COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Collecting Without the Password

Locked Devices, Withheld Credentials and the Law of Compelled Access

The device is in hand, but it is locked; the account holds the evidence, but the password is withheld; the container is encrypted, and the key is "forgotten". Access denial is one of the most common obstacles in digital evidence, and it sits at the meeting point of technology and law. On the technical side, some locks can be bypassed and many cannot: modern device encryption is genuinely strong, and the honest examiner distinguishes what is recoverable from what is not. On the legal side, English law has real tools to compel the production of a password or key, from civil disclosure orders to a specific statutory notice regime, but they carry conditions, limits and consequences that a lawyer must understand before relying on them. The wrong move, self-help access that breaks the law, or a compulsion application that fails, wastes the evidence and the opportunity. This guide sets out for UK lawyers what can and cannot be accessed technically, the lawful routes to compel or obtain access, and how to deploy them without breaching the very law the case depends on.

⏱ Estimated reading time: 25 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-device and withheld-credential problems are recurring instructions: the honest assessment of what is technically accessible, the lawful pursuit of passwords and keys through civil orders and, in criminal matters, the statutory notice regime, and the preservation of admissibility throughout: reported under CPR Part 35 and CrimPR Part 19, with the technical limits stated as plainly as the possibilities.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | LOCKED-DEVICE ASSESSMENT | COMPELLED-ACCESS SUPPORT | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: A LOCKED DEVICE OR WITHHELD PASSWORD IS A PROBLEM WITH TWO HALVES: AN HONEST TECHNICAL ASSESSMENT OF WHAT CAN ACTUALLY BE ACCESSED, AND A LAWFUL LEGAL ROUTE TO COMPEL OR OBTAIN THE KEY, CHOSEN FOR THE CIVIL OR CRIMINAL CONTEXT, BECAUSE SELF-HELP ACCESS CAN BE A CRIME AND MODERN ENCRYPTION IS OFTEN GENUINELY UNBREAKABLE

The technical reality (§3): some locks yield (weak passwords, older devices, cached credentials, recovery keys held by an organisation, cloud copies that were never locked) and many do not (modern full-device encryption with strong passcodes is, honestly, not brute-forceable in any useful time): the examiner's first job is the truthful assessment of which situation applies, so effort is not wasted and expectations are not falsely raised. **The civil routes (§4):** in civil litigation, orders requiring a party to provide passwords and decryption keys as part of their disclosure obligations, unless orders backing them, and adverse inferences and strike-out where a party refuses: the court's power to make withholding access costly, deployed through the disclosure machinery (guides 95, 110). **The criminal route (§5):** in the criminal and investigatory context, a specific statutory notice regime under the Regulation of Investigatory Powers Act 2000 Part III compels the production of a key or protected information, with failure to comply a criminal offence in itself: a powerful but condition-bound tool, distinct from the civil routes and not available to private litigants. **Reaching around it (§6):** the locked device is rarely the only source: cloud backups made before the lock, organisational recovery keys and escrow, synced copies, counterparts' copies, and the estate's redundancy (guides 95, 111 to 114) frequently deliver the evidence without ever opening the device. **Deployment (§7):** the route chosen for the context and the honest technical position, the consequences of refusal (inference, strike-out, or a criminal offence) understood, and self-help access avoided because unauthorised access to a device or account can itself be a crime (Computer Misuse Act 1990).

- **Assess honestly first:** some locks open and many do not: the truthful technical position governs everything after it.
- **Civil courts compel by disclosure:** passwords and keys ordered, backed by unless orders, inference and strike-out.
- **Criminal law has a key regime:** the RIPA Part III notice compels keys, with non-compliance a distinct offence.
- **Reach around the lock:** backups, recovery keys, syncs and counterparts often hold the evidence unlocked.
- **Never self-help:** unauthorised access to a device or account can be a crime: use the lawful route.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the evidence is there but locked away

Access denial feels like a technical problem, and lawyers instinctively ask the examiner to "crack it". Sometimes that is possible; increasingly it is not. Device and file encryption has become genuinely strong, to the point where a modern phone or laptop secured with a good passcode is, for practical purposes, not openable by brute force within the lifetime of the case or the litigant. An examiner who promises otherwise is either lucky in the particular device or overselling. So the first task is not to attack the lock but to assess it honestly: is this a lock that yields, or one that does not?

