COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

FileVault, the Secure Enclave and Apple Encryption

Why the Data Is Locked to the Machine and the Person, and Where the Recovery Keys Live

Apple encryption is the reason a modern Mac cannot be imaged the old way, and understanding it is essential to knowing what can and cannot be done with a seized machine. FileVault is Apple's full-disk encryption; the Secure Enclave is a dedicated security chip that holds and protects the keys and ties decryption to both the specific machine and successful authentication. Together they mean the data is not merely password-protected but cryptographically bound: readable only on that machine, only when unlocked by the right credential. For the lawyer, the practical questions are precise. Can the data be reached? Only with the credential, or a recovery key, on the machine. Where do recovery keys live? With the user, with an organisation that manages the device, or escrowed in the user's iCloud account, and the existence of an escrowed key is itself a finding. This guide explains for UK lawyers how Apple encryption works, why it binds the data to machine and person, what the honest limits are on a locked or powered-off device, and where the recovery keys that lawfully unlock it may be found.

⏱ Estimated reading time: 24 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. Understanding Apple encryption, FileVault, the Secure Enclave and how decryption binds to the machine and the credential, underpins all its Mac work: knowing what a locked or powered-off device will yield, where recovery keys are held, and how to reach the data lawfully. The work is conducted with honest limits stated plainly and reported under CPR Part 35 and CrimPR Part 19, so instructing lawyers know what is truly possible with an encrypted Apple device.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | FILEVAULT & SECURE ENCLAVE | RECOVERY-KEY ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: Apple encryption binds a device's data to both the specific machine and successful authentication, so the credential or a recovery key is the only route in, and the realistic questions are where the recovery keys live and how to obtain access lawfully, not how to break the encryption.

How it works (§3): FileVault encrypts the whole disk and the Secure Enclave, a dedicated security chip, holds the keys and handles authentication, so the encryption key is protected in hardware, not simply stored on disk. **Tied to authentication (§4):** decryption happens only on the specific machine and only when the correct credential is presented, so the data is bound to machine and person, not merely to a password on a file. **Recovery keys (§5):** a FileVault recovery key, or an institutional key on a managed device, or a key escrowed in the user's iCloud account, can unlock the data, and finding where a key lives is often the practical route in. **Honest limits (§6):** a locked, powered-off device without any credential or recovery key is, realistically, inaccessible by direct attack, and that limit is stated plainly. **Deployment (§7):** obtaining access through cooperation, orders and the escrowed recovery key, whose very existence in an account is itself a finding.

- **Bound to machine and person:** data decrypts only on the specific machine with the right credential.
- **The Secure Enclave holds the keys:** encryption keys are protected in hardware, not stored plainly on disk.
- **The credential is the way in:** access depends on the password or a recovery key, not on breaking the cipher.
- **Recovery keys live in three places:** with the user, with a managing organisation, or escrowed in iCloud.
- **State the limit honestly:** a locked, powered-off device with no key is realistically inaccessible.

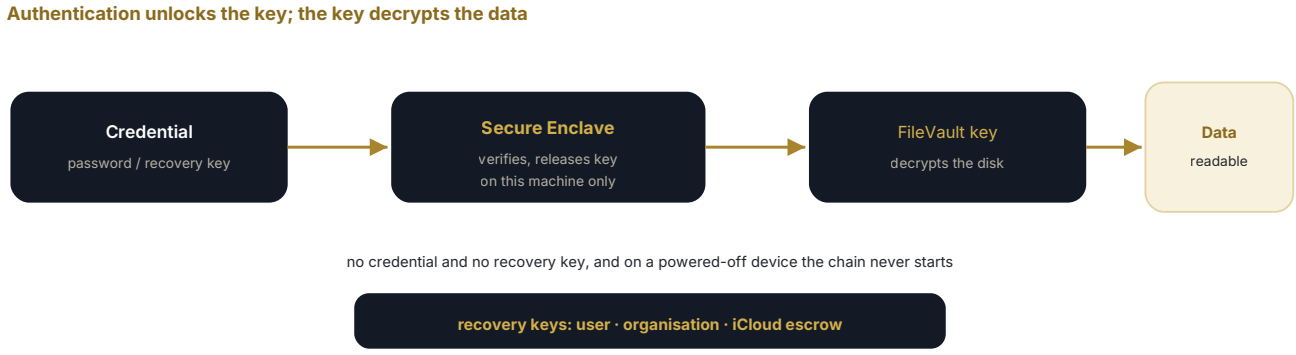

Figure 1 - the credential unlocks the Secure Enclave, which releases the FileVault key that decrypts the disk; without a credential or a recovery key from user, organisation or iCloud, the chain never starts.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: bound to machine and person

