echoing guide 33's disciplines by lens instead of presence.
- **The pre-session window:** a custodian warned of tomorrow's collection has tonight; remote timing therefore compresses notice where interference is a live risk (agent deployment before announcement, where lawful and proportionate under the organisation's policies), or accepts and bounds the window with artefact analysis afterwards: deletion in the pre-session hours is exactly what the collected artefacts will show.
- **Consent and instruction paperwork:** the custodian's written instruction (what will happen, what they must and must not do) and, for personal devices, the consent machinery of the BYOD guide; remote collection performed on ambiguous authority is a dispute with extra steps.

§ 0 7 · BORDERS AND DUTIES

Security, privacy and cross-border considerations

- **Security of the pipeline is part of the evidence:** ISO 27001-aligned handling, encrypted storage at the receiving end, access-controlled staging, and prompt deletion of transient copies: the collection that secures its own product is the collection whose product is believed.
- **UK GDPR travels with the data:** minimisation shapes remote scope exactly as in guide 37; transparency duties inform custodian communications; and the security principle is answered by the §4 disciplines themselves, documented.
- **Cross-border endpoints raise two distinct questions:** data transfer (moving personal data from the endpoint's jurisdiction to the UK laboratory engages transfer rules: UK adequacy, standard clauses, or derogations for legal claims, assessed per route) and local law (some jurisdictions restrict collection, export or even remote examination of data on their soil: blocking statutes, employment codetermination, state-secrecy regimes). Neither is usually fatal; both are lawyer's questions to answer before the agent deploys, and the multi-jurisdiction guide later in this series expands them.
- **The receiving record:** where evidence crosses borders, the file shows the route, the basis and the safeguards: one paragraph now against one satellite dispute later.

§ 0 8 · THE RESIDUAL CASE FOR THE FLIGHT

When attendance still wins

- **The contested device:** where the machine itself is the battleground (planting, deletion, attribution), physical control, write-blocked imaging and the examiner's own eyes remain the gold standard, and the cost of a train ticket is not the place to economise.
- **The powered-on problem:** guide 33's live decisions (memory capture, encryption assessment, isolation) want hands and judgment at the machine; remote sessions can perform some of it, but the fleeting-opportunity cases justify presence.
- **The hostile or evasive custodian:** remote collection hands the uncooperative exactly the distance they want; attendance (or agent deployment without their participation) removes it.
- **Court-supervised executions:** search orders and imaging orders assume presence: the supervising solicitor, the respondent's rights, the sealed exhibits; remote has no role at the sharp end of these.
- **Failing media and exotic hardware:** the dying drive, the RAID, the soldered-storage device: laboratory problems, requiring the object itself.
- **The honest default:** remote first where the five disciplines can run and the source is uncontested; attendance where the device, the custodian or the order says otherwise; and the protocol records which and why, so the choice itself is method.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · TWELVE CUSTODIANS, FOUR COUNTRIES, ONE WEEK

A supply-chain dispute needed collection from twelve custodians across the UK, Ireland, Germany and Singapore before a limitation-driven deadline. Attendance would have taken a month of travel; instead, enterprise agents were deployed through the client's endpoint management overnight, scoped per the protocol (mailboxes were collected server-side in parallel), each endpoint's identity logged by serial and hostname, everything hashed at source and streamed encrypted to the laboratory, with German endpoints routed via a transfer-assessed path agreed with local counsel. Eleven completed inside the week; the twelfth, a failing laptop in Singapore, was couriered for laboratory imaging: the hybrid working as designed. The opponent's methodology questions were answered with the remote protocol and session logs, and went no further.

EXAMPLE 2 · THE SELF-COLLECTION KIT AND THE ACCUSED CUSTODIAN

Before instructing us, a claimant had posted a collection drive to the very ex-employee suspected of taking its designs, with instructions to run the collector on his personal laptop and return it. He did, eleven days later. The collection was technically tidy (hashed, logged) and evidentially hollow: the tool could only attest what the laptop contained on day eleven, the artefacts showed a bulk deletion on day nine, and every inference the claimant wanted was met with "you gave him the tool and the fortnight". The eventual order for delivery-up and laboratory imaging recovered some of the position; the lesson was §6's first rule: the accused never gets the kit, and remote collection from adverse custodians is done by agent, by order, or by attendance, not by post.

