



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Locked Mobile Devices

Preservation, Access Routes, Legal Authority and the Decisions That Must Be Made Before Anyone Tries the Passcode

Sooner or later every mobile matter meets the lock screen: the custodian who will not share the passcode, the deceased account holder, the dismissed employee who "forgot", the seized device nobody can open. What happens in the following days: how the device is kept, whether anyone guesses at the code, which legal levers are pulled and in what order: determines whether the lock is a delay or a wall. This guide covers the locked-device problem end to end: why state preservation is the first and least forgiving decision, the realistic access routes (credentials by consent, contract or compulsion; lawful-access tooling; the ensemble around the device), the legal authority questions in civil and criminal contexts including section 49 RIPA, the risks of repeated attempts and biometric improvisation, and the strategy framework that keeps costs proportionate to what the device can actually deliver.

⌚ Estimated reading time: 26 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. Locked devices arrive weekly: employment seizures, estates of the deceased, matrimonial disputes, corporate investigations: and the practice's method is the one this guide teaches: preserve state first, establish the five access facts, run the legal and technical tracks in parallel, and build the ensemble while the gate is worked. Its eDiscovery arm, **e-discovery.uk**, integrates whatever route succeeds into disclosure.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

LOCKED-DEVICE ASSESSMENT

LAWFUL ACCESS & ENSEMBLE STRATEGY

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the wall that is sometimes a door
- 03 First decisions: state, custody and the things nobody must do
- 04 The access routes, ranked by realism
- 05 Legal authority: consent, contract, compulsion and s.49 RIPa
- 06 Risk management: attempts, biometrics, lockouts and wipes
- 07 Strategy: the parallel-tracks framework
- 08 Source architecture: where else the evidence lives
- 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

Executive summary

THE HEADLINE POINT: A LOCKED DEVICE IS A STRATEGY PROBLEM WITH A TECHNICAL COMPONENT, AND THE STRATEGY HAS PARALLEL TRACKS

The lock screen changes the question from "what does the phone hold" to "which of four routes reaches it": and competent practice runs the routes in parallel rather than sequence. **Route one, credentials:** the passcode obtained: by consent (negotiated, incentivised, or offered with privacy protections such as examiner-only handling per guide 117); by contract (employment terms and device policies that oblige disclosure: checked before they are needed); by compulsion (civil courts can order disclosure of access information in support of their processes, with adverse inferences for refusal; criminal and regulatory contexts reach section 49 RIPA notices with their own regime and penalties). Credentials convert most locked-device problems into guide 61's ordinary FFS work: which is why the legal track starts day one, not after the technical track disappoints. **Route two, lawful-access tooling:** the device-, version-, patch- and state-specific frontier of §4: real, uneven, changing monthly, and assessed by a dated capability check rather than assumed in either direction. **Route three, the ensemble:** the cloud accounts, backups, paired computers, counterpart devices and provider records of guide 61 §8: pursued from day one because they frequently answer the case's actual questions while the handset stays shut, and because their own clocks (cloud retention, backup rotation) do not wait for the lock. **Route four, time and events:** devices resurface, passcodes are remembered, litigation positions shift, and capability frontiers move: preserved state keeps every future option open, which is why the first decisions of §3: keep it powered, never reboot, isolate, count and control every attempt: outrank everything else in this guide. The discipline that binds the routes: a written access plan, made early, recording state, the five facts, the routes selected, the attempt budget and the legal steps in motion: the document that keeps a locked device from becoming either a forgotten exhibit or an unbudgeted adventure.

- **State first, always:** AFU preserved is capability preserved; the reboot that closed guide 61's Example 2 is this guide's founding cautionary tale.
- **The legal track is usually the fast track:** ordered or contractually obliged credentials beat months of tooling work: start the correspondence immediately.
- **Attempts are budgeted, never improvised:** lockout escalations and wipe-after-failures settings make every guess a spend from a small account: examiners hold the account.
- **The ensemble runs regardless:** most locked-device matters are decided by evidence that never needed the lock opened.
- **Refusal is evidence:** in civil proceedings, unexplained refusal to provide access invites adverse inference: pleaded properly, it does work the passcode would have.

