COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iPhone and iPad Forensics: The Acquisition Challenge

Why the Phone in the Evidence Bag Is the Hardest Device to Open, and What Decides Whether It Can Be

The iPhone is, for most people, the single richest record of their life, messages, photos, location, health, apps, accounts, and it is also the hardest mainstream device to acquire forensically. Everything is encrypted, tied to a passcode and to a dedicated security chip, and the phone actively resists extraction: it locks, limits passcode attempts, and can be wiped remotely. What can actually be obtained from a given iPhone is not a fixed thing; it depends on a handful of specific factors, the model and iOS version, whether the device is locked or unlocked, whether the passcode is known, and the state it is in when it reaches the examiner. The single most consequential moment is often the first one: how the phone is handled at seizure frequently decides how much can ever be recovered. This guide opens the iPhone and iPad block and sets out for UK lawyers why iOS acquisition is so constrained, what factors govern it, how a phone should be handled to preserve the possibilities, and how to set realistic, honest expectations.

⏱ 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. iPhone and iPad acquisition is a core competence: assessing what a specific device will yield given its model, iOS version, lock state and passcode, handling and preserving devices so possibilities are not lost at seizure, and reaching the evidence lawfully through the device, its backups and the iCloud estate. The work is reported under CPR Part 35 and CrimPR Part 19 with the feasibility and honest limits of each acquisition set out plainly, because on iOS what can be obtained is never assumed.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | IPHONE & IPAD ACQUISITION | LOCK-STATE & PASSCODE ASSESSMENT | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: the iPhone is the richest record of a person's life and the hardest mainstream device to acquire, because everything is encrypted and passcode-bound and the phone actively resists extraction, so what can be obtained depends on specific factors, and how the device is handled at seizure often decides how much can ever be recovered.

Why iOS resists (§3): full encryption tied to the passcode and a dedicated security chip, limited passcode attempts, auto-lock and remote-wipe, all designed to make extraction hard. **The deciding factors (§4):** the model and iOS version, whether the device is locked or unlocked, whether the passcode is known, and the state it arrives in, together govern what is feasible. **Handling at seizure (§5):** the decisive first moments, keeping the device from locking, from the network and from remote wipe can preserve possibilities that are otherwise lost forever. **Realistic expectations (§6):** feasibility is assessed and stated honestly per device, since what a phone will yield is never assumed. **Deployment (§7):** preservation, lawful access to the passcode, and the backups and iCloud estate that hold much of the same data.

- **Richest device, hardest to open:** the iPhone holds everything and resists extraction by design.
- **Feasibility is not fixed:** what can be obtained depends on model, iOS, lock state and passcode.
- **Seizure decides the outcome:** the first moments often set how much can ever be recovered.
- **Keep it unlocked, off the network:** prevent locking and remote wipe to preserve possibilities.
- **Set honest expectations:** feasibility is assessed per device, never assumed.

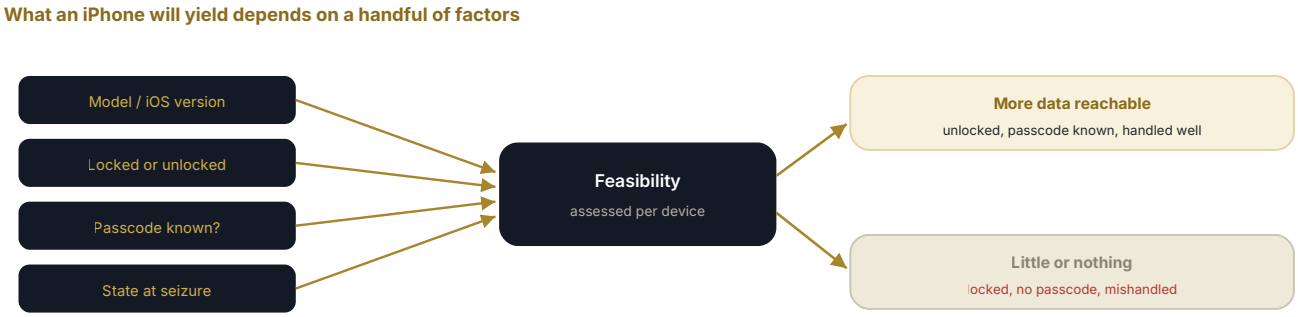

Figure 1 - what an iPhone will yield is not fixed: model, iOS version, lock state, passcode and handling at seizure together decide whether much, or almost nothing, can be recovered.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the richest device, the hardest to open

For most people, the iPhone is the most complete record of their life that exists anywhere. It holds their messages across many apps, their photographs and the places those photos were taken, their movements, their health data, their web activity, their accounts, and the traces of almost everything they do. In litigation, that makes it often the single most important source of evidence. It is also, paradoxically, the hardest mainstream device to get evidence out of, and it is important that lawyers understand why, because the assumption that a phone can simply be plugged in and read is wrong, and acting on it can destroy evidence.

