COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Planning an On-Site Digital Evidence Collection

Access, Equipment, Credentials, Disruption and the Day That Goes to Plan

An on-site collection succeeds or fails before anyone arrives. Access arranged, devices located, credentials and encryption recovery keys assembled, equipment packed for what the site actually holds, business disruption negotiated, roles assigned, custody and transport planned: these are the decisions that make collection day an execution rather than an adventure. This guide is the planning manual for the site visit: what to establish in advance, what to bring, how to sequence the day, how to keep the business running while its machines are imaged, and how to leave with sealed exhibits, complete logs and no surprises left behind.

⏱ 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 attend sites weekly: offices, data centres, warehouses, homes under order, from single-laptop visits to multi-day corporate collections, each planned to the disciplines in this guide and executed to the protocol and custody standards of the wider series. Its eDiscovery arm, **e-discovery.uk**, coordinates the on-site legs of disclosure-scale collections.

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

§ CONTENTS

In this guide

01 Executive summary

02 The problem in plain English: why site days go wrong

03 The pre-visit reconnaissance

04 Access, authority and the people question

05 Credentials, encryption and the keys to the estate

06 Equipment: what the kit list actually contains

07 The day itself: sequence, disruption and logging

08 Departure: sealing, transport and the site left behind

09 Worked examples

10 Common mistakes and technical limitations

11 Questions to ask · Suggested wording

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

13 Frequently asked questions

14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: THE SITE VISIT IS WON IN THE WEEK BEFORE IT

On-site collection is the discipline of bringing the laboratory to the evidence: examiners, write blockers, imaging rigs and evidence media travelling to where the devices are, because the devices cannot travel, cannot be interrupted, or must be handled under someone's supervision. Its failure modes are almost never forensic; they are logistical: the server room nobody could unlock, the BitLocker key nobody had, the RAID that needed an adapter the kit lacked, the finance team whose quarter-end collided with the imaging schedule, the fire-escape desk nobody listed, the taxi at six with unsealed drives. Every one of those is preventable by planning: a reconnaissance that establishes what the site holds and what it needs; access, authority and credentials assembled in advance; a kit list built from the reconnaissance rather than habit; a sequencing plan that respects both volatility (guide 33) and the business's pulse; and departure logistics (sealing, custody, transport) arranged before arrival. The visit itself then becomes what it should be: the calm execution of a written plan, logged as it happens, with the protocol of guide 36 as its score.

- **Reconnaissance is not optional:** a site questionnaire and a call with IT the week before answer the questions that otherwise get answered at the door, expensively: device inventory, encryption posture, network topology, physical access, power and space.
- **Credentials decide the day:** admin accounts, BitLocker/FileVault recovery keys, NAS and hypervisor logins, safe combinations: assembled and verified beforehand, because guide 33's encryption realities apply to every machine on the schedule.
- **Disruption is negotiated, not discovered:** what stops, what slows, what runs overnight; agreed with the business in advance and written into the sequence, so the collection is remembered as professional rather than as the day the company stopped.
- **The day produces three things:** sealed exhibits with custody records, verified images with hash schedules, and a contemporaneous log (including deviations): the deliverables are defined before the van is loaded.
- **Plan the departure like the arrival:** sealing, signatures, courier or escorted transport, and the state the site is left in (devices returned or retained, users re-enabled, a named contact for the morning after).

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: why site days go wrong

Collection day concentrates risk. Everything the wider series treats as a discipline (preservation, method, custody, protocol) has to happen in one place, on one schedule, with the business watching and sometimes with the other side's solicitor in the corridor. And the site always knows something the plan does not: the second server room, the machine under the receptionist's desk, the departed director's laptop in a cupboard, the RAID enclosure from 2011, the encrypted NAS whose password left with the IT contractor. Teams that arrive with generic kit and no reconnaissance meet these surprises at retail prices: return visits, missed devices, improvised decisions of exactly the kind guides 31 and 36 exist to prevent.