When the lock does not yield, the problem stops being technical and becomes legal, and here English law is more helpful than lawyers sometimes realise, but in ways that differ sharply between the civil and criminal contexts. A civil court can order a party to hand over their passwords and keys as part of disclosure, and punish refusal with the full weight of the disclosure sanctions, up to striking out their case. In the criminal and investigatory sphere, a specific statutory regime compels the production of keys, with a criminal penalty for refusal, but it is available only to the authorities and only on conditions. And running underneath both is a hard limit: nobody may simply help themselves to a locked device or account, because unauthorised access is itself a criminal offence. The art is to assess the lock honestly, reach around it through the estate wherever possible, and where the key is genuinely needed, compel it by the route the context allows, never by self-help. This guide takes those in turn.

§ 0 3 · WHAT CAN AND CANNOT BE ACCESSED

What can and cannot be accessed technically

- **Locks that often yield:** weak or common passwords vulnerable to dictionary attack; older devices and operating systems without modern encryption; unencrypted devices where only a login stands in the way; cached and saved credentials in browsers and keychains (guide 51); and organisational recovery keys held in device management or escrow: the situations where lawful access is realistic.
- **Locks that generally do not yield:** modern full-device encryption (contemporary phones and laptops) secured with a strong passcode, where the encryption is sound and no shortcut exists; well-implemented container encryption with a strong key; and hardware-backed keys tied to a secure element: the situations where the honest answer is that brute force will not work in any useful time.
- **The recovery-key route:** full-disk encryption in a managed environment usually has a recovery key held by the organisation (BitLocker recovery keys in the directory, FileVault institutional keys): the "locked" device opened lawfully with the key the employer already holds (guide 118's territory): the first thing to check in any corporate matter.
- **The cloud copy that was never locked:** the device is locked but its data was backed up unencrypted, or with a recoverable key, to a cloud account (guide 5): the evidence reached from the backup without touching the lock at all: §6's principle, previewed.
- **The honest assessment:** the examiner's first deliverable is the truthful statement of which category the device falls into, so that the legal strategy is built on reality, effort is not wasted on unbreakable locks, and the client is not promised access that cannot be delivered (guide 100's honest-limits discipline).

§ 0 4 · THE CIVIL ROUTES

The civil routes: disclosure orders, unless orders and inference

- **Passwords and keys as part of disclosure:** in civil litigation, a party's disclosure obligation can extend to providing the passwords and decryption keys needed to access relevant documents within their control: the court ordering the key as the means of giving disclosure of what it unlocks (guide 94's control principle).
- **Specific disclosure and access orders:** applications for specific disclosure, and orders for access to or imaging of devices and accounts on defined terms, requiring the respondent to enable access: the machinery of PD 57AD and CPR 31 pointed at the locked source.
- **Unless orders:** orders that a party provide the password or key by a date, failing which their statement of case is struck out (in whole or relevant part): the compulsion given teeth, so refusal risks losing the case rather than merely the document.
- **Adverse inference:** where a party withholds a key to relevant material, the court may draw inferences against them about what the material would have shown (guide 95 §7), so that the refusal itself becomes evidence: the withholding costly even if the lock is never opened.
- **The independent-examiner safeguard:** access ordered on terms that an independent examiner opens the device and discloses only the relevant material, protecting privilege and private data (guides 97 §7, 115 §7): the access compelled without handing the whole device to the opponent, which the court prefers and the respondent can accept.

§ 0 5 · THE CRIMINAL ROUTE

The criminal route: the statutory notice regime for keys

- **The RIPA Part III notice:** in the investigatory and criminal context, Part III of the Regulation of Investigatory Powers Act 2000 empowers a notice requiring a person to disclose a key, or to put protected information into an intelligible form: the statutory compulsion of decryption, available to the authorities on the Act's conditions and with the requisite permissions.
- **Failure to comply is an offence:** non-compliance with a valid Part III notice is itself a criminal offence, with a higher penalty in national-security and certain other cases: the refusal criminalised directly, distinct from any offence the protected data might reveal.
- **Conditions and safeguards:** the regime carries conditions (the requisite authority, the necessity and proportionality tests, the handling of keys and the safeguards around them): the notice not a free-standing demand but a controlled statutory power, and its use a matter for those authorised to wield it.
- **Not a private-litigant tool:** the Part III regime is for the authorities, not for parties to civil litigation, who must use the civil routes of §4: the distinction critical, because a civil litigant who imagines they can invoke a key-disclosure notice is mistaken.
- **The privilege-against-self-incrimination debate:** the tension between compelled key disclosure and the privilege against self-incrimination has been litigated, with the courts upholding the regime in defined terms: an area where the criminal-law position is specialist and current authority is checked, not assumed.