The problem in plain English: the wall that is sometimes a door

The locked phone triggers two opposite instincts, both expensive. The first is defeatism: the device shelved as inaccessible, the case built without it, the shelf outlasting the limitation period: when a contract clause, a court order or a capability check would have opened it in weeks. The second is obsession: the lock treated as the case's central puzzle, budgets consumed by access attempts, while the cloud account that answered everything sat one preservation letter away. Both instincts share a mistake: treating the lock as a technical fact rather than a strategic position with legal, technical and architectural moves available simultaneously.

The professional posture is the parallel plan: on the day the locked device enters the matter, the state is preserved, the five facts are gathered, the legal levers are identified and pulled, the capability check is commissioned, and the ensemble preservation goes out: five moves, one afternoon, after which the lock is being worked from every side at once and the strategy can follow whichever route opens first.

First decisions: state, custody and the things nobody must do

- **Power and state:** keep it charged; never power off or reboot; record whether it has been unlocked since boot if known: the AFU/BFU position (guide 148) is the single most valuable perishable fact about the device.
- **Isolation:** airplane mode or Faraday handling: the remote-wipe risk is real (personal panic, MDM policy, account-level erase commands) and permanent.
- **No guessing:** no passcode attempts by clients, HR, IT or lawyers: attempt counters, escalating lockouts and wipe-on-failure settings mean improvised guesses spend the budget \$6 manages: sometimes all of it.
- **No biometric improvisation:** presenting the device to its owner's face or finger without authority and planning raises legal and practical issues: biometric windows expire, attempts count, and the lawfulness of compelled biometrics differs from compelled passcodes: examiner-planned or not at all.
- **Custody and record:** photographed state, custody log, storage in controlled conditions: the locked device may wait months for its route; it waits documented.

§ 0 4 · THE ROUTES

The access routes, ranked by realism

ROUTE	REALISM · WHAT GOVERNS IT
Consent (negotiated)	The commonest successful route: custodians provide codes when privacy protections (targeted scope, examiner-only handling, guide 117's password-free patterns) meet their actual concerns: which are usually about exposure, not concealment. Costs a conversation; try it properly first.
Contract / policy	Employment contracts, device policies and MDM terms frequently oblige credential disclosure or permit corporate unlock: checked in every employment and corporate matter before harder levers are reached for.
Court compulsion (civil)	Orders for access information in support of imaging and disclosure obligations; refusal invites adverse inference and enforcement: the route that converts "forgot" into a costed position. Timing: weeks, not months.
Statutory compulsion (s.49 RIPA)	The criminal/regulatory regime for compelled decryption with penal consequences: available to appropriate authorities under its own safeguards, not to civil litigants: known about so its boundaries are not blurred.
Lawful-access tooling	Device/version/patch/state-specific: assessed by dated capability check; sometimes immediate, sometimes contingent (AFU vs BFU), sometimes unavailable: never assumed, in either direction, and re-checked as frontiers move.
The ensemble	Always available in some measure: cloud, backups, paired devices, counterparts, providers: and frequently sufficient: guide 61 §8, run from day one in parallel.

Legal authority: consent, contract, compulsion and s.49 RIPA

- **Consent, documented:** scope, purpose and handling recorded: the consent that protects both sides, and the withdrawal-of-consent position understood before work starts.
- **Contractual obligations, read early:** what the employment contract, acceptable-use policy and MDM enrolment actually say about codes, inspection and return-condition: the clause found in week one is a route; found at trial it is a regret.
- **Civil compulsion and inference:** courts order what disclosure requires, and treat unexplained refusal as it deserves: the correspondence that builds the refusal record (requests, offers of protections, warnings of inference) is itself evidence architecture.
- **Section 49 RIPA, in its lane:** compelled disclosure of protected information's keys under the statutory regime, with offences for non-compliance: the province of investigating authorities under safeguards: civil practitioners cite its existence accurately and do not imitate it.
- **Proportionality and privacy throughout:** the college extraction guidance's concerns govern here at maximum strength: the locked device's owner has rights the access plan must respect, and targeted-scope offers are both lawful practice and the best consent-unlocking tool available.