The remedy is unglamorous: treat the visit as a small project. A week of preparation (questionnaire, IT call, credential assembly, kit build, sequence plan, disruption agreement, transport booking) converts a day of adventure into a day of execution. The examiners still bring judgment for the genuine surprises; the point of planning is that judgment is spent on the two things the questionnaire could not know, not on the forty it could.

§ 0 3 · THE WEEK BEFORE

The pre-visit reconnaissance

- **The site questionnaire,** completed by client IT and the site contact: device inventory against the protocol's Schedule B (makes, models, counts, locations); servers, NAS and network equipment with roles; operating systems and ages; encryption in use; cloud versus on-premises split; physical layout (rooms, floors, locked areas); power sockets and desk space where the rigs will run; parking, loading and building hours.
- **The IT call,** examiner to administrator, walking the questionnaire and probing its edges: the systems that "aren't really used any more", the backup regime, the machines off-inventory, the credentials landscape. Half the surprises die on this call.
- **Volume arithmetic:** total storage on the schedule, divided by realistic imaging throughput, gives the honest duration and the rig count; a day planned by hope runs into night, and night runs into the next section's disruption budget.
- **Risk pass:** which devices are contested (full image, examiner-only handling), which are live systems (guide 33 planning), which are fragile (old drives, RAID sets: laboratory candidates), and which custodians need managing rather than merely scheduling.
- **Verification against drift:** the questionnaire is re-confirmed within days of the visit (guide 36's verification step), because estates move: leavers, reissues, migrations, and the cupboard's contents all change between planning and execution.

§ 0 4 · DOORS AND PEOPLE

Access, authority and the people question

- **Physical access, arranged and named:** building passes, escorts, server-room keys, safe access, out-of-hours arrangements where the plan uses the quiet hours; the person who can open each door is named per door, with a deputy.
- **Legal authority, carried in writing:** the instruction or consent under which the team attends; for ordered executions, the order and its machinery (and the supervising solicitor's role) govern everything, per guide 36. The team carries what it may show, and knows what it may say, to anyone who asks why they are unplugging the finance server.
- **The people plan:** who at the site knows, who does not, and what the cover story or open explanation is; collections framed as "IT maintenance" versus announced exercises have different sequencing and different UK GDPR transparency answers, decided by the lawyer beforehand, not by the examiner in the kitchen.
- **Roles per guide 36:** examiners execute; IT opens doors and answers questions; the supervising lawyer (on site or on the phone) owns scope, privilege and people decisions; a client contact manages staff and rooms; and the decision number is printed on the day plan.
- **Third parties on site:** landlords, managed-service providers, shared-office neighbours: anyone whose consent, notice or cooperation the visit needs is identified in planning, because the server room that turns out to belong to the MSP is a doorstep discovery nobody enjoys.

§ 0 5 · KEYS

Credentials, encryption and the keys to the estate

- **The credential schedule:** assembled before the visit: domain and local admin accounts; BitLocker recovery keys (from AD, Entra ID or management tooling, per guide 33's escrow hunt) for every Windows device on the list; FileVault recovery for Macs; NAS, hypervisor, firewall and backup-system logins; BIOS/UEFI passwords where set; safe combinations and key locations for physical storage.
- **Verified, not assumed:** credentials are tested (or their escrow existence confirmed) in the reconnaissance window; the recovery key that "should be in AD" is confirmed to actually be in AD, because the difference is the difference between imaging and guide 33's locked-box problem.
- **Handled as secrets:** the schedule travels encrypted, access-limited, and is destroyed or returned per agreement afterwards; credential handling is itself a security event the client will remember.
- **The gaps, planned for:** devices whose credentials cannot be assembled get a written contingency (live acquisition while unlocked; imaging encrypted with the key hunt continuing; laboratory referral), decided per guide 33 before the team stands at the machine.
- **Departed-employee devices:** the leavers' cupboard is a credential desert; the plan flags these devices early, hunts escrow through management tooling, and where nothing exists, schedules them honestly as encrypted acquisitions rather than day-of disappointments.