Encryption, at its simplest, scrambles data so that it is meaningless without a key. Older encryption was often something added on top of a device, a password protecting a file or a volume, and the weakness was frequently in how and where the key was kept. Apple encryption is different in a way that matters for evidence: it is built into the hardware and bound to the machine. FileVault encrypts the entire disk, and the key that decrypts it is not simply sitting on that disk waiting to be found; it is protected by the Secure Enclave, a dedicated security chip that holds keys, performs authentication, and will only release the decryption key on that specific machine and only when the correct credential, the user's password, and by extension their biometrics or a recovery key, is presented. The data is therefore bound to two things at once: the particular machine, and the person who can authenticate.

The consequence is that the usual forensic instinct, get the key, or attack the cipher, largely does not apply. The cipher is strong and the key is protected in hardware; there is no realistic prospect of breaking the encryption itself or extracting the key from the Secure Enclave by direct attack. What matters instead is authentication. If the device is running and unlocked, the data is decrypted and readable and can be acquired (guide 131). If it is locked or powered off, the data is inaccessible unless a credential or a recovery key can be presented on the machine. So the practical questions for a lawyer are not about cryptography but about access: is the machine unlocked; can the user's credential be obtained by cooperation or lawful compulsion; and, crucially, does a recovery key exist and where is it held, with the user, with an organisation that manages the device, or escrowed in the user's iCloud account. This guide explains how Apple encryption achieves this binding, why it makes authentication rather than cryptanalysis the issue, what the honest limits are, and where the recovery keys that lawfully open the device may be found.

§ 0 3 · HOW APPLE ENCRYPTION WORKS

How Apple encryption works: FileVault and the Secure Enclave

- **FileVault, full-disk encryption:** Apple's system that encrypts the entire startup disk, so all data at rest is scrambled and unreadable without the key, and on Apple Silicon the storage is hardware-encrypted regardless, with FileVault binding decryption to the user's credential (guide 131): the encryption that covers everything.
- **The Secure Enclave:** a dedicated, isolated security chip that generates, holds and protects the keys and performs authentication, so the decryption key never simply sits in accessible memory or on disk and cannot be extracted by direct attack: the hardware vault for the keys.
- **Keys wrapped, not stored plainly:** the disk-encryption key protected (wrapped) by keys the Secure Enclave controls and releases only on authentication, so possessing the disk does not yield the key: the reason imaging the storage alone is futile (guide 131 §4).
- **Bound to the machine:** the keys tied to that specific Secure Enclave, so the encrypted data cannot be moved to another machine and decrypted there, it is bound to the hardware it was created on (§4): the machine-binding.
- **Authentication paths:** the credential presented as a password, and by extension Touch ID or a recovery key, all resolving through the Secure Enclave to release the key, so authentication, not the cipher, is the gate (§4): the ways in, all through the same gate.

Figure 2 - the chain from FileVault's encrypted disk through the Secure-Enclave-protected key to authentication, which alone releases the key and yields decrypted data.

§ 0 4 · TIED TO AUTHENTICATION

Why decryption is tied to authentication

- **Authentication is the gate, not the cipher:** because the key is protected in hardware and released only on authentication, the way to the data is to authenticate, not to break the encryption, so effort goes to credentials and recovery keys, not cryptanalysis (§2): the reframing that governs strategy.
- **Unlocked equals readable:** once the correct credential is presented and the machine unlocked, the data is decrypted and can be acquired live (guide 131), which is why keeping a seized machine powered and unlocked is decisive (§6): the running-machine advantage.
- **Locked or off equals bound:** without authentication the key stays wrapped and the data stays scrambled, so a locked or powered-off device is, absent a credential or recovery key, closed (§6): the closed state.
- **Bound to the person via the credential:** because only the correct credential releases the key, access is, in effect, bound to whoever holds it, which is why lawful compulsion of the credential, or a recovery key, is the route (guide 117): the person-binding.
- **No moving the disk elsewhere:** the machine-binding means copying the encrypted storage to another system to decrypt it does not work, the keys are tied to the original Secure Enclave, defeating that classic workaround (§3): the workaround that fails.