Risk management: attempts, biometrics, lockouts and wipes

- **The attempt budget:** known-candidate passcodes (family dates, patterns from other devices, codes the client half-remembers) are tried by the examiner, in a planned order, with lockout schedules understood and the wipe-after-failures setting assessed first: the budget is small and spent deliberately.
- **Lockout arithmetic:** escalating delays make scattergun guessing self-defeating within attempts, not days: another reason the candidate list is curated before anything is typed.
- **Biometric windows:** devices demand passcodes after time, restarts and failed attempts: biometric opportunities, where lawful and planned, are used early or lost.
- **Wipe vectors closed:** remote-erase capability (account-level and MDM) confirmed suspended before any network exposure; the §3 isolation maintained until then.
- **Everything logged:** every attempt, prompt and state change recorded: the examination log that answers "what did you do to the device" with a document instead of a memory.

Strategy: the parallel-tracks framework

- **Track A, legal:** consent conversation with protections offered; contract clauses invoked; compulsion applications prepared with the refusal record building: begun day one, because it is usually the fastest route that actually opens.
- **Track B, technical:** dated capability check; attempt budget executed if candidates exist; state preserved for frontier movement: with honest interim reporting ("possible now", "possible if AFU", "not currently possible for this device") that strategy can rely on.
- **Track C, ensemble:** cloud, backup, paired-device and counterpart preservation and collection: often delivering the case's answers while A and B run: and always delivering the comparison layer if the device later opens.
- **Track D, forensic patience:** the device held in preserved state under custody: the option that costs storage and keeps every future route alive: reviewed at case milestones rather than forgotten.
- **The access plan document:** one page recording state, facts, tracks, budgets and review dates: circulated, updated, and doing for locked devices what the layer schedule (guide 60) does for cloud estates.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the locked handset is one node, and the map around it is the working strategy while the gate holds. The ensemble: cloud accounts (message sync, photo libraries, location services, app data: preserved by legal process against the account, which needs no passcode); computer backups (point-in-time phones on laptops and desktops, imaged under guides 41-42); paired computers' sync artefacts (message mirrors, cached media); counterpart devices (every conversation's other end, unlocked by their own owners' cooperation); provider and platform records (operator call/cell data, app-provider business records via legal process); MDM consoles (device state, inventory, compliance history: and the wipe suspension); and physical context (SIMs, memory cards where present, packaging with codes written on it: checked, because people do). The locked device's own future accessibility is part of the map: preserved state is an asset with option value, and the map is what the case runs on while that option matures.

EVIDENCE	LOCKED HANDSET (IF OPENED)	CLOUD ACCOUNT	COMPUTER BACKUPS	PAIRED COMPUTERS	COUNTERPARTS / PROVIDERS	DELETED / RECOVERABLE
Messages	FFS internals + deleted layer	Synced sets: no passcode needed	Point-in-time copies	Mirrors + caches	Other ends; provider records	Ensemble usually suffices
Media	Full stores + caches	Photo libraries	Y	Sync copies	As shared	Cloud recently- deleted windows
Locations	Caches + system artefacts	Location services / timeline	Snapshotted	Limited	Cell records: window-bound	Provider clocks run regardless of the lock
Calls	Logs	Sometimes synced	Y	n/a	Operator records: the independent spine	Y from operators, in window
Account / app activity	FFS artefacts	Provider activity logs	Partial	Session traces	Platform records via process	Varies

Fallback strategy in one line: the lock stops the handset, not the case: cloud process, backups, counterparts and operators proceed on their own authority, and their clocks: not the lock: set this week's priorities.