§ 0 6 · THE VAN

Equipment: what the kit list actually contains

- **Acquisition:** hardware write blockers (multiple interfaces: SATA, NVMe, USB, and the legacy adapters the questionnaire justified); imaging rigs or forensic duplicators, enough to run the volume arithmetic in parallel; boot media and live-acquisition tooling for machines that must be imaged in place; memory-capture tools for the powered-on plan.
- **Destination media:** sanitised, encrypted evidence drives with headroom above the arithmetic (sites always hold more than the questionnaire), plus spares for failure.
- **Interfaces and the drawer of adapters:** the enclosure openers, drive caddies, cables and connectors for what the inventory listed, and the pessimistic extras for what it did not; the 2011 RAID is imaged by the team that packed for 2011.
- **Custody and recording:** tamper-evident bags and seals, exhibit labels, the forms of guide 35, cameras for state photography (guide 33), and the printed day plan, protocol, credential schedule and contact sheet.
- **Site survival:** power strips and extensions, network isolation kit (for live machines that must leave the network), torches, tools, antistatic bags: and the humility items: spare write blocker, spare rig, because single points of failure travel badly.
- **Packed against the plan:** the kit list is generated from the reconnaissance, checked against the sequence, and loaded the day before; "the van has everything" is a claim audited on paper, not discovered on site.

§ 0 7 · EXECUTION

The day itself: sequence, disruption and logging

- **Arrival routine:** sign in, meet the contacts, walk the site against the questionnaire (the walk finds the fire-escape desk), confirm rooms and power, and brief the client team on the day's shape before the first machine is touched.
- **Sequence by the plan:** powered-on and contested devices first (guide 33's decisions, made by the playbook), then the volume work in parallel: user machines in batches, servers in their negotiated windows, loose media swept methodically room by room against a floor plan that gets ticked.
- **Disruption managed as agreed:** users lose machines in scheduled batches with loaners or downtime windows; servers image out-of-hours or from snapshots per the negotiated plan; the business's calendar (payroll runs, quarter-end, shift patterns) was consulted in planning and is respected on the day. The collection that respects the business gets cooperation; cooperation is an evidential asset.
- **Logging as the work happens:** the running log (times, devices, serials, actions, who, surprises) and the exhibit and custody forms are completed at each event, per guides 31 and 35; photographs record device state before handling; deviations go to the deviation log with the referral call noted.
- **Surprises to the protocol:** the unlisted device, the unexpected encryption, the custodian objection: each has a contingency or an escalation trigger from guide 36; the field team's job is stop-preserve-call, not invention.
- **Parallel quiet work:** while rigs run, examiners document the network, photograph the server room, collect the loose media drawer, and verify completed images: idle imaging time is where the day's documentation debt is paid.

§ 0 8 · LEAVING WELL

Departure: sealing, transport and the site left behind

- **The closing hour is scheduled:** verification hashes completed or logged as in-progress, exhibits sealed with recorded numbers, forms signed both sides, the evidence schedule agreed with the site contact, and the kit inventory re-checked (what came in leaves, what stays is listed).
- **Transport as custody:** sealed exhibits travel by the arrangements booked in planning: escorted vehicle or tracked secure courier, transfer rows completed at both ends per guide 35; evidence does not ride unsealed in footwells, and the courier does not get booked at 5pm.
- **The site's morning after:** devices retained versus returned is per the plan and recorded; users and systems re-enabled by IT on the agreed schedule; a named laboratory contact given for the questions that surface tomorrow; and where devices were retained, the business impact (loaners, data access) was solved in planning, not left as resentment.
- **The report clock starts:** the collection report (guide 36's reconciliation of plan against execution, with logs, deviations, evidence and hash schedules) is drafted while the day is fresh; the deliverable set defined in the protocol is issued on its stated timetable.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE QUESTIONNAIRE THAT FOUND THE SECOND SERVER ROOM

A fraud collection was scoped for "the office server and twelve laptops". The site questionnaire's topology questions surfaced a rack in a locked comms cupboard on another floor: the previous finance system, retired but powered, holding the ledger database for the disputed years. Planning absorbed it calmly: credentials traced through the former MSP, an extra rig packed, the sequence extended by a negotiated evening. Discovered on the day instead, it would have meant a return visit weeks later to a system someone might by then have "tidied": and the ledger history was, in the event, the case.