The reason is that the iPhone is built, deliberately and thoroughly, to resist exactly what a forensic examiner wants to do. Its storage is fully encrypted, and the key is tied to the user's passcode and protected by a dedicated security chip, so without the passcode the data is unreadable. The phone limits how many passcode guesses can be made and slows them down, so brute force is impractical. It locks itself automatically, and once locked it yields far less. And it can be wiped remotely, so a device left connected to a network can be erased before it is examined. The consequence is that what can actually be obtained from a particular iPhone is not a fixed quantity; it varies enormously depending on the specific device and its circumstances, above all its model and iOS version, whether it is locked or unlocked, and whether the passcode is known. And because the phone actively degrades the possibilities, by locking, by accepting a remote wipe, the moment of seizure is frequently decisive: how the device is handled in the first minutes often determines how much can ever be recovered from it. This guide, opening the iPhone and iPad block, explains why iOS resists acquisition, what factors govern the outcome, how a phone should be handled to preserve the possibilities, and how to set honest expectations about what any given device will yield.

§ 0 3 · WHY IOS RESISTS

Why iOS resists acquisition

- **Full encryption tied to the passcode:** the device's storage encrypted and the key bound to the user's passcode and the security hardware, so without the passcode the data is unreadable, the foundation of iOS's resistance (guide 133's Apple-encryption theme): the locked-by-default state.
- **A dedicated security chip:** a Secure Enclave holding keys and enforcing protections, so the encryption cannot be defeated by attacking the storage and the passcode cannot be extracted, access is by authentication (guide 133): the hardware guardian.
- **Limited passcode attempts:** the device limiting and slowing passcode guesses, and optionally wiping after too many, so brute force is impractical and reckless attempts risk destroying the data: the anti-guessing defence.
- **Auto-lock and reduced access when locked:** the phone locking itself and yielding far less once locked, so an unlocked device is vastly more acquirable than a locked one, making lock state pivotal (§4): the locking penalty.
- **Remote wipe:** the ability to erase the device remotely, so a phone left on a network can be wiped before examination, making network isolation urgent (§5): the remote-erasure risk.

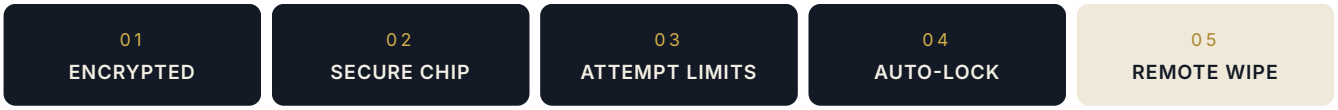

Figure 2 - the layers of iOS resistance, from full encryption and the security chip to attempt limits, auto-lock and remote wipe, each shaping what can be acquired.

§ 0 4 · THE DECIDING FACTORS

The factors that decide what can be obtained

- **Model and iOS version:** the specific hardware and software generation determining which acquisition methods are even possible, since capabilities differ sharply across models and versions, so the device is assessed, not assumed (§6): the first, foundational factor.
- **Locked or unlocked:** whether the device is locked, the single biggest lever, an unlocked phone yields far more than a locked one, so its state on arrival is decisive (§5): the pivotal factor.
- **Passcode known or not:** whether the passcode is available, by cooperation or lawful compulsion, since with it the device can be unlocked and far more obtained, and without it access is severely limited (guide 117): the access factor.
- **State at seizure:** the condition the device arrives in, powered, unlocked, network-isolated, or off, locked and exposed, reflecting how it was handled, and directly shaping feasibility (§5): the handling factor.
- **Together, not singly:** these factors interacting, so feasibility is a judgement on the specific device in its specific state, not a general rule, which is why every phone is assessed individually (§6): the combined assessment.

