COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

macOS and Apple Silicon Forensics

The Mac That Cannot Be Imaged the Old Way: Encryption, Secure Boot and Live Acquisition

A modern Mac is not the computer a decade of forensic training assumed. On Apple Silicon machines, the ones with Apple's own M-series chips, the storage is soldered to the board and encrypted by hardware by default, the boot process is locked down, and the familiar move of pulling the disk and imaging it is simply impossible: there is no disk to pull, and what is on it is unreadable without the machine and its credentials. This does not mean a Mac cannot be examined; it means it must be examined differently, through live and logical acquisition on the running, unlocked machine, with the user's cooperation or lawful compulsion for the credentials, and with a clear understanding of what the hardware will and will not surrender. This guide opens the Apple block of the series and sets out for UK lawyers how modern Macs store and protect data, why the old imaging approach fails, how a Mac is actually acquired forensically today, and how the results, and the honest limits, are handled in evidence.

⏱ 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. Apple work is a core competence: forensic acquisition of Intel and Apple Silicon Macs, live and logical collection where imaging is impossible, and the handling of FileVault, the Secure Enclave and Apple's cloud, examined in this and the guides that follow. The work is conducted to preserve integrity on machines that cannot be imaged the old way, and reported under CPR Part 35 and CrimPR Part 19 with the method and the honest limits of each acquisition set out plainly.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | APPLE SILICON & INTEL MACS | LIVE & LOGICAL ACQUISITION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: a modern Apple Silicon Mac cannot be imaged the old way, its storage is soldered and hardware-encrypted and its boot is locked down, so it is acquired live and logically on the running, unlocked machine with the credentials obtained by cooperation or lawful compulsion, and what it yields, and does not, is stated honestly.

How it stores data (§3): Apple Silicon Macs have soldered storage encrypted by hardware through the Secure Enclave, a locked-down secure boot, and deep integration with the user's Apple account and iCloud. **Why old imaging fails (§4):** there is no removable disk, the storage is encrypted at rest and inaccessible without the machine and its keys, and secure boot prevents the traditional boot-from-external-media imaging, so pulling the disk yields nothing readable. **How it is acquired today (§5):** live and logical acquisition on the running, unlocked machine, capturing the decrypted file system, memory and artefacts, in a documented, integrity-preserving way. **Credentials and limits (§6):** access depends on the user's password or cooperation, or lawful compulsion, and a locked, powered-off Apple Silicon Mac is, without them, largely inaccessible, an honest limit. **Deployment (§7):** preservation and seizure that keep the machine live and unlocked, and the Apple cloud estate that often holds the same data.

- **No disk to pull:** Apple Silicon storage is soldered and hardware-encrypted; the old imaging move is impossible.
- **Secure boot locks it down:** booting from external media to image the drive no longer works.
- **Acquire live and unlocked:** the Mac is collected on the running machine with its credentials, not powered off.
- **Credentials are the key:** access depends on the password by cooperation or lawful compulsion.
- **The cloud holds much of it:** iCloud and the Apple account often carry the same data independently.

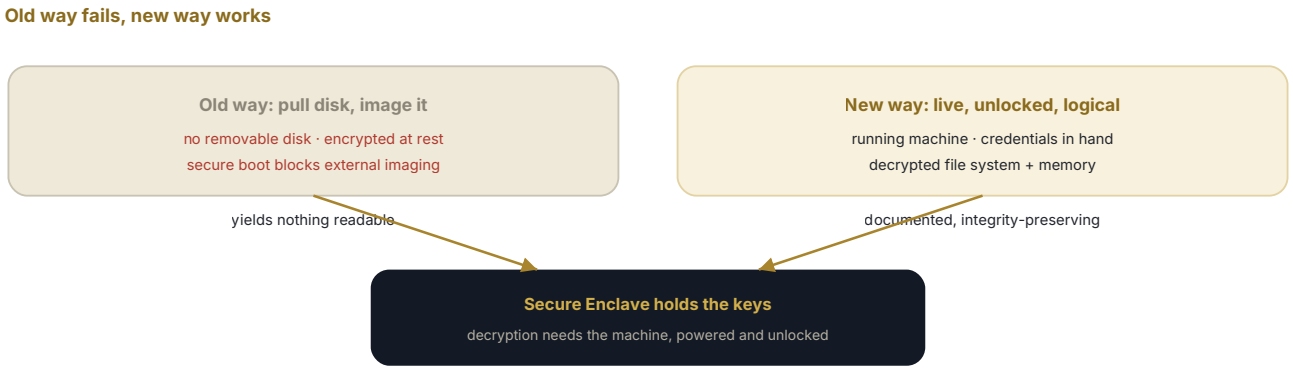

Figure 1 - on Apple Silicon the old pull-and-image method yields nothing; the data is reached only live, on the running, unlocked machine, because the Secure Enclave holds the keys.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: no disk to pull