§ 0 6 · REACHING AROUND IT

Reaching the evidence another way: the estate around the locked device

- **Cloud backups made before the lock:** the locked phone's iCloud or Google backup, the locked laptop's cloud sync: copies of the data made automatically and held in an account that may be accessible by consent, recovery or order (guide 5): the evidence reached from the backup, the lock irrelevant.
- **Organisational recovery keys and escrow:** in corporate environments, the recovery keys the organisation already holds (guide 118), and credential escrow in identity and device-management platforms: the "locked" corporate device opened with the employer's own key, no compulsion of the custodian needed.
- **Synced and counterpart copies:** the synced copies on the custodian's other devices, the counterparties' copies of every message and shared document, other members' copies of shared workspaces (guides 101, 111 to 114): the content that lives in many places, only one of which is locked.
- **Server-side platform data:** the mailbox, the SaaS records, the cloud-infrastructure logs (guides 113, 114) held server-side and reachable through the controlling account, quite independent of any locked endpoint: the modern estate frequently accessible while the device stays shut.
- **The lock as a last resort, not a first:** the discipline of asking, before any attempt to compel or open the device, what the estate already holds unlocked: often the answer is most of it, and the locked device is needed only for the deleted or local-only residue (guide 95's redundancy principle).

§ 0 7 · DEPLOYMENT

Deployment: choosing the route and the consequences of refusal

- **Context decides the route:** civil litigation uses the disclosure-order, unless-order and inference machinery of §4; the criminal and investigatory context uses the Part III regime of §5; and both begin with the honest technical assessment of §3 and the reach-around of §6: the route matched to the forum, never confused between them.
- **The consequences of civil refusal:** a party who defies an order to provide a key faces adverse inference, an unless order, strike-out of the relevant case, and a collapse of credibility on every issue (guides 95 §7, 110 §7): the refusal, in practice, often worse for them than the disclosure would have been.
- **The consequences of criminal refusal:** failure to comply with a valid Part III notice is a criminal offence in itself (§5): the refusal a separate crime, whatever the protected data holds.
- **The self-help prohibition:** under no route may a party simply access a locked device or account without authority, because unauthorised access is an offence under the Computer Misuse Act 1990 (guide 42): the lawful route used, however tempting the shortcut, because self-help access poisons the evidence and exposes the accessor.
- **The proportionality of pursuit:** where the estate (§6) already holds the material, an expensive fight to compel a key may be disproportionate; where the locked device holds unique, central evidence, the compulsion is justified: the pursuit sized to what the lock actually guards (guide 20's balance).

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a locked device is one node, and the evidence it guards is usually reflected across an estate whose other nodes are not locked. The device holds the local and deleted material behind the lock. But the cloud backup holds a copy made before or despite the lock; the organisation's recovery-key store holds the means to open a managed device; the synced copies on other devices hold the same data; the server-side mailbox, drives and SaaS hold much of it independent of any endpoint; and the counterparties hold their side of every communication. The discipline is to map these before attacking the lock: to ask what is already reachable unlocked, and to reduce the locked-device problem to the residue that genuinely exists only behind the lock. Then, for that residue, the lawful compulsion route is chosen by context. When the lock is unbreakable and the custodian refuses the key, the estate often still delivers the case, and the refusal itself becomes evidence; when the estate is thin and the locked device holds unique material, the compulsion machinery, civil or criminal, is deployed in earnest.

QUESTION	LOCKED DEVICE	CLOUD BACKUP	RECOVERY-KEY STORE	SYNCED / COUNTERPART COPIES	SERVER-SIDE PLATFORMS	COMPULSION ROUTE
Messages	Behind the lock	Y: pre-lock backup	n/a	Y: other devices, counterparts	Y: platform-held	Civil order / Part III
Documents	Behind the lock	Y: synced copy	Opens managed device	Y: shared copies	Y: drives, SaaS	Civil order
Local-only / deleted	Y: device only	Sometimes in backup	Opens the device to reach it	n/a	Version history	Needed where estate is thin
The key itself	Held by custodian	n/a	Y: org holds it	n/a	n/a	Y: compelled by order / notice
Refusal as evidence	n/a	n/a	n/a	n/a	n/a	Y: inference / offence