§ 0 5 · HANDLING AT SEIZURE

Handling at seizure: the decisive first moments

- **Keep it unlocked if it is:** a device found unlocked kept unlocked and prevented from locking or sleeping, since an unlocked phone is far more acquirable and letting it lock can be irreversible (§4): the possibility preserved.
- **Isolate from the network:** the device isolated from mobile and Wi-Fi networks promptly to prevent remote wipe and remote locking, using appropriate shielding, so it cannot be erased before examination (guide 110): the wipe prevented.
- **Do not guess the passcode:** passcode guessing avoided, since attempts are limited and may trigger a wipe, so access is sought lawfully rather than by risky guessing (§3): the data not destroyed.
- **Preserve power appropriately:** the device's power managed so it does not run flat or, where relevant, enter a more locked state, keeping it in the most acquirable condition (guide 131's keep-alive theme): the state maintained.
- **Get it to an examiner fast:** the phone brought to a forensic examiner quickly, in its preserved state, so the acquisition is attempted while the possibilities remain, because delay and mishandling close doors (§7): the speed that saves the evidence.

§ 0 6 · REALISTIC EXPECTATIONS

Setting realistic expectations honestly

- **Assess, do not assume:** the feasibility of acquisition assessed for the specific device given its model, iOS, lock state and passcode, so expectations rest on the real device, not a general belief (§4): the honest starting point.
- **No universal promise:** no blanket assurance that any iPhone can be fully extracted, since capability varies and some locked devices yield little, so overpromising is avoided (guide 100): the promise not made.
- **The passcode changes everything:** the presence or absence of the passcode explained as the central determinant, so the value of obtaining it lawfully is understood (guide 117): the key variable communicated.
- **The estate as the fallback:** where the device yields little, the backups and iCloud estate often hold much of the same data, so a difficult phone does not always mean lost evidence (§8): the alternative kept in view.
- **State limits plainly:** what can and cannot be obtained, and the confidence in it, stated clearly to instructing lawyers, so decisions rest on reality (guide 100): the truthful account.

§ 0 7 · DEPLOYMENT

Deployment: preservation, access and the estate

- **Preservation first:** the device preserved correctly at seizure, unlocked if possible, network-isolated, unguessed, so the acquisition possibilities are kept open, the single most consequential step (§5): the doors kept open.
- **Lawful access to the passcode:** the passcode obtained by cooperation or lawful compulsion where available, since it transforms what can be acquired (guide 117): the access secured lawfully.
- **Acquisition matched to the device:** the acquisition method chosen for the specific device and its state (the subject of guide 146), so the most is obtained within what is feasible: the right method applied.
- **The backups and iCloud estate:** the device's backups and the iCloud account preserved and, where authorised, collected alongside, since they hold much of the same data and can be reached independently (guides 147, 148): the estate worked with the device.
- **Honest reporting:** the feasibility, method and limits reported plainly under CPR Part 35 or CrimPR Part 19, so the court and the parties understand what an iOS acquisition did and did not obtain (guide 100): the truthful record.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: an iPhone is one node in a tightly integrated Apple estate, and much of what it holds also lives elsewhere, which matters especially because the device itself is so hard to open. The phone holds the local, encrypted data reachable only within the constraints above. But iCloud holds synced messages, photos, notes, files, health and backups; a computer used to sync the phone holds local iTunes or Finder backups (guide 147); the paired Mac and iPad (guides 131, 135) hold the same synced data through continuity; the counterpart devices of the people the user communicated with hold their side of the conversations; and the carriers and service providers hold their own records. The discipline is to map this estate so that a locked or difficult iPhone is not the end of the enquiry: the iCloud account, a computer backup and the paired devices frequently hold much of the same evidence, reached through the account or the other devices by lawful means. When the phone cannot be acquired, the backups and iCloud carry the record; when the device is wiped, a prior backup preserves a past state; and the account is the thread that ties the estate together, which is why the estate is preserved alongside the device from the outset.