EXAMPLE 3 · THE INTERRUPTED IMAGE THAT SURVIVED BECAUSE THE LOG DID

A supervised remote session imaged a director's laptop over a hotel connection that dropped four times. The tooling checkpointed and resumed each time; the session recording and log captured every interruption, resumption and block-verification pass; and source-side hashes matched laboratory recomputation on receipt. Eighteen months later the acquisition was challenged as "cobbled together over a failing link". The response exhibited the log: four interruptions, four verified resumptions, end-to-end values matching at source and destination, session recording available. The challenge collapsed into a complaint about aesthetics, and the judgment's only comment was that the record "answered the point completely". Interruption is not the risk; the unlogged interruption is.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Kits to the accused:** Example 2, committed weekly across the profession.
- **No endpoint verification:** collecting from "his laptop" with nothing in the log proving which machine answered.
- **Transfer trusted instead of verified:** no source-side hashes, so the wire's integrity rests on hope.
- **Unrecorded custodian sessions:** the one part of the exercise a challenge will target, left without its exhibit.
- **Sleep, power and lunch:** multi-hour acquisitions launched without the pre-session script, failing at 40 per cent.
- **Silent restarts:** interrupted transfers begun again without end-to-end re-verification.
- **Cross-border collection before the transfer question:** the agent deployed to Frankfurt while the legal basis is still an email thread.
- **Remote used because it was easy, on the contested device** that needed the laboratory: geography chosen by convenience rather than by risk.

Technical limitations

- **What agents cannot do:** capture the room, prevent physical substitution before deployment, or perform the full guide 33 live-machine judgment; remote memory capture exists but is more constrained than at-machine work.
- **Endpoint state is inherited, not controlled:** the machine's encryption, corporate policies, connectivity and health set what is collectable; the plan discovers these in the pre-flight, not mid-acquisition.
- **Deep recovery stays physical:** imaging failing media, chip-level work and exotic storage need the object; remote collection's ceiling is what the running system will give a well-behaved tool.
- **Networks impose their own metadata:** collection timing reflects transfer schedules, not user activity; analysts and reports must not confuse the two clocks.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What endpoint-management infrastructure exists for agent deployment, and which relevant devices sit outside it?
- Which custodians are cooperative, neutral or adverse? (The model-per-custodian answer.)
- Where are the endpoints physically, and do any sit in jurisdictions needing transfer or local-law analysis first?

Ask your opponent

- For each remotely collected source: the model used, the endpoint-verification record, and the session logs.
- Were hashes computed at source before transfer, and do laboratory values match? Please provide the schedule.
- What steps were custodians asked to perform themselves, under what supervision, and where is that recorded?

Ask your eDiscovery / forensic provider

- Which remote models do you operate, and how do you verify endpoint identity in each?
- Show us a specimen session log and interruption-resumption record.
- How do you handle bandwidth-heavy sources: staging, couriered media, and the custody of both?
- What is your cross-border routine: transfer assessment, routing, and the receiving record?

SUGGESTED WORDING · REMOTE ANNEX FOR THE COLLECTION PROTOCOL

> "R1. Remote collection shall proceed per the model assigned to each source in Schedule B (enterprise agent / supervised session / assisted kit), assessed against custodian posture; no assisted kit shall be used for any custodian identified as adverse. R2. For each endpoint, the collection record shall include hardware and system identifiers verifying the device's identity against the asset schedule. R3. Hash values shall be computed at source prior to transfer and re-computed on receipt; any mismatch or interrupted transfer shall be re-verified end to end, and all interruptions and resumptions logged. R4. Custodian-performed steps shall be limited to those scripted in Annex R-A, performed on a recorded supervised session, the recording retained as an exhibit. R5. For endpoints outside the United Kingdom, collection shall not commence until the data-transfer basis and any local-law constraints have been confirmed by [named lawyer] and recorded."