Worked examples

EXAMPLE 1 · THE CLAUSE THAT OPENED THE PHONE

A suspended trader refused his corporate iPhone's passcode: "personal stuff on there": and the bank's investigation stalled at the lock screen for a fortnight until someone read the device policy he had signed: codes disclosable on request for devices holding firm data, non-compliance a disciplinary matter. Presented with the clause, a targeted-scope offer (trading apps and firm accounts only, examiner-side filtering, personal content unreviewed) and the alternative inference, he provided the code the same afternoon. The examination took four days; the access argument had taken fourteen; and the matter's postscript is this guide's §5: the clause had been sitting in the HR file since onboarding.

EXAMPLE 2 · THE BFU WALL AND THE ENSEMBLE THAT WENT ROUND IT

A deceased director's Android arrived BFU: powered off in a drawer for months, passcode known to nobody, and the capability check honest: not currently accessible for that model and patch. The estate dispute proceeded on the map instead: Google account collection under the estate's authority delivered mail, Drive, photos and location history; his home PC held two full device backups; and the counterpart phones of both co-directors supplied the disputed WhatsApp threads with their own FFS-level deletion analysis. The handset stayed in preserved custody: and eight months later a frontier movement opened its model. The unlock added corroboration; the case had already settled on the ensemble. Both facts belong in this guide.

EXAMPLE 3 · THE REFUSAL THAT TESTIFIED

In a shareholder dispute, a respondent director declined every route: no consent despite protections offered, "forgotten" passcode for a phone in daily use until the week proceedings issued, resistance to the access-information order until compliance was ordered with costs. The phone, finally opened, held little: he had wiped the relevant apps months earlier: but the refusal record had already done the work: the correspondence chronology (offers, protections, warnings, "forgetting") went into the trial bundle, the judge drew the inference the conduct invited, and the judgment's phrase: "a man with nothing to hide rarely needs three court orders to remember a number he typed daily": has outlived the dispute. The lock was empty; the locking was not.

Common mistakes and technical limitations

Common mistakes

- **State destroyed in hour one:** the power-off, the reboot, the client's dozen guesses: capability spent before an examiner was called.
- **Sequential thinking:** months on the technical track before the contract clause was read or the consent conversation attempted: Example 1's fortnight, extended.
- **The ensemble deferred:** cloud and backup clocks running while everyone stared at the lock screen.
- **Defeatism and obsession:** §2's twin failures: the shelved device; the budget-eating siege.
- **Refusal unrecorded:** no protections offered, no warnings given: the inference forfeited by a correspondence file that never built it.
- **Biometric improvisation:** the device waved at its owner in a meeting: unlawful in some contexts, attempt-spending in all.
- **Capability folklore:** access asserted or conceded on last year's news, in either direction.
- **The waiting device forgotten:** preserved custody without milestone reviews: option value left to expire unexamined.

Technical limitations

- **Some walls hold:** current-generation devices in BFU with strong passcodes and no credentials may be genuinely inaccessible today: the honest report says so and dates itself.
- **Frontiers move both ways:** patches close routes as research opens them: capability checks expire.
- **Compulsion compels people, not mathematics:** orders produce codes only from those who yield to orders: the inference, not the unlock, is sometimes the ceiling.
- **Ensemble coverage varies:** a cloudless, backup-less, counterpart-less device exists: rarely: and the map must be walked before its emptiness is asserted.
- **Time costs:** preserved options are not free options: storage, review and the case's own clock are weighed at each milestone.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- State and custody: powered, unbooted, isolated, logged: confirmed in writing today?
- Every credential source: contracts and policies, MDM powers, family/colleague knowledge, written-down codes, other devices sharing the pattern?
- The ensemble census: accounts, backups, paired machines, counterparts: and are their preservations out?