EVIDENCE	THE IPHONE	ICLOUD	COMPUTER BACKUP (ITUNES/ FINDER)	PAIRED MAC / IPAD	COUNTERPART DEVICES	IF DEVICE LOCKED/ WIPED
Messages	Y: if accessible	Y: synced	Y: in backup	Y: same threads	Y: their side	Estate holds them
Photos / media	Y: if accessible	Y: iCloud Photos	Y: in backup	Y: same library	Shared media	iCloud / backup
Location / health	Y: if accessible	Often synced	Some in backup	Paired data	n/a	iCloud / backup
App data	Y: if accessible	Varies	Varies	Some synced	Provider records	Backup / provider
Accounts / keys	Keychain	iCloud Keychain	Backup keychain	Paired trust	n/a	iCloud / account

Fallback strategy in one line: preserve the estate alongside the device; when the iPhone is locked, difficult or wiped, iCloud, a computer backup and the paired devices hold much of the same evidence, reached lawfully.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE UNLOCKED PHONE THAT WAS ALLOWED TO LOCK

An iPhone central to a matter was seized while unlocked, but, treated casually, it was set down and allowed to lock before it reached an examiner, and its network was not isolated. The §4 and §5 consequences followed: once locked, and without the passcode, the device yielded far less than it would have unlocked, and the lost first moments could not be recovered, the possibility that existed at seizure was gone. Fortunately the §8 estate softened the blow, an iCloud account and a computer backup held much of the same data, but some device-only material was lost. The lesson is §5's: the moment of seizure is often decisive, an iPhone found unlocked must be kept unlocked, prevented from locking and isolated from the network, because letting it lock can irreversibly reduce what can ever be recovered, and no later effort can reopen the door that closed when it locked.

EXAMPLE 2 · THE HONEST ASSESSMENT THAT SET THE STRATEGY

Instructed on a locked iPhone of a particular model and iOS version, with no passcode available, the §6 honest assessment was given plainly: on this specific device, in this state, direct acquisition would yield little, and no promise to fully extract it would be made (guide 100). Rather than raise false hopes, the assessment shaped a sound strategy: the passcode was sought by §7 lawful means (guide 117), and, in parallel, the §8 iCloud estate and a computer backup were preserved and, with authority, collected, holding much of the relevant data. The matter advanced on what was genuinely achievable. The lesson is §6's: what an iPhone will yield is never assumed, it is assessed for the specific device, and an honest assessment, including that a locked device may yield little without the passcode, is not defeatism but the basis of a realistic strategy that turns to lawful access and the estate.

EXAMPLE 3 · THE PHONE WIPED REMOTELY BEFORE EXAMINATION

A seized iPhone was left powered and connected to a network while awaiting examination. Before it could be acquired, it was wiped remotely by someone with access to the account (guide 110), and its local data was gone. The §5 network-isolation failure had allowed the erasure. But the §8 estate again proved its worth: an iCloud backup and a computer backup, preserved earlier, held a prior state of the device, from which much of the evidence was recovered, and the remote wipe itself became a finding. The lesson is §5's and §8's: a seized phone must be isolated from the network at once to prevent remote wipe, because a device left connected can be erased before examination, and while the backups and iCloud estate frequently preserve the evidence even then, the network isolation that would have prevented the wipe is far preferable to relying on the fallback.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Letting an unlocked phone lock:** the classic, costly error, allowing a device found unlocked to lock before acquisition (Example 1, §5).
- **Not isolating from the network:** leaving the device connected and exposed to remote wipe (Example 3, §5).
- **Guessing the passcode:** risking a wipe by trying passcodes, when attempts are limited (§3).
- **Assuming any phone can be extracted:** promising full acquisition without assessing the specific device (Example 2, §6).
- **Ignoring the estate:** overlooking the iCloud and backup sources when the device is difficult (Examples 1 to 3, §8).
- **Delay:** not getting the device to an examiner while its state is favourable (§5).
- **Not securing the passcode lawfully:** failing to seek the passcode by cooperation or order, the single biggest access lever (§4, guide 117).
- **Treating iOS like a computer:** assuming plug-in-and-read, when iOS actively resists (§2).

Technical limitations

- **Locked, no passcode is severe:** a locked device without the passcode may yield little by direct means: the central limit (§4).
- **Capability varies by device:** model and iOS version determine what is possible, so no universal method exists (§4).
- **The encryption is not broken:** access is by authentication, not by defeating the cipher (§3, guide 133).
- **Mishandling is irreversible:** a lock or wipe cannot be undone, so seizure handling is decisive (§5).
- **iOS evolves rapidly:** Apple changes protections frequently, so feasibility is current-aware (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What is the device's model and iOS version, is it locked or unlocked, and is the passcode available, so feasibility can be assessed?
- How was the device handled at seizure, was it kept unlocked and network-isolated, or allowed to lock and stay connected?
- Are the iCloud account and any computer backups available as a fallback?