SUGGESTED WORDING · CUSTODIAN PRE-SESSION INSTRUCTION

> "Your device will be collected remotely on [date/time]. Before the session: connect the device to mains power and a reliable network, and do not delete, move, install or 'tidy' anything on it: the collection must capture the device as it is, and changes made beforehand will themselves be visible. During the session: you will be asked only to [join the video call, confirm your identity, and run the collector when instructed]; please do not use the device otherwise, close the lid, or allow others to use it until we confirm completion. The session will be recorded as part of the evidence record."

§ 12 · QUICK CONTROL

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

The remote-collection checklist

- ☐ Model chosen per source and custodian posture; adverse custodians never on kits
- ☐ Remote annex in the protocol; custodian scripts written; supervision and recording arranged
- ☐ Endpoint identity verified and logged: serials, identifiers, user, encryption state
- ☐ Hash at source, verify on receipt; interruptions checkpointed, resumed and re-verified
- ☐ Transport encrypted and authenticated; channel configuration recorded
- ☐ Session logs and recordings retained as exhibits; custody record opened at the endpoint
- ☐ Bandwidth plan made: targeted scope, staging hygiene, couriered media for bulk
- ☐ Cross-border endpoints cleared (transfer basis, local law) before deployment, and recorded
- ☐ Pre-session instructions issued; power, sleep and do-not-touch covered
- ☐ Attendance reserved and used for contested devices, live-machine problems and ordered executions

Red flags

- A collection drive in the post to the person under investigation.
- Logs that cannot say which physical machine was collected.
- No source-side hashes; transfer integrity by assertion.
- A custodian session nobody recorded.
- A restarted transfer with no end-to-end re-verification.
- Foreign endpoints collected while the transfer analysis was "in progress".
- "We did it remotely because it was quicker" about the case's central device.

When to involve a digital forensic expert

At planning, to assign models per source, write the remote annex and custodian scripts, and make the bandwidth and staging decisions before they are made by a hotel network. At execution, because the five disciplines are tooling-and-procedure work: agent deployment, endpoint verification, hash-verified transfer and the session record are what the laboratory's remote practice exists to do. In challenge, both directions: the session logs and hash schedules that answer an attack on your remote collection, or the CPR Part 35 review that dismantles an opponent's ("on the disclosed records, the identity of the collected endpoint cannot be established, and no source-side verification exists"). And whenever the question is remote-or-attend for a specific device: that judgment call, made early with an examiner, is the cheapest decision in this guide.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is remotely collected evidence weaker in court than evidence collected in person?

Not inherently: courts assess method, and a remote collection with endpoint verification, source-side hashing, complete logs and a recorded session proves integrity exactly as an attended one does. Weakness enters through the gaps distance can create (unverified endpoints, custodian-executed steps, silent restarts), which is why the §4 disciplines exist. The honest comparison is not remote versus attended but disciplined versus casual, in either geography.

Can a custodian defeat a remote collection?

Before it, yes, in the way they can defeat any collection: by deleting in the notice window: which is why timing is compressed for risky custodians and why the collected artefacts themselves usually record the attempt (mass deletions leave traces that survive into the acquisition). During a properly designed session, their role is too small to exploit: identity confirmed, actions scripted and recorded, the examiner driving. The genuinely dangerous configuration is the unsupervised kit with a generous deadline: Example 2, avoid.

How long does remote collection take?

Deployment can be same-day where agent infrastructure exists; per-endpoint acquisition then runs from under an hour (targeted sets) to a day or more (large volumes on modest links), with mailbox and cloud sources collected server-side in parallel at platform speed. The honest variable is the wire: which is why scoping (guide 37) and the courier hybrid are part of remote planning rather than afterthoughts, and why twelve custodians in a week (Example 1) is realistic while twelve full images over home broadband is not.