For decades, computer forensics rested on a simple, reliable move: power the machine down, remove the hard drive, attach it to a write-blocker, and make a bit-for-bit image of it, so the original was never touched and the copy could be examined at leisure. That move defined the discipline. On a modern Apple Silicon Mac, it is impossible. There is no drive to remove: the storage is soldered directly to the logic board. Even if it could be removed, its contents are encrypted by the hardware and would read as meaningless noise without the machine and its keys. And the boot process is locked down by secure boot, so the old trick of starting the Mac from an external forensic drive to image the internal one no longer works. The three assumptions the classic method relied on, a removable disk, readable-at-rest data, and the ability to boot external media, are all gone.

The temptation, for anyone trained on the old method, is to conclude either that a Mac cannot be examined or that it can be examined the same way as always. Both are wrong. A Mac holds just as much evidence as any other computer, often more, given how tightly it integrates with the user's phone and cloud. But reaching that evidence requires a different approach, built around the reality that the data is only readable when the machine is running and unlocked. Acquisition happens live, on the powered-on, logged-in Mac, capturing the file system in its decrypted state along with memory and system artefacts, rather than from a dead disk. That in turn makes credentials, the user's password, or lawful means of compelling it, central, and makes how the machine is seized and preserved, kept powered and unlocked rather than switched off, a decisive early decision. This guide sets out how modern Macs work, why the old way fails, and how they are properly acquired today.

§ 0 3 · HOW IT STORES AND PROTECTS DATA

How modern Macs store and protect data

- **Soldered, integrated storage:** on Apple Silicon Macs the flash storage is part of the logic board, not a removable drive, so there is nothing to detach and image, and the storage cannot be read outside the machine (§4): the physical reality behind the method change.
- **Hardware encryption by default:** the storage is encrypted by the hardware, with keys managed by the Secure Enclave (covered in guide 133), so data is unreadable at rest without the machine and its credentials, whether or not the user enabled FileVault: the encryption that is always on.
- **The Secure Enclave:** a dedicated secure subsystem that holds keys and handles authentication, so decryption is tied to the specific machine and to successful authentication, not to the storage alone (guide 133): the keeper of the keys.
- **Secure boot:** a locked-down startup process that verifies the operating system and restricts booting from external or modified media, preventing the classic boot-and-image approach (§4): the locked front door.
- **Apple account and iCloud integration:** deep integration with the user's Apple account and iCloud, so much of the Mac's data is also synced to the cloud and shared with the user's other Apple devices (guide 133 and the iCloud guides), a second home for the same data (§8).

Figure 2 - the modern Mac's protective stack: soldered encrypted storage, keys in the Secure Enclave, a locked boot, and deep iCloud integration, each shaping how it must be acquired.

§ 0 4 · WHY OLD IMAGING FAILS

Why the old imaging approach fails

- **Nothing to remove:** the storage is soldered to the board, so the physical removal at the heart of classic imaging is simply not possible on Apple Silicon: the first assumption gone (§3).
- **Unreadable at rest:** even accessed in place, the storage is hardware-encrypted, so a raw image of it, if obtainable, is meaningless noise without the keys held in the Secure Enclave and unlocked by authentication: the second assumption gone (§3).
- **Secure boot blocks external imaging:** the locked-down boot prevents starting the Mac from an external forensic environment to image the internal storage, defeating the traditional workaround: the third assumption gone (§3).
- **Powered-off and locked is opaque:** a Mac that is switched off and locked presents, without credentials, an encrypted brick, which is why switching a seized Mac off can be the worst possible move (§7): the preservation consequence.
- **The method must change, not the goal:** the goal, a faithful, integrity-assured collection of the evidence, is unchanged; only the method must adapt to a machine whose data lives readable only while it runs unlocked (§5): the reframing.