Fallback strategy in one line: map what the estate already holds unlocked and take it; reduce the problem to the genuinely locked-only residue; then compel the key by the civil or criminal route the context allows, never by self-help.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE UNBREAKABLE PHONE AND THE BACKUP THAT WAS NOT

A commercial-fraud claimant needed the WhatsApp messages on a defendant's modern smartphone, which was locked with a strong passcode. The instinct was to demand the laboratory "crack it"; the §3 honest assessment was that the device's encryption was sound and brute force would not open it in any useful time. Rather than fight an unwinnable technical battle or an expensive compulsion application for a key the defendant might genuinely refuse, the §6 reach-around was tried first: the defendant's own disclosure listed an iCloud account, and that account held an automatic backup of the phone made two days before the litigation, including the WhatsApp database, recoverable with the account credentials the defendant was ordered to provide as part of ordinary disclosure (§4). The locked phone was never opened; the evidence came from the backup it had made of itself. The lesson is §6's: the lock guards the device, not always the data, and the data had copied itself somewhere unlocked.

EXAMPLE 2 · THE UNLESS ORDER AND THE SUDDEN RECOLLECTION

In a partnership dispute, a partner's laptop held the relevant accounts in an encrypted container, and he claimed to have "forgotten" the password. The §3 assessment was that the container's encryption was strong and the password genuinely necessary. The §4 civil route was deployed: the court ordered him to provide the password, and when the claimed amnesia persisted, made an unless order that his defence be struck out unless the password was provided within fourteen days, on terms that an independent examiner would open the container and disclose only the relevant material (the §4 safeguard, protecting his unrelated private data). The forgotten password was recollected with two days to spare. The §7 consequence, the real prospect of losing the case, achieved what no technical attack could, and the independent-examiner term made compliance acceptable to him. The court's power to make refusal costlier than compliance is often the most effective decryption tool there is.

EXAMPLE 3 · THE CORPORATE DEVICE THAT WAS NEVER REALLY LOCKED

An employer believed a departed employee's company laptop, encrypted and returned locked, was inaccessible, and considered an expensive application to compel the password. The §3 and §6 first questions saved the cost entirely: the laptop's full-disk encryption was managed through the company's own device-management platform, which held the recovery key (guide 118). The employer already possessed the means to open its own device; no compulsion of the former employee was needed at all. The independent examiner used the recovery key to image the laptop lawfully, and the collection proceeded normally. The lesson is the one §3 and §6 press in every corporate matter: before treating a managed device as locked, check whether the organisation holds the recovery key, because it very often does, and the "locked" device is open with a key already in the employer's hands.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Assuming everything can be cracked:** the examiner asked to brute-force a modern strong-passcode device, effort and money spent on an unwinnable technical fight: §3's honest assessment skipped.
- **Assuming nothing can be accessed:** the opposite error: a "locked" managed device abandoned when the organisation held the recovery key all along (Example 3), or the data sat in an unlocked backup (Example 1).
- **Confusing the civil and criminal routes:** a civil litigant imagining they can invoke a Part III key-disclosure notice, which is for the authorities only (§5).
- **Self-help access:** a party accessing a locked device or account without authority, committing a Computer Misuse Act offence and poisoning the evidence (§7).
- **The estate unmapped:** an expensive fight to open the device run while backups, syncs and counterparts held the material unlocked (§6).
- **Orders without teeth:** a disclosure order for a password made without the unless-order backing that makes refusal costly (§4).
- **Whole-device access demanded:** the opponent's whole device sought where the independent-examiner term would have secured the relevant material and protected privilege and privacy (§4).
- **Refusal not exploited:** a withheld key treated only as an obstacle, not deployed as the adverse-inference evidence it also is (§7).

Technical limitations

- **Strong modern encryption is genuinely unbreakable:** a contemporary device with a strong passcode will not yield to brute force in any useful time: the honest position, stated, not wished away.
- **Recovery keys depend on the environment:** managed devices usually have them; personal devices usually do not: the corporate case is far more openable than the personal one.
- **Backups may be encrypted too:** a backup secured with a strong key is as locked as the device: the reach-around works only where the copy is genuinely accessible.
- **Compulsion cannot conjure a forgotten key:** where a key is genuinely lost, no order recovers it; the estate and the inference must carry the case (Example 2 turned on the key not being truly forgotten).
- **The law is specialist and current:** the self-incrimination and Part III case law evolves; the criminal-access position is checked against current authority, not assumed.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the locked device company-managed, so a recovery key may already be held, or personal, where it usually is not?
- What backups, syncs, cloud accounts and counterpart copies exist that may hold the same data unlocked?
- Is this a civil matter (disclosure-order routes) or a criminal or investigatory one (the statutory notice regime)?