Do we need the custodian's consent to deploy an agent to a company laptop?

Deployment to organisation-owned, policy-governed devices generally proceeds on the employer's authority, with UK GDPR transparency handled through existing policies and, where appropriate, matter-specific notice: but the position depends on the policies actually in force, the jurisdiction, and employment-law overlays, so the lawyer clears it per estate rather than by assumption. Personal devices are different territory entirely: consent or compulsion, per the BYOD guide, and never a silent agent.

What happens if the connection dies halfway through?

With proper tooling: nothing evidentially interesting. The transfer checkpoints, resumes and re-verifies across the seam; the log records the event; and the end-to-end hash comparison proves the assembled acquisition identical to source. Example 3 is the pattern: four drops, one clean exhibit. What must never happen is the quiet manual restart without re-verification: that is the version of the story cross-examination enjoys.

Can search orders or imaging orders be executed remotely?

The supervised execution itself, no: the machinery (supervising solicitor, respondent's rights, sealed exhibits, the premises) assumes presence, and courts expect it. Remote techniques serve around the edges: preserving cloud sources simultaneously, collecting from consenting third parties in parallel, and processing the seized material thereafter. If a matter needs compelled access to a distant respondent's devices, the answer is the order plus local execution, not an agent: which is a planning point to raise with both counsel and examiner early.

§ 14 · REFERENCE

Glossary

Assisted kit
A pre-configured collector run by the custodian per script; the weakest model, never for adverse custodians.

Checkpointed transfer
Transmission that resumes after interruption with integrity verified across the seam.

Endpoint verification
Technical confirmation of which machine was collected: serials, identifiers, state, logged.

Enterprise agent
Forensic software deployed via IT infrastructure, collecting without custodian involvement.

Hash at source
Values computed on the endpoint before transfer, making the wire verifiable.

Pre-session script
The custodian's written do-and-do-not instructions for the collection session.

Remote annex
The protocol section governing models, verification, supervision and cross-border clearance.

Session log / recording
The timestamped record (and video) of everything the remote process and session did; an exhibit.

Staging
Local encrypted holding of collected data pending upload or courier; a custody location.

Supervised session
Examiner-driven remote acquisition on a recorded call, custodian's role minimised to physical acts.

Transfer assessment
The lawyer's clearance of cross-border data movement before collection begins.

Sources and authoritative references

The remote-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 (remote and on-site acquisition, agent-based collection, verified transfer and CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection (distributed custodian collection at disclosure scale; "defensibility is built, not retrofitted"): e-discovery.uk/edrm/collection · Phase 02 · Preservation: e-discovery.uk/edrm/preservation
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance · Forensic Science Regulator Code: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 and ISO/IEC 27001 (evidence handling; information security): iso.org, 27037 · iso.org, 27001
- ICO, UK GDPR guidance including international transfers: ico.org.uk · CPR Part 35: justice.gov.uk, Part 35 · CPR Part 25 / PD 25A (search orders): justice.gov.uk, Part 25

DISCLAIMER

This publication provides general information about remote forensic collection in the United Kingdom as at August 2026. The worked examples are fictional and the clause wording illustrative. Cross-border collection engages jurisdiction-specific law on which specific advice is required. 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. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Remote collection is a standing capability of the laboratory: enterprise agents deployed through client infrastructure, supervised recorded sessions for one-off devices, hash-at-source verified transfer, and session records built as exhibits, with the same custody and reporting standards as our attended work. We assign models per custodian, write the remote annex and pre-session scripts, run the bandwidth arithmetic (wire, staging, courier) before it runs the schedule, and coordinate cross-border clearance with instructing lawyers so agents deploy on a recorded basis. Where the matter needs presence (contested devices, live machines, ordered executions) we attend; the point of a laboratory that does both is that the choice is made on risk, not on convenience. Through **e-discovery.uk**, remote collection scales across distributed custodian populations and feeds directly into processing. 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