Ask your opponent

- Please provide access information for the device per [order/contract/undertaking], or state the grounds of refusal; our client offers [targeted scope / examiner-only handling / independent review] to meet any privacy concern.
- Please confirm the device's state has been preserved (no power-off, reboot, reset, sync or attempts) since [date], and provide its custody record.
- Please confirm suspension of any remote-wipe capability (account and MDM) affecting the device.

Ask your eDiscovery / forensic provider

- The dated capability position for this exact device and state: and what state preservation keeps open?
- The attempt budget: candidates, order, lockout arithmetic, wipe-setting assessment?
- What does the ensemble deliver this month while the tracks run?

SUGGESTED WORDING · ACCESS-INFORMATION REQUEST (CIVIL, WITH PROTECTIONS)

"We require access to the device for the purposes of [imaging/disclosure] and request that your client provide its passcode within [7] days. To meet any privacy concerns, we propose: examination limited to the categories at Schedule A; extraction and first-stage review by an independent forensic examiner only, with personal content outside Schedule A neither reviewed nor produced; and the examiner's methodology disclosed to you in advance. Please note that the device's state has been forensically preserved, that this request and its response will be before the court on any application, and that unexplained refusal will be relied on in support of adverse inference. Alternatively, we invite your client's proposals for achieving the same evidential result."

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

The locked-device checklist

- ☐ State preserved and recorded hour one: powered, unbooted, isolated
- ☐ Remote-wipe vectors (account, MDM) suspended in writing
- ☐ Five access facts gathered; dated capability check commissioned
- ☐ Contract and policy clauses read; consent conversation had, with protections
- ☐ Ensemble preservations out day one; collections running in parallel
- ☐ Attempt budget curated and examiner-held; every attempt logged
- ☐ Refusal record building in correspondence where consent is withheld
- ☐ Access plan documented: tracks, budgets, review dates
- ☐ Compulsion application prepared while the softer routes run
- ☐ Preserved device reviewed at case milestones against the moving frontier

Red flags

- A device rebooted, reset or "tidied" after the dispute began.
- Client-side passcode guessing already spent.
- A daily-use phone's code "forgotten" on litigation's arrival: Example 3's signature.
- Wipe capability still live over an evidence device.
- Capability assertions without dates or device specifics.
- An ensemble untouched weeks into a lock siege.
- Biometric stunts proposed by anyone but the examiner.

When to involve a digital forensic expert

In hour one, for the state and handling instructions that keep every route alive; at assessment, for the dated capability check and attempt-budget design; through the tracks, where technical work, ensemble collection and the legal correspondence's technical content (protections offered, preservation confirmations demanded) run together; and at milestones, where the preserved device is re-assessed against the frontier. Examples 1-3 are the practice's standing shapes: the clause, the ensemble, the inference: three ways the same lock resolves. Reported under CPR Part 35 with capability positions dated and limits stated: and through **e-discovery.uk**, whichever route opens feeds one integrated disclosure.

§ 1 3 · COMMON QUESTIONS

Frequently asked questions

Can a court really order someone to hand over their passcode?

In civil proceedings, courts order disclosure of access information where necessary to make imaging and disclosure effective, and meet refusal with adverse inference, costs and enforcement: Example 3's machinery. The criminal/regulatory sphere has section 49 RIPA's compelled-disclosure regime with penal teeth, operated by authorities under safeguards. Neither guarantees the code appears: what they guarantee is that refusal acquires a price, which is frequently enough.

How long should we keep a device we cannot currently open?

In preserved custody for the matter's life, reviewed at milestones: Example 2's eight-month frontier movement is not rare, and storage is cheap against the option it keeps open. The review discipline matters more than the duration: a dated re-check at each case stage, and a deliberate decision: not a default: if preservation is ever abandoned.

Is it worth paying for exotic unlocking services?

Frame it as the capability check frames it: what does this device, in this state, actually admit: at what cost, risk and lawfulness: against what the ensemble already delivers? Sometimes specialist access is decisive and proportionate; often the same spend on cloud process and counterpart collection answers the case faster. Beware unconditional promises and provenance-free tools: the access must be lawful, documented and explicable in a CPR 35 report, or it is a liability wearing a receipt.