§ 0 5 · RECOVERY KEYS

Recovery keys and where they live

- **The FileVault recovery key:** a key generated when FileVault is enabled that can unlock the disk in place of the password, so a party who has it, or has recorded it, holds a route in, and its whereabouts is a key question (§7): the alternative to the password.
- **With the user:** the recovery key may be held by the user, written down, saved, or stored, so it can be sought by disclosure or produced under an order, a lawful route that avoids any need to break anything (guide 117): the user's copy.
- **With an organisation:** on a managed or corporate device, an institutional recovery key or device-management system may hold the means to unlock it, so the employer or administrator can lawfully provide access (guides 111 to 114's admin-console theme): the organisation's key.
- **Escrowed in iCloud:** the user may have chosen to escrow the FileVault recovery key in their Apple account, so it can be recovered through the account by lawful process, and the very existence of an escrowed key is itself a finding worth establishing (§7): the escrowed copy.
- **Finding the key is the task:** the practical work being to locate a lawful key, user, organisation or escrow, rather than to attack the encryption, because a found recovery key opens the device cleanly and lawfully (§7): the real route in.

§ 0 6 · HONEST LIMITS

Honest limits on locked and powered-off devices

- **No credential, no key, no entry:** the central honest limit, that a locked or powered-off Apple device with no available credential and no recovery key is, realistically, inaccessible by direct attack, and a credible expert says so (guide 118): the limit stated without euphemism.
- **The encryption is not broken:** the practical route is always a lawful credential or recovery key, not cryptanalysis, so no reputable practitioner promises to break FileVault or extract the Enclave's keys (§4): the promise never made.
- **Powered-off is worse than locked:** a running-but-locked machine may retain more options than one fully powered off, which is why switching a seized device off is so damaging (guide 131 §7): the preservation consequence restated.
- **The estate as the realistic alternative:** where the device stays closed, the iCloud and paired-device estate frequently holds much of the same data and is reached through the account, so the enquiry is not necessarily over (§8): the way around the closed device.
- **Honesty protects the case:** stating the limit plainly, and pursuing cooperation, orders and recovery keys instead, is both more truthful and more effective than an overstated claim that collapses (guide 100): the honesty that serves the client.

§ 0 7 · DEPLOYMENT

Deployment: lawful access, orders and the escrowed key

- **Cooperation and orders for the credential:** the primary route, obtaining the password by cooperation in civil and internal work, or by an order compelling it where available, so the machine can be unlocked and acquired lawfully (guide 117): the front-door approach.
- **Disclosure of recovery keys:** the recovery key sought by disclosure from the user, or from the organisation managing a corporate device, so a lawful key opens the device without any attack on the encryption (§5): the key requested, not forced.
- **The escrowed key via the account:** where a recovery key is escrowed in the user's iCloud account, it is obtained through the proper account process, and its existence established as a finding, so the account becomes the route to the device (§5, §8): the escrow route.
- **Keeping the device open:** operationally, keeping a seized machine powered and unlocked so it need not be re-authenticated, coordinated with the preservation discipline of guide 131 (§6): access preserved.
- **Honest reporting of feasibility:** the feasibility of access, whether by unlocked state, credential or recovery key, reported plainly to instructing lawyers so decisions rest on what is truly possible, under CPR Part 35 or CrimPR Part 19 (guide 100): expectations set truthfully.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: encryption locks the device, but the data and the keys both live in more than one place across the Apple estate, which is exactly why a locked device is not always the end. The device holds the encrypted data, readable only when unlocked. But the FileVault recovery key may live with the user, with an organisation's device-management system, or escrowed in the user's iCloud account; and the data itself is frequently synced to iCloud and to paired iPhones and iPads, reachable through the account independently of the locked machine (guide 131). The discipline is to look for the key across its possible homes and for the data across the estate, so that a closed device is approached through a lawful recovery key or through the cloud copies rather than through a futile attack on the cipher. When the password is unavailable, an escrowed or institutional recovery key opens the device; when the device stays locked, the iCloud and paired-device data carry much of the same evidence; and the account is both a source of the key and a source of the data.