Ask your opponent

- Please preserve the device in its current state, keeping it unlocked if it is, isolating it from all networks to prevent remote wipe, and not attempting passcode guesses, and provide the passcode.
- Please preserve and disclose the associated iCloud account and any iTunes or Finder backups.
- Please confirm the device model, iOS version and lock state.

Ask your eDiscovery / forensic provider

- Given this device's model, iOS, lock state and passcode, what is realistically achievable?
- What must be done now to preserve the possibilities, and is remote wipe a risk?
- What do the backups and iCloud estate hold if the device yields little?

SUGGESTED WORDING · INSTRUCTION FOR AN IOS ACQUISITION ASSESSMENT

> "We instruct you to preserve and assess the acquisition of the Apple mobile device at Schedule 1. Please: (1) advise immediately on preservation, in particular keeping the device unlocked if found unlocked and preventing it from locking, isolating it from all mobile and Wi-Fi networks to prevent remote wipe or lock, not attempting to guess the passcode, and managing power, and arrange for it to reach an examiner promptly; (2) identify the device model, iOS version, lock state and passcode availability, and assess honestly what acquisition is feasible on this specific device in this state, making no blanket promise of full extraction; (3) advise on obtaining the passcode by cooperation or lawful compulsion, explaining that it is the central determinant of what can be acquired; (4) preserve and, where authorised, collect the associated iCloud account and any iTunes or Finder backups, which often hold much of the same data; and (5) report the feasibility, the method to be used and the honest limits, so expectations rest on the real device rather than a general assumption."

§ 12 · QUICK CONTROL

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

The iOS acquisition checklist

- ☐ Device kept unlocked if found unlocked; prevented from locking
- ☐ Isolated from all networks to prevent remote wipe
- ☐ No passcode guessing attempted
- ☐ Power managed to keep the most acquirable state
- ☐ Device brought to an examiner promptly
- ☐ Model, iOS version, lock state and passcode established
- ☐ Feasibility assessed for the specific device, not assumed
- ☐ Passcode sought by cooperation or lawful compulsion
- ☐ iCloud account and computer backups preserved as fallback
- ☐ Feasibility, method and honest limits reported

Red flags

- An unlocked phone allowed to lock before acquisition: Example 1.
- A seized device left connected to a network: Example 3.
- Passcode guessing attempted, risking a wipe.
- A promise to fully extract any phone, unassessed: Example 2.
- The iCloud and backup estate ignored.
- Delay while the device's state degrades.
- iOS treated as a plug-in-and-read computer.

When to involve a digital forensic expert

Immediately, ideally before the phone is even moved, because on iOS the first moments at seizure so often decide the outcome and cannot be redone: the expert advises at once on keeping an unlocked device unlocked, isolating it from the network to prevent remote wipe, not guessing the passcode, and getting it to acquisition promptly (Examples 1 and 3, §5); assesses honestly what the specific device, given its model, iOS, lock state and passcode, will realistically yield, making no blanket promise (Example 2, §6); advises on obtaining the passcode lawfully, the single biggest lever (§4, guide 117); and preserves and, where authorised, collects the iCloud and backup estate that so often holds the same data (§8). The feasibility, method and limits are reported plainly under CPR Part 35 or CrimPR Part 19. This guide opens the iPhone and iPad block; the acquisition methods, backups and app data that follow build on it. Through **cflab.uk** and **e-discovery.uk**, iOS work meets the paradox of the phone, richest in evidence, hardest to open, with the discipline it demands: preserve the possibilities at seizure, assess feasibility honestly, and use the estate, because on an iPhone, how it is handled first often decides what can ever be found.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can't you just plug the iPhone in and read it?

No, iOS actively resists that (§2, §3). The storage is fully encrypted and tied to the passcode and a security chip, the device limits passcode attempts, locks itself, and can be wiped remotely. So what can be obtained depends on the specific device, its model and iOS version, whether it is locked or unlocked, and whether the passcode is known, and treating an iPhone like an ordinary computer, plug in and read, is not only wrong but can destroy evidence, for instance by letting it lock or allowing a remote wipe.

What is the single most important thing at seizure?