EXAMPLE 2 · THE QUARTER-END COLLISION THAT PLANNING DISSOLVED

An imaging visit was first proposed for the last week of March: the finance team's quarter-end, with the ERP under continuous use and the FD immovably hostile. The disruption negotiation moved the visit forward, split it (user machines in scheduled batches over two days; servers imaged from storage snapshots overnight with IT in attendance), and put loaner laptops on desks before each batch was lifted. The business lost no reporting day; the FD's witness statement later described the exercise as "conducted without disruption"; and that sentence, in a dispute partly about the company's conduct, was worth more than the convenience it cost.

EXAMPLE 3 · THE KIT LIST VERSUS THE 2011 RAID

Two collections, same month, same model of elderly NAS with a proprietary four-disk RAID. Team A had run the reconnaissance: the questionnaire flagged the unit, the IT call confirmed its vintage, and the van carried the right caddies, a compatible enclosure and the decision (pre-made with the lawyer) to image the disks individually for laboratory reconstruction. Four hours, sealed exhibits, done. Team B, on another matter with no reconnaissance, met the same hardware cold: no caddies, no plan, an improvised attempt to copy shares over the network that captured half the data with rewritten timestamps, and a return visit after the respondent had, in the interval, disposed of the unit "as obsolete". The hardware was identical; the week before was not.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **No reconnaissance:** the day planned from the instruction letter instead of from the site.
- **Credentials assumed:** the recovery keys "in AD" that were not, discovered at the machine.
- **Generic kit:** the van packed by habit meeting the estate packed by history.
- **Volume optimism:** one rig, eleven terabytes, one booked day, and a schedule that dies at lunch.
- **Disruption unnegotiated:** the business ambushed, cooperation lost, and the collection remembered as an occupation.
- **The unswept room:** desks and drawers not walked against a floor plan; the loose media and the cupboard laptop left behind.
- **Documentation deferred:** logs and forms "to be written up later", which is guide 35's reconstructed-record mistake in field clothing.
- **Departure improvised:** the 5pm courier hunt, the unsealed boot, the custody chain's first gap created in the car park.

Technical limitations

- **Imaging throughput is physics:** interfaces and drive health set the pace; parallelism is the only honest accelerator, and some old drives will be slower than their size suggests.
- **Some hardware defeats the field:** failing media, exotic RAID, soldered storage: laboratory problems, and the plan says so in advance, scheduling seizure rather than on-site imaging for them.
- **Live systems constrain:** the server that cannot stop is acquired by the negotiated route (snapshot, live logical, out-of-hours) with guide 33's live-acquisition record, not by wishing it were otherwise.
- **The site is a moment:** the visit captures the estate as found; what left the building before the plan was made (leaver devices, tidied cupboards) is a preservation question from earlier guides, which the visit can document but not reverse.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Who will complete the site questionnaire, and who is the IT voice for the reconnaissance call this week?
- What are the business's immovable dates and rhythms in the visit window, and who can negotiate the disruption plan?
- Who holds, or can retrieve, every credential and recovery key on the schedule, and can we verify them beforehand?

Ask your opponent (for agreed or supervised visits)

- Please confirm site access, the rooms and systems available, and the named contacts for [date], per the agreed protocol.
- Please confirm the credentials and recovery keys that will be made available at the visit, and the arrangements for devices whose credentials are not held.
- Please confirm which devices, if any, are contended to be out of scope, so the question is resolved before attendance rather than at the machine.

Ask your eDiscovery / forensic provider

- What does your reconnaissance ask, and what did the answers change in the plan?
- Walk us through the day plan: sequence, rigs, throughput arithmetic, disruption windows and the closing hour.
- What are the transport and same-day custody arrangements, and when does the collection report land?