EVIDENCE	THE DEVICE	USER-HELD KEY	ORGANISATION KEY	ICLOUD ESCROW / DATA	PAIRED IPHONE / IPAD	RECOVERABLE ROUTE
Disk data	Y: if unlocked	Unlocks device	Unlocks managed device	Escrow unlocks; data synced	Same synced data	Via credential or key
Recovery key	n/a (protected)	Y: possible	Y: managed devices	Y: if escrowed	n/a	Disclosure / account
Files / messages	Encrypted at rest	n/a	n/a	Y: iCloud	Y: synced	Account / device
Account access records	Local logs	n/a	Admin logs	Y: account	Sign-in records	Account disclosure
Key existence (a finding)	Config state	Known to user	Known to admin	Y: escrow present	n/a	Established as fact

Fallback strategy in one line: seek the recovery key across user, organisation and iCloud escrow, and the data across iCloud and paired devices; a locked machine is opened by a lawful key or bypassed through the estate, never by breaking the cipher.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE ESCROWED KEY THAT OPENED THE DEVICE

A locked Apple Silicon Mac held key evidence, and the respondent would not provide the password. Rather than promise to break FileVault, which the §6 honest limit ruled out, the §5 recovery-key analysis asked where a key might live. The answer was in the §8 estate: the respondent had, at some point, escrowed the FileVault recovery key in his iCloud account. Its existence was established as a §7 finding, and the key was obtained through the proper account process under the relevant order (guide 117), unlocking the device lawfully and cleanly, with no attack on the encryption at all. What had looked like an impasse was resolved by finding the key the user had themselves stored in the cloud. The lesson is §5's: the route into an encrypted Apple device is a lawful credential or recovery key, and recovery keys live in identifiable places, with the user, an organisation, or escrowed in iCloud, so the practical task is to find the key, not to break the cipher.

EXAMPLE 2 · THE CORPORATE DEVICE THE EMPLOYER COULD OPEN

An employee under investigation used a company-managed MacBook and refused to cooperate. The §5 organisation route resolved it: because the device was enrolled in the employer's device-management system, an institutional FileVault recovery key was held centrally, and the employer, as owner and administrator, could lawfully provide it (consistent with the firm's policies and guides 111 to 114). The device was unlocked and acquired live (guide 131) without any need to compel the employee or attack the encryption. The §7 feasibility had been reported honestly at the outset: on a managed device, the organisation's key is the clean route in. The lesson is §5's: on corporate and managed Apple devices, the employer frequently holds an institutional recovery key or the management means to unlock the machine, so the organisation, not the individual, is often the lawful source of access, and establishing how a device is managed is an early and valuable question.

EXAMPLE 3 · THE HONEST LIMIT THAT SET THE STRATEGY

A powered-off, personal Apple device was recovered with no credential, no cooperation, and no recovery key anywhere to be found, not with the user, not escrowed, not institutional. The §6 honest limit was stated to the instructing lawyers without softening: this device, as it stood, could not be opened by direct means, and no reputable expert would claim otherwise (guide 118). That honesty shaped the strategy productively: effort turned to the §8 estate, the iCloud account and a paired iPhone that held much of the same synced data, and to an application for orders compelling any credential the user did in fact possess (guide 117). The case proceeded on what was truly achievable, rather than stalling on a false hope of cracking the device. The lesson is §6's: the honest limit is not a failure but the start of a sound strategy, saying plainly what cannot be done directs energy to the recovery keys, the estate and the lawful orders that actually deliver the evidence.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Believing the encryption can be broken:** the fundamental error, expecting cryptanalysis to open FileVault, when the route is a lawful credential or key (§4, §6).
- **Switching the device off:** powering down a locked machine and closing off options, the same costly reflex as in guide 131 (§6).
- **Not looking for recovery keys:** failing to ask where a recovery key lives, user, organisation, iCloud escrow, and missing the clean route in (Examples 1 and 2, §5).
- **Overlooking managed-device keys:** not establishing whether a corporate device has an institutional key the employer can provide (Example 2).
- **Trying to move the disk:** attempting to decrypt the storage on another machine, defeated by the machine-binding (§4).
- **Overpromising to the client:** claiming access to a locked, powered-off device with no key, then failing (§6).
- **Ignoring the estate:** the iCloud and paired-device data overlooked when the device is closed (Examples 1 and 3, §8).
- **Not establishing key existence:** failing to treat the presence of an escrowed key as a finding worth proving (§7).

Technical limitations

- **No realistic attack on the cipher:** FileVault and the Secure Enclave cannot be defeated by direct attack; access is via authentication: the core limit (§4, §6).
- **Locked or off is closed:** without a credential or key, a locked or powered-off device is inaccessible directly (§6).
- **Keys may simply not exist accessibly:** if no recovery key was recorded or escrowed, that route is absent (Example 3).
- **Machine-binding blocks transfer:** encrypted data cannot be decrypted off the original machine (§3, §4).
- **Apple security evolves:** encryption and Enclave behaviour change across models and OS, so feasibility is assessed per device (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the device unlocked, and are the user's credentials available by cooperation, so it can be acquired now?
- Is there a FileVault recovery key, and where might it live, with the user, an employer or device-management system, or escrowed in iCloud?
- Is the device personal or company-managed, since a managed device may have an institutional key the organisation can provide?