§ 0 5 · HOW IT IS ACQUIRED TODAY

How a Mac is acquired today

- **Live acquisition on the running machine:** the Mac collected while powered on and unlocked, capturing the file system in its decrypted state, because that is the only state in which the data is readable (guide 99's live-acquisition discipline): the core of the modern approach.
- **Logical and targeted collection:** a logical image or targeted collection of the relevant data, user files, mail, messages, browser and application artefacts, system logs, taken from the live system in a documented, reproducible way (guide 71), rather than a physical image that the hardware will not yield.
- **Memory capture:** the machine's memory captured while it runs, preserving keys, running processes and volatile data that vanish at shutdown (guide 99), which on an encrypted machine can be especially valuable.
- **Integrity without a physical image:** integrity preserved and documented through hashing of the collected data and a recorded, reproducible method, so a logical acquisition is as accountable as a classic image even though the storage was never physically copied (guides 2, 3): the accountability maintained.
- **Consistency and validation:** the collection validated (does it mount, is it complete for the relevant scope) and the acquisition tool and steps documented, so the result can be explained and, where possible, reproduced (guide 71): the defensible live collection.

§ 0 6 · CREDENTIALS AND HONEST LIMITS

Credentials, cooperation and honest limits

- **Credentials are central:** because the data is readable only when the machine is unlocked, the user's password or account credentials are the key, obtained by cooperation in civil and consensual work or by lawful compulsion where available (guide 117's compelled-access discipline): the access question that governs everything.
- **Cooperation in civil work:** in most civil and internal matters the user cooperates or is ordered to provide access, so the machine can be acquired live and unlocked, the common and straightforward path (guide 117).
- **The locked, powered-off limit:** a switched-off, locked Apple Silicon Mac without credentials is, honestly, largely inaccessible by direct attack, so the realistic route is cooperation, compulsion or the cloud estate, not a promise of breaking the encryption (guide 118's honest-limit discipline): the limit stated plainly.
- **Keep it live and unlocked:** the practical corollary, that the single most important preservation step is to keep a seized Mac powered and unlocked, because switching it off surrenders access (§7): the decision that preserves the evidence.
- **The estate as the alternative:** where the Mac itself cannot be accessed, the iCloud and Apple-account estate often holds much of the same data, reached through the account by consent or lawful process (§8): the reach-around when the device is closed.

§ 0 7 · DEPLOYMENT

Deployment: preservation, seizure and the estate

- **Seize live, not dead:** the decisive operational point, that a Mac should be seized and kept powered on and unlocked wherever lawful and possible, because a running, unlocked machine is acquirable and a switched-off, locked one may not be (§6): the seizure decision that makes or breaks the acquisition.
- **Preserve promptly and correctly:** the machine preserved without shutting it down, letting it lock, or allowing remote wipe (guide 110's anti-forensic context), and acquired as soon as possible while access endures: the preservation discipline for encrypted machines.
- **Cooperation and orders early:** access, by cooperation or order, arranged early so the machine is acquired while unlocked, rather than discovering after shutdown that it is inaccessible (guide 117): access secured in time.
- **The cloud estate in parallel:** the iCloud and Apple-account data preserved and collected alongside the Mac, because it holds much of the same material and can be reached independently of the device (§8, and the iCloud guides): the estate worked with the device.
- **Honest scope in evidence:** the acquisition and its limits, what was collected live, what the hardware would not yield, presented plainly under CPR Part 35 or CrimPR Part 19, so the court understands the nature and completeness of a modern Mac collection (guide 100): the honest account of the method.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a Mac is one node in a tightly integrated Apple estate, and much of what it holds also lives elsewhere in that estate, which matters especially when the machine itself is locked. The Mac holds the local, decrypted-while-running data. But iCloud holds synced files, mail, messages, photos, notes and backups; the user's iPhone and iPad (later guides) hold the same messages, photos and app data through Apple's continuity and sync; Time Machine and other backups hold prior states of the Mac; and the Apple account holds the account-level records and the keys to much of the cloud. The discipline is to map this estate so that a Mac which cannot be accessed directly is not the end of the enquiry: the iCloud account, the paired iPhone and the backups frequently hold the same evidence, reached through the account or the other devices. When a Mac is switched off and locked beyond direct access, the cloud and the paired devices carry the record; when the local data is unavailable, a Time Machine backup holds a prior state; and the account is the thread that ties the whole Apple estate together.

EVIDENCE	THE MAC (LIVE)	ICLOUD	PAIRED IPHONE / IPAD	TIME MACHINE / BACKUPS	APPLE ACCOUNT	DELETED / RECOVERABLE
Files / documents	Y: decrypted live	Y: iCloud Drive	Shared files	Y: prior versions	Account storage	Varies (guide 132)
Mail / messages	Y: local stores	Y: synced	Y: same threads	Backup copies	Account mail	Varies
Photos	Y: library	Y: iCloud Photos	Y: same library	Backup copies	Account	Recently deleted
System activity	Y: unified logs	Limited	Device analytics	Backup snapshots	Account sign-ins	Log rotation (guide 134)
Keys / access	Secure Enclave	Keychain in iCloud	Paired trust	n/a	Y: recovery	n/a

Fallback strategy in one line: keep the Mac live and unlocked to acquire it directly; and where it is locked beyond reach, the iCloud account, the paired iPhone and the backups hold much of the same evidence.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE MAC SWITCHED OFF, AND THE LESSON LEARNED

An Apple Silicon MacBook central to an investigation was seized and, by reflex from the old training, switched off for transport. When it reached the laboratory the §4 and §6 reality bit: powered off and locked, with no credentials, its soldered, hardware-encrypted storage was inaccessible by direct means, there was no disk to pull and no way to boot around the secure boot. Fortunately the §8 estate rescued the position: the user's iCloud account, accessed through lawful process, held synced copies of much of the relevant material, and a paired iPhone held the same messages and photos. But the Mac's local-only artefacts, some system logs and unsynced data, were lost to the shutdown. The lesson is §7's: an Apple Silicon Mac must be kept powered on and unlocked wherever lawful, because switching it off can turn an acquirable machine into an encrypted brick, and while the cloud estate often saves the day, the local-only evidence may not survive the mistake.

EXAMPLE 2 · THE LIVE ACQUISITION DONE RIGHT

In an internal investigation, an employee's Apple Silicon Mac was to be examined. Rather than attempt the impossible physical image, the §5 modern approach was used: with the employee's cooperation (and consistent with the firm's policies and guide 117), the machine was acquired live and unlocked, a logical collection of the relevant user files, mail, messages, browser and application artefacts and system logs, together with a memory capture, all hashed and the method documented. The §5 integrity discipline meant the logical acquisition was as accountable as a classic image would have been: reproducible, validated and explainable. No attempt was made to defeat the encryption, because none was needed, the machine was unlocked. The collection was complete for its scope and sound. The lesson is §5's: a modern Mac is acquired live and logically on the running, unlocked machine, and done with proper hashing, documentation and validation, that collection is fully defensible, the change is in the method, not in the rigour.

EXAMPLE 3 · THE HONEST LIMIT AND THE ESTATE THAT ANSWERED

A respondent in a civil matter declined to provide his Mac password, and no order compelling it was yet in place. The §6 honest limit was stated plainly to the instructing solicitors: a locked Apple Silicon Mac, without the credentials, could not simply be broken into, and no promise to the contrary would be made (guide 118). But the §8 estate offered a lawful route: the respondent's iCloud data, obtainable through the proper process, and a Time Machine backup found on an external drive that was not itself encrypted, together held much of the relevant material, and an application for an order compelling the password was advised for the remainder (guide 117). The case advanced without an overstated claim about cracking the Mac. The lesson is §6's: honesty about the limit is not defeat, a locked modern Mac may resist direct access, but the cloud estate, backups and lawful compulsion frequently deliver the evidence, and the credible expert says what can and cannot be done.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Switching the Mac off:** the classic and costly error, powering down a seized Apple Silicon Mac and turning it into a locked, encrypted brick (Example 1, §7).
- **Attempting a physical image:** trying to pull and image a soldered, encrypted disk that cannot be removed or read that way (§4).
- **Trying to boot external media:** attempting the old boot-and-image workaround that secure boot now blocks (§4).
- **Not securing credentials early:** failing to arrange cooperation or an order while the machine is still unlocked (Example 3, §6).
- **Promising to crack it:** overstating the ability to break into a locked, powered-off Mac (§6).
- **Ignoring the estate:** the iCloud, paired-device and backup sources overlooked when the Mac is inaccessible (Examples 1 and 3, §8).
- **Treating a logical acquisition as second-rate:** assuming a live logical collection is less defensible, when done properly it is fully accountable (Example 2, §5).
- **Allowing remote wipe:** the machine left network-connected and open to remote erasure before acquisition (§7, guide 110).

Technical limitations

- **Powered-off and locked is opaque:** without credentials, a switched-off Apple Silicon Mac is largely inaccessible by direct means: the central honest limit (§6).
- **No physical image is available:** soldered, encrypted storage cannot be imaged the classic way; acquisition is live and logical (§4, §5).
- **Access depends on credentials:** the data is readable only unlocked, so cooperation or compulsion is required (§6).
- **Local-only data is fragile:** unsynced, local-only artefacts can be lost if the machine is shut down before acquisition (Example 1).
- **Apple technology evolves:** hardware, encryption and boot protections change across models and OS versions, so the approach is checked per machine (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the Mac Apple Silicon or Intel, and is it currently powered on and unlocked, so we know how it must be acquired and how urgent access is?
- Are the user's credentials available by cooperation, and is the iCloud account and any backup accessible?
- Has the machine been kept powered on, or was it switched off, and is it still network-connected and open to remote wipe?

Ask your opponent

- Please preserve the Mac without switching it off, letting it lock or permitting remote erasure, and provide the credentials or access necessary for live acquisition.
- Please preserve and disclose the associated iCloud account data, paired-device data and any Time Machine or other backups.
- Please confirm the model, operating system and whether the machine has been powered down since the relevant date.

Ask your eDiscovery / forensic provider

- Can this Mac be acquired given its state (powered, unlocked, credentials), and what will it yield?
- What must be done now to preserve access, and is remote wipe a risk?
- What does the iCloud and backup estate hold if the Mac itself is inaccessible?

SUGGESTED WORDING · INSTRUCTION FOR A MAC ACQUISITION

> "We instruct you to preserve and acquire the Apple Mac at Schedule 1. Please: (1) advise immediately on preservation, in particular that the machine be kept powered on and unlocked and prevented from locking, shutting down or being remotely erased, and identify the model and operating system; (2) acquire the machine live on the running, unlocked system, taking a logical or targeted collection of the relevant data (user files, mail, messages, browser and application artefacts, and system logs) together with a memory capture, preserving integrity by hashing and documenting a reproducible method, since a physical image of the soldered, hardware-encrypted storage is not obtainable; (3) advise on the credentials required and the route to them (cooperation or an order), and state honestly that a switched-off, locked Apple Silicon machine may be inaccessible by direct means without them; (4) preserve and, where authorised, collect the associated iCloud account, paired-device and backup data, which often hold much of the same material; and (5) report the acquisition method and its honest limits, distinguishing what was collected from what the hardware would not yield."

§ 12 · QUICK CONTROL

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

The Mac acquisition checklist

- ☐ Model and OS identified; Apple Silicon or Intel established
- ☐ Machine kept powered on and unlocked; not switched off
- ☐ Remote wipe prevented; network isolated as appropriate
- ☐ Credentials arranged by cooperation or order, early
- ☐ Live logical or targeted acquisition performed on the running machine
- ☐ Memory captured while the machine runs
- ☐ Integrity hashed and method documented and reproducible
- ☐ Collection validated and complete for scope
- ☐ iCloud, paired-device and backup estate preserved in parallel
- ☐ Method and honest limits reported plainly

Red flags

- A seized Apple Silicon Mac switched off before acquisition: Example 1.
- An attempt to pull and image a soldered, encrypted disk: §4.
- A promise to crack a locked, powered-off Mac: §6.
- Credentials not secured while the machine is still unlocked: Example 3.
- The iCloud and backup estate ignored when the Mac is inaccessible.
- A live logical acquisition dismissed as second-rate.
- The machine left open to remote erasure.

When to involve a digital forensic expert

Before the Mac is touched, and certainly before it is switched off, because the single most damaging error, powering down an Apple Silicon machine, happens in the first minutes and cannot be undone (Example 1, §7): the expert advises immediately on keeping it live, unlocked and safe from remote wipe, and on securing credentials while access endures (§6); performs the acquisition the modern way, live and logical on the running machine with memory capture, hashed and documented, so the collection is fully defensible despite the absence of a physical image (Example 2, §5); states honestly what a locked, powered-off machine will and will not yield, without overpromising (Example 3, §6); and preserves and collects the iCloud and backup estate that so often holds the same data (§8). Reports run under CPR Part 35 or CrimPR Part 19. This guide opens the Apple block; the encryption, file system and artefacts that follow build on it. Through **cflab.uk** and **e-discovery.uk**, Mac work meets the reality that the old imaging method is dead: the goal of a faithful, integrity-assured collection is unchanged, but on a modern Mac it is reached live, unlocked and honestly bounded.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can you just image the Mac's hard drive like any other computer?

Not on Apple Silicon (§4). The storage is soldered to the board, so there is nothing to remove; it is hardware-encrypted, so it is unreadable at rest without the machine and its keys; and secure boot blocks the old trick of