SUGGESTED WORDING · CLIENT SITE-PREPARATION INSTRUCTION

> "Ahead of the collection on [date]: (1) please complete the attached site questionnaire by [date], and make [IT contact] available for a planning call with the examiners; (2) assemble and verify the credentials on the attached schedule, including BitLocker/FileVault recovery keys for every listed device, and notify us immediately of any that cannot be obtained; (3) confirm access arrangements: building passes, server-room and safe access, and out-of-hours availability of [named keyholder]; (4) agree with us by [date] the disruption plan: which users and systems are affected, when, and what interim arrangements (loaner devices, downtime windows) the business needs; and (5) make no changes to the devices and systems on the schedule in the meantime: no reissues, rebuilds, tidying or disposals, per the preservation notice already in effect."

SUGGESTED WORDING · DAY-PLAN HEADER (THE ONE-PAGE VERSION THE TEAM CARRIES)

> "Matter [ref] · Site [address] · Protocol v[The] [date]. Decision-maker: [named lawyer, phone]. Site contact: [name, phone]. IT: [name, phone]. Sequence: 09:00 arrival, walk-through and briefing; 09:30 powered-on and priority devices per Annex 1; 10:30 user batches A-C per rota; servers 18:00 window per IT agreement; sweep of rooms per floor plan throughout. Contingencies and escalation: per protocol §§7-8: stop, preserve, photograph, call. Closing hour from 16:30: verification, sealing, signatures, evidence schedule, courier [booking ref] at 17:30."

§ 12 · QUICK CONTROL

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

The on-site planning checklist

- ☐ Site questionnaire completed and reconnaissance call held; inventory reconciled to the protocol's schedules
- ☐ Volume arithmetic done; rigs, duration and (if needed) multi-day plan set accordingly
- ☐ Credential schedule assembled and verified; gaps given written contingencies per guide 33
- ☐ Access named per door; legal authority documents carried; third parties identified and squared
- ☐ Disruption plan negotiated with the business and written into the sequence
- ☐ Kit list generated from the reconnaissance, packed against the plan, with spares for single points of failure
- ☐ Day plan printed: sequence, roles, decision number, contingencies, closing hour
- ☐ Custody materials ready (seals, forms, labels, camera); transport booked in advance
- ☐ Logging live all day: running log, exhibit and custody forms, photographs, deviation log
- ☐ Departure executed: sealed, signed, scheduled, couriered; site state and morning-after contact agreed; report clock started

Red flags

- A visit scheduled with no questionnaire and no IT call.
- "The keys will be around somewhere."
- One rig for a double-digit terabyte schedule.
- A business that learns about the visit when the team arrives.
- No floor plan, no sweep, no loose-media pass.
- Forms blank at 4pm on a day that started at 9.
- Unsealed exhibits leaving in personal vehicles.

When to involve a digital forensic expert

From the moment a site visit becomes likely: the reconnaissance, credential hunt, kit build and sequence plan are examiner's work, and a week of their planning is the cheapest insurance in this guide. On the day, examiners execute and hold the method line while the supervising lawyer holds scope and people. For ordered executions, the examiner's independence and the supervising solicitor's machinery are load-bearing, per guide 36. And after a visit that went wrong (another party's, or a client's own pre-instruction attempt), an examiner's review of what the day's records can and cannot establish (which devices, which handling, which gaps) is the CPR Part 35 foundation for either repairing the position or exploiting it.

§ 1 3 · COMMON QUESTIONS

Frequently asked questions

How long does an on-site collection take?

The arithmetic answer: total scheduled storage divided by parallel imaging throughput, plus the fixed costs (walk-through, powered-on work, sweeping, sealing): typically a day for a handful of machines, two to three for a small office, and a planned campaign for anything larger, with servers often taken in overnight windows. The planning answer: however long the reconnaissance says, plus margin: because the schedule that assumed the questionnaire was complete meets §2's cupboard eventually.

Can the business keep working while we collect?

Largely, if planning made it so: user machines lifted in batches against loaners or downtime windows, servers imaged from snapshots or out-of-hours, and the sequence built around the business calendar. The honest exceptions: the specific machine being imaged is unavailable while it images (unless live-acquired), and contested devices leave immediately and stay gone. Example 2 is the model: disruption is a negotiation the week before, not a discovery on the day.

Should devices be imaged on site or taken to the laboratory?