Ask your opponent (or the reluctant party)

- Please provide the passwords and decryption keys necessary to access the relevant material on the device(s) and account(s) identified, as part of your disclosure obligation, on terms that an independent examiner will access the device and disclose only the relevant material.
- Please confirm whether the device(s) are managed such that a recovery key is held by the organisation, and if so provide it, and identify all backups, synchronised copies and cloud accounts holding the same data.
- Please confirm that no attempt has been made, and none will be made, to access any device or account without authority, and that the devices have been preserved unaltered.

Ask your eDiscovery / forensic provider

- Honestly, is this lock one that yields or one that does not?
- What does the estate already hold unlocked, and what genuinely exists only behind the lock?
- Is there an organisational recovery key or an accessible backup that opens this without compelling the custodian?

SUGGESTED WORDING · APPLICATION NOTE FOR A PASSWORD / KEY ORDER (CIVIL)

> "The Respondent holds relevant documents within its control on the encrypted device(s) and account(s) identified, access to which requires passwords or decryption keys the Respondent has not provided. The Applicant seeks an order that the Respondent provide the necessary passwords and keys, alternatively enable access, by [date], such access to be effected by an independent forensic examiner who shall image the device(s), apply the agreed search terms and date ranges, and disclose only the relevant material, holding all other data under the examiner's control to protect privilege and private data. The Applicant seeks that the order be made an unless order, such that in default the Respondent's [statement of case / relevant part] be struck out, and reserves the right to invite the court to draw adverse inferences from any failure to provide access as to the content of the material withheld. The Applicant confirms that no unauthorised access to the device(s) has been or will be attempted."

§ 12 · QUICK CONTROL

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

The locked-access checklist

- ☐ Honest technical assessment obtained: does this lock yield or not?
- ☐ Device ownership established: managed (recovery key likely) or personal
- ☐ Organisational recovery-key and escrow stores checked first
- ☐ Estate mapped for backups, syncs, cloud and counterpart copies
- ☐ Locked-only residue identified after the reach-around
- ☐ Correct route chosen: civil disclosure machinery or the statutory notice regime
- ☐ Order sought with unless-order backing and independent-examiner terms
- ☐ Adverse-inference position preserved against refusal
- ☐ No self-help access attempted; devices preserved unaltered
- ☐ Proportionality of pursuit weighed against what the estate already holds

Red flags

- A demand to "just crack" a modern strong-passcode device: Example 1's instinct.
- A managed corporate device abandoned as locked without checking for a recovery key: Example 3.
- A civil litigant reaching for the criminal key-notice regime.
- Any sign of self-help access to a device or account.
- A key "forgotten" only once disclosure was ordered: Example 2.
- An expensive compulsion fight run while the estate holds the data unlocked.
- Whole-device access demanded without the independent-examiner safeguard.

When to involve a digital forensic expert

At the outset, for the honest assessment of whether the lock yields, so the legal strategy is built on reality rather than hope (Example 1); before any compulsion application, to map the estate and check for recovery keys and backups that may open the source without compelling the custodian (Example 3); at the application, where the independent-examiner terms and the imaging are specified so access is compelled safely and admissibly (Example 2); and at deployment, where the technical position and any refusal are explained under CPR Part 35 or CrimPR Part 19, and self-help is scrupulously avoided. Through **cflab.uk** and **e-discovery.uk**, locked-access problems are met with a truthful technical assessment, a mapped reach-around, and support for the lawful compulsion route the context allows: because the honest answer about a lock, and the lawful way around or through it, is worth more than a promise to crack the uncrackable.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can you just crack the password on a locked phone?

Sometimes, and often not: weak passwords and older devices may yield, but a modern phone with a strong passcode has sound encryption that brute force will not open in any useful time (§3). The honest assessment comes first, so effort is not wasted. And frequently it is unnecessary: the data may sit in an unlocked backup or a synced copy the lock does not guard (§6, Example 1).

Can a civil court make someone hand over their password?