Ask your opponent

- Please provide the device password or FileVault recovery key necessary to access the device at Schedule 1, and preserve the device powered on and unlocked.
- Please confirm whether a FileVault recovery key exists and where it is held, including whether it is escrowed in an Apple account or held by an organisation.
- Please preserve and disclose the associated iCloud account and paired-device data.

Ask your eDiscovery / forensic provider

- Given this device's state, can it be accessed, and by what lawful route, credential or recovery key?
- Where might a recovery key live, and can its existence be established?
- If the device stays locked, what does the iCloud and paired-device estate hold?

SUGGESTED WORDING · INSTRUCTION FOR ENCRYPTED-DEVICE ACCESS

> "We instruct you to advise on and, where lawful, obtain access to the encrypted Apple device at Schedule 1. Please: (1) advise immediately on preservation, in particular keeping the device powered on and unlocked and not switching it off, and assess its current state (unlocked, locked, powered off); (2) identify the lawful routes to access, the user's credential by cooperation or order, and any FileVault recovery key, establishing where such a key may live (with the user, with an organisation managing the device, or escrowed in the user's Apple account) and treating the existence of an escrowed or institutional key as a finding; (3) obtain access by the appropriate lawful route and acquire the device live once unlocked (per our separate acquisition instruction); (4) state honestly the feasibility of access, and in particular that a locked or powered-off device with no available credential or recovery key is realistically inaccessible by direct means, making no claim to break the encryption; and (5) where the device remains closed, preserve and, where authorised, collect the associated iCloud and paired-device data, which often hold much of the same material. Report the routes attempted, the outcome and the honest limits."

§ 12 · QUICK CONTROL

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

The encrypted-device checklist

- ☐ Device state established (unlocked, locked, powered off)
- ☐ Device kept powered on and unlocked; not switched off
- ☐ User credential sought by cooperation or order
- ☐ Recovery key sought: user, organisation, iCloud escrow
- ☐ Management status established for corporate devices
- ☐ Existence of any escrowed or institutional key established as a finding
- ☐ Access obtained by a lawful route, not by attacking the cipher
- ☐ No promise made to break the encryption
- ☐ iCloud and paired-device estate preserved if device stays closed
- ☐ Feasibility and honest limits reported plainly

Red flags

- An expectation that FileVault can be broken by cryptanalysis: §6.
- A locked device switched off, closing off options: §6.
- No search made for where a recovery key lives: Examples 1 and 2.
- A managed device's institutional key not pursued: Example 2.
- An overstated promise to open a locked, powered-off device: Example 3.
- The iCloud and paired-device estate ignored.
- An escrowed key's existence not established as a finding.

When to involve a digital forensic expert

At the very start, because access to an encrypted Apple device is decided by early choices and lawful routes, not by later cleverness: the expert advises immediately on keeping the device powered and unlocked (guide 131), and assesses honestly what its state allows (§6); identifies the real way in, the credential by cooperation or order, and above all the FileVault recovery key, working out where it may live, with the user, an organisation, or escrowed in iCloud, and establishing its existence as a finding (Examples 1 and 2, §5); obtains access by that lawful route and acquires the device once open, without ever claiming to break the encryption (§7); and, where the device stays closed, turns to the iCloud and paired-device estate that so often holds the same data (Example 3, §8). Throughout, the feasibility is reported plainly under CPR Part 35 or CrimPR Part 19, so lawyers plan around what is truly possible. Through **cflab.uk** and **e-discovery.uk**, encrypted-device work replaces the false hope of cracking FileVault with the effective reality: find the lawful key, keep the machine open, and use the estate, and the encrypted device is far more often opened than the encryption's strength would suggest.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can you break FileVault or extract the key from the chip?

No, and a reputable expert will not claim to (§4, §6). FileVault's encryption is strong and the key is protected in hardware by the Secure Enclave, which cannot be defeated by direct attack or by extracting the key. The realistic route is never cryptanalysis but authentication: obtaining the user's credential by cooperation or order, or a lawful recovery key. Anyone promising to break the encryption should be treated with caution; the honest and effective approach is to find a lawful way to authenticate.

What is a FileVault recovery key, and why does it matter?