Per device, by plan: on-site imaging suits healthy, standard hardware the business needs back and uncontested contexts; seizure to the laboratory suits contested devices (custody strength), failing or exotic media (§10), encrypted machines pending key recovery, and anything the volume arithmetic cannot fit into the site window. The protocol's method matrix records which, and the site plan books transport and loaners accordingly; "we'll decide at the desk" is the answer this guide exists to delete.

What if we find devices on site that are not on the schedule?

The standard contingency: record them (photograph, location, description), preserve them in place or seize per the protocol's unexpected-source clause, and refer the scope question to the decision number the same hour: guide 36's stop-preserve-call, which converts the surprise into a documented decision. What the team never does is silently image them (scope without authority) or silently ignore them (the omission cross-examination finds): the corridor of guide 36's first example runs through every site.

Do we need to tell staff what is happening?

A lawyer's decision made in planning, balancing UK GDPR transparency, employment-relations reality, tipping-off risk in fraud contexts, and the practicalities of lifting machines from desks. Options run from full announcement through need-to-know framing to covert out-of-hours collection where the risk analysis and legal basis support it; each has different sequencing and different paperwork, and the examiner executes whichever was chosen: the kitchen is not where this gets decided.

What does the client get after the visit?

The deliverable set the protocol promised: the evidence schedule (every exhibit, reference, seal and location), the hash schedule, the collection report reconciling plan against execution with the running and deviation logs, photographs, and the custody records: plus the practical outputs: retained-device list, return timetable, and the named contact for the morning-after questions. If the matter proceeds, the same set is what makes the collection exchangeable and defensible; it is written once, for both audiences.

§ 14 · REFERENCE

Glossary

Closing hour
The scheduled end-of-day block: verification, sealing, signatures, schedule, transport.

Credential schedule
The verified list of accounts, recovery keys and combinations assembled before the visit.

Day plan
The one-page sequence, roles, contacts and contingencies the team carries.

Disruption plan
The negotiated agreement on what stops, slows or shifts, and the interim arrangements.

Floor-plan sweep
The methodical room-by-room pass for devices and loose media, ticked against a plan.

Loaner
The replacement device that lets a user work while theirs is imaged or retained.

Reconnaissance
The questionnaire, IT call and verification that make the plan match the site.

Rig
An imaging workstation or duplicator; rig count times throughput is the day's capacity.

Running log
The contemporaneous record of the day: times, devices, actions, surprises.

Volume arithmetic
Scheduled storage divided by throughput: the honest duration calculation.

Walk-through
The arrival tour reconciling the site against the questionnaire before work begins.

Sources and authoritative references

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

- cflab.uk, digital forensics services (on-site acquisition, seizure and laboratory imaging, custody and CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (the on-site legs of disclosure-scale exercises; "defensibility is built, not retrofitted"): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance · Forensic Science Regulator Code: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 (identification, collection, acquisition and preservation) and ISO/IEC 17025: iso.org, 27037 · iso.org, 17025
- CPR Part 35 and CPR Part 25 / PD 25A (search orders and interim remedies): justice.gov.uk, Part 35 · justice.gov.uk, Part 25 · ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about planning on-site digital evidence collection in the United Kingdom as at August 2026. The worked examples are fictional and the wording illustrative. Site collection engages matter-specific legal, employment and data-protection questions on which advice should be taken. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice 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

Site work is core laboratory practice: we run the reconnaissance (questionnaire, IT call, credential verification), build the kit and the day plan from what the site actually holds, negotiate the disruption schedule with your client's business, and execute with the logging, sealing and custody disciplines of the wider series, from single-device visits to multi-day, multi-site campaigns and ordered executions alongside supervising solicitors. Devices that defeat the field (failing media, exotic RAID, locked hardware) come to the laboratory under seal; everything else is imaged where it lives, verified, and couriered on the day's booked transport. The deliverable set (evidence and hash schedules, collection report, logs) lands on the protocol's timetable, exchange-ready, and through **e-discovery.uk** flows straight into processing. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine, and urgent site attendance can usually be mobilised within days, or faster where preservation demands it.

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