Preserve the device's favourable state and isolate it from the network (§5). If the phone is found unlocked, keep it unlocked and stop it locking, because a locked device yields far less. Isolate it from all networks at once to prevent a remote wipe. Do not guess the passcode, since attempts are limited and may trigger a wipe. Then get it to an examiner quickly. These first moments are frequently decisive, and mishandling, a lock, a wipe, cannot be undone.

Why does the passcode matter so much?

Because it is the central determinant of access (§4, guide 117). With the passcode, the device can be unlocked and far more can be acquired; without it, a locked device may yield very little by direct means, since the encryption is bound to it. So obtaining the passcode lawfully, by the user's cooperation or by lawful compulsion where available, transforms what is possible. Where the passcode cannot be obtained, the strategy turns to the backups and iCloud estate, which often hold much of the same data.

Can every iPhone be extracted?

No, and a reputable expert will not claim so (§6, Example 2). Capability varies sharply by model and iOS version, and a locked device without the passcode may yield little. So feasibility is assessed for the specific device in its specific state rather than promised in general. This honesty is not defeatism: it directs the strategy to obtaining the passcode lawfully and to the iCloud and backup estate, so the matter proceeds on what is genuinely achievable rather than on a false assurance of full extraction.

If the phone can't be opened, is the evidence lost?

Often not (§8). An iPhone sits in a tightly integrated Apple estate: iCloud holds synced messages, photos, location, health and backups; a computer used to sync the phone holds local backups; and the paired Mac and iPad hold much of the same data. Reached through the account or the other devices by lawful means, these frequently hold the evidence the difficult phone will not give up. So a locked or wiped device is a serious setback but not usually the end, which is why the estate is preserved alongside the device from the start.

Someone might wipe the phone remotely. What do we do?

Isolate it from the network immediately (§5, Example 3). A device left connected to mobile or Wi-Fi networks can be erased remotely by anyone with account access before it is examined, so it is shielded from all networks at seizure using appropriate methods. If a remote wipe has already occurred, the iCloud and computer backups preserved earlier often still hold a prior state of the device, and the wipe itself may become a relevant finding, but prompt network isolation is far preferable to relying on that fallback.

§ 14 · REFERENCE

Glossary

Acquisition
Obtaining a forensic copy of a device's data.

Passcode
The user's device code, to which the encryption is tied.

Lock state
Whether the device is locked or unlocked.

Secure Enclave
The security chip protecting keys (see guide 133).

Auto-lock
The device locking itself after inactivity.

Attempt limit
The cap on passcode guesses before delay or wipe.

Remote wipe
Erasing the device remotely via the account.

Network isolation
Shielding the device from networks at seizure.

Feasibility
What can realistically be acquired from a device.

Estate
iCloud, backups and paired devices holding the data.

Sources and authoritative references

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

- cflab.uk, digital forensics services (iPhone and iPad acquisition, lock-state and passcode assessment, 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 (mobile-device preservation and acquisition 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
- Apple Platform Security guide (iOS data protection, the Secure Enclave, passcode protections and remote wipe): support.apple.com, Platform Security
- NPCC / police digital-forensics guidance on device seizure and network isolation, and ISO/IEC 27037 (identification, collection, acquisition and preservation of mobile devices): iso.org, 27037 · Forensic Science Regulator, Code of Practice v2: gov.uk, FSR Code
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

iOS work at the laboratory begins with the advice that most often decides the outcome, given the instant a relevant phone is found, because the first moments at seizure cannot be redone. An unlocked device is kept unlocked and prevented from locking; the phone is isolated from all networks at once to prevent a remote wipe; the passcode is never guessed, since attempts are limited and may trigger erasure; and the device is brought to acquisition promptly, in its most favourable state (Examples 1 and 3, §5). Feasibility is then assessed honestly for the specific device, given its model, iOS version, lock state and passcode, with no blanket promise that any iPhone can be fully extracted, because capability varies and a locked device without the passcode may yield little (Example 2, §6). The passcode is pursued lawfully as the single biggest lever (guide 117), the acquisition method is matched to the device (guide 146), and, decisively, the iCloud account and any computer backups are preserved and, with authority, collected alongside, since they so often hold much of the same data when the device is difficult or wiped (§8). The feasibility, method and honest limits are reported under CPR Part 35 or CrimPR Part 19. This guide opens the iPhone and iPad block that follows. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the first message about any iPhone is the urgent one: preserve its state now, because how it is handled first often decides what can ever be recovered.

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