It is a key created when FileVault is enabled that can unlock the disk instead of the password (§5). It matters because it is a clean, lawful route into an encrypted device that avoids any need to break anything. The practical task is to find where it lives: the user may hold it, an organisation may hold an institutional one for a managed device, or it may be escrowed in the user's iCloud account. Locating a recovery key often opens a device that otherwise looked inaccessible.

Why can't you just copy the disk and decrypt it elsewhere?

Because the encryption is bound to the machine (§3, §4). The keys are tied to that specific Secure Enclave, so the encrypted storage cannot be moved to another computer and decrypted there, the classic imaging workaround does not work. Decryption happens only on the original machine, and only on authentication. This machine-binding is a core reason the old forensic methods fail on Apple devices and why access is about authenticating on the device itself, not about the disk.

The device is company-owned. Does that help?

Often significantly (§5, Example 2). A corporate or managed Apple device is frequently enrolled in a device-management system, and the organisation may hold an institutional FileVault recovery key or the means to unlock it. As owner and administrator, the employer can lawfully provide access, without compelling the individual or attacking the encryption. So establishing how a device is managed is an early and valuable question, the organisation is often the cleanest lawful source of access to a managed device.

If the device is locked and no key exists, is the data gone?

The device itself may be inaccessible, but the evidence often is not (§6, §8, Example 3). Honesty requires acknowledging that a locked or powered-off device with no credential or recovery key cannot be opened by direct means. But the data frequently lives elsewhere in the Apple estate: iCloud holds synced files, mail, messages and photos, and a paired iPhone or iPad holds much of the same, reachable through the account by lawful process. So a closed device redirects the enquiry to the estate rather than ending it.

Why does it matter that a recovery key is escrowed in iCloud?

For two reasons (§5, §7, Example 1). Practically, an escrowed key can be obtained through the proper account process and used to unlock the device lawfully, a clean route in. Evidentially, the very existence of an escrowed recovery key in an account is itself a finding: it establishes a lawful means of access and can be significant to how the matter proceeds. So establishing whether a key is escrowed, and obtaining it properly, is often the decisive step with an otherwise locked device.

§ 14 · REFERENCE

Glossary

FileVault
Apple's full-disk encryption for the startup disk.

Secure Enclave
A hardware security chip holding keys and doing authentication.

Full-disk encryption
Encrypting all data at rest on the disk.

Key wrapping
Protecting the disk key with keys the Enclave controls.

Authentication
Presenting the correct credential to release the key.

Recovery key
A key that unlocks FileVault in place of the password.

Institutional key
An organisation's recovery key for a managed device.

Escrow
Storing a recovery key in the user's Apple account.

Machine-binding
Keys tied to one Enclave, so data cannot decrypt elsewhere.

Powered-off state
The closed state where the key is wrapped and data locked.

Sources and authoritative references

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

- cflab.uk, digital forensics services (FileVault and Secure Enclave, recovery-key analysis, lawful encrypted-device 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 (access to encrypted devices 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 (FileVault, the Secure Enclave, key management, recovery keys and escrow): support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (honest reporting of feasibility and limits): gov.uk, FSR Code · guidance on compelled access and self-incrimination applies to obtaining credentials by order.
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35

DISCLAIMER

This publication provides general information about FileVault, the Secure Enclave and Apple encryption as at August 2026. Apple security architecture changes across models and operating-system versions, and the feasibility of access depends on the specific device, its state and the availability of a credential or recovery key; a locked or powered-off device without either may be inaccessible by direct means, and no reputable practitioner claims to break the encryption. 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

Encrypted-device work at the laboratory replaces a false hope with an effective method. The false hope is breaking FileVault: the encryption is strong, the key is protected in the Secure Enclave and bound to the machine, and no reputable practitioner claims to defeat it by direct attack, a limit stated plainly from the outset (§6, Example 3). The effective method is authentication and lawful keys. The device is kept powered and unlocked wherever possible so its data stays accessible (guide 131); the user's credential is pursued by cooperation or order (guide 117); and, decisively, the FileVault recovery key is sought where it actually lives, with the user, with an organisation managing a corporate device, or escrowed in the user's iCloud account, with the existence of such a key established as a finding in its own right (Examples 1 and 2, §5). Where the device stays closed, the enquiry turns to the iCloud and paired-device estate that so often holds the same data (§8). Feasibility is reported honestly under CPR Part 35 or CrimPR Part 19, so lawyers plan around what is real. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding truth is that the encrypted Apple device is far more often opened, lawfully, by finding the right key and keeping the machine open, than the strength of its encryption would ever suggest.

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