Yes: a party's disclosure obligation can require them to provide the passwords and keys needed to access relevant material within their control, and the court backs this with unless orders (comply or be struck out) and adverse inferences (§4). Access is usually ordered on terms that an independent examiner opens the device and discloses only the relevant material, which protects privilege and privacy and makes compliance acceptable (Example 2).

Is there a law that forces someone to decrypt data?

In the criminal and investigatory context, yes: Part III of the Regulation of Investigatory Powers Act 2000 lets the authorities serve a notice compelling a key or the intelligible form of protected information, and failure to comply is itself an offence (§5). But it is a tool for the authorities on statutory conditions, not for private civil litigants, who use the disclosure-order routes of §4 instead.

Can we just try to guess the password or get into the account ourselves?

No: unauthorised access to a device or account is a criminal offence under the Computer Misuse Act 1990 (§7), and self-help access poisons the evidence and exposes whoever attempts it. Use the lawful route: the recovery key the organisation holds, the accessible backup, or a court order compelling the key. However tempting the shortcut, it is a crime and it ruins the case.

The device is locked and encryption is unbreakable. Is the case lost?

Rarely: the lock guards the device, not usually the data (§6). Cloud backups, synced copies on other devices, organisational recovery keys, server-side mailbox and SaaS data, and counterparts' copies frequently hold the same material unlocked (Example 1, Example 3). Map the estate first; the locked device is often needed only for deleted or local-only residue, and even a refused key becomes adverse-inference evidence (§7).

The employee returned a locked company laptop. What now?

Check for the recovery key before anything else (§3, §6): managed corporate devices are almost always encrypted through a platform that holds a recovery key, so the employer can open its own device without compelling the former employee at all (Example 3, guide 118). If it is genuinely unmanaged, then the estate reach-around and, if needed, a disclosure order follow. But in most corporate cases the "locked" device is open with a key you already hold.

§ 14 · REFERENCE

Glossary

Full-device encryption
Encryption of a whole device, unlocked by a passcode or key.

Recovery key
A key held to unlock an encrypted device, often by an organisation.

Brute force
Trying many keys or passwords; defeated by strong modern encryption.

Unless order
An order striking out a case unless a step (providing a key) is taken.

Adverse inference
A conclusion drawn against a party who withholds evidence.

RIPA Part III
The statutory regime compelling disclosure of keys in the criminal context.

Computer Misuse Act
The Act criminalising unauthorised access to computers.

Independent examiner
A neutral examiner opening a device and filtering relevant material.

Escrow
Credentials or keys held by an organisation for recovery.

Secure element
Hardware storing keys, resistant to extraction.

Sources and authoritative references

The compelled-access 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, recovery-key and independent-examiner access, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (estate reach-around and access collection as practised): 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
- Regulation of Investigatory Powers Act 2000, Part III (investigation of protected electronic information): legislation.gov.uk, RIPA Part III · Computer Misuse Act 1990: legislation.gov.uk, CMA 1990
- PD 57AD (disclosure duties and control) and CPR Part 31 (specific disclosure): justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- Home Office, RIPA Part III Code of Practice (investigation of protected electronic information): gov.uk, Part III Code · ISO/IEC 27037: iso.org, 27037

DISCLAIMER

This publication provides general information about collecting from locked devices and withheld credentials as at August 2026. Encryption technology, the case law on compelled key disclosure and the privilege against self-incrimination, and the statutory access regime all evolve; verify the current position for the devices and matter at hand, and take specialist criminal-law advice before relying on the statutory notice regime. Nothing here endorses unauthorised access to any device or account, which is a criminal offence. 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-access work at the laboratory starts with the truth: an honest assessment of whether the lock yields or does not, so no money is spent attacking unbreakable encryption and no client is promised access that cannot be delivered (Example 1). Before any compulsion is contemplated, the estate is mapped for the copies the lock does not guard, the organisation's own recovery keys, the pre-lock cloud backups, the synced and counterpart copies, the server-side mailbox and SaaS data, because in most corporate matters the device is open with a key the employer already holds or the data sits somewhere unlocked (Example 3). For the residue that genuinely exists only behind the lock, the lawful route is supported by context: the civil disclosure-order, unless-order and independent-examiner machinery in litigation (Example 2), and, in the criminal and investigatory sphere, the statutory notice regime in the hands of those authorised to use it. Self-help access is never attempted, because it is a crime and it ruins the evidence. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a device has come back locked, the first questions are the useful ones: does this lock actually yield, and what does the estate already hold unlocked?

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