The custodian offers to unlock it himself and show us the messages. Acceptable?

As a route to scoping conversations, perhaps; as evidence, no: the self-guided tour is uncontrolled (what was scrolled, what was deleted mid-demonstration, what the reading did to disappearing messages) and unrepeatable. The counter-offer is the protections package: examiner extraction, targeted scope, personal content filtered: which meets the legitimate concern behind the offer while producing evidence that survives challenge. Guide 117 details the password-free variants.

What if the device wipes itself during examination?

Planned examination makes this a managed risk, not a gamble: wipe-on-failure settings assessed before attempts, budgets that stop short of trigger counts, isolation preventing remote commands, and: where risk remains: the ensemble collected first so the worst case is bounded. A wipe under uncontrolled amateur attempts is a catastrophe; under laboratory protocol it is a foreseen contingency with the evidence already banked elsewhere.

Does a factory-reset device end the inquiry?

It ends the handset inquiry and starts two others: the ensemble reconstruction (guide 61's Example 3: cloud, backups, mirrors, counterparts routinely rebuild the estate) and the conduct inquiry (the reset's timing, from activation and account records, read against the duty chronology). Modern resets on encrypted devices are genuinely effective against recovery: which is exactly why the reset itself, dated, so often becomes the exhibit.

§ 1 4 · REFERENCE

Glossary

Access plan

The one-page record of state, facts, tracks, budgets and review dates.

Adverse inference

The civil consequence of unexplained refusal; Example 3's engine.

Attempt budget

The curated, examiner-held allowance of passcode candidates.

Biometric window

The expiring period in which face/finger unlock remains available.

Capability check

The dated, device-specific access assessment; never assumed.

Ensemble

The cloud/backup/counterpart/provider map that proceeds despite the lock.

Parallel tracks

Legal, technical, ensemble and patience, run simultaneously.

Refusal record

The correspondence chronology that converts refusal into evidence.

Section 49 RIPA

The statutory compelled-disclosure regime for protected information.

Wipe vectors

Remote and on-device erasure routes; closed before anything else.

Sources and authoritative references

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

- cflab.uk, digital forensics services (locked-device assessment, lawful access, ensemble reconstruction, 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 (parallel-track preservation; whichever route opens, one disclosure): 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
- RIPA 2000 Part III (s.49) and code of practice: legislation.gov.uk, [RIPA Part III](https://legislation.gov.uk/ukpga/2000/24/schedule/1/part_iii) · College of Policing, extraction guidance: college.police.uk
- ISO/IEC 27037: [iso.org](https://www.iso.org), [27037](https://www.iso.org/standard/55855.html) · Forensic Science Regulator: gov.uk/forensic-science-regulator
- PD 57AD and CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad) · justice.gov.uk, [Part 35](https://justice.gov.uk/cpr-part-35) · ICO: ico.org.uk

DISCLAIMER

This publication provides general information about locked mobile devices as at August 2026. Device security and lawful-access capability change rapidly and vary by model, version, patch and state; statutory regimes carry their own conditions and safeguards; verify the current position for the specific device and context in the matter at hand. 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. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Locked devices are managed at the laboratory as strategy, not siege: the hour-one handling instructions issued to whoever holds the device; the five facts and dated capability check within days; the parallel tracks: consent-with-protections drafting support, contract-clause identification, compulsion-application technical content, attempt budgets, ensemble preservation and collection: run together under a written access plan with milestone reviews. Examples 1-3 are the practice's recurring resolutions: the clause, the ensemble, the inference: and the preserved-custody service keeps the fourth resolution, frontier movement, permanently in play. Reporting is CPR Part 35 with capability positions dated and privacy architecture built in; through **e-discovery.uk**, whichever route opens is processed into one coherent disclosure. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a locked device is sitting in someone's drawer on your matter, the first call is about its battery.



I N S T R U C T T H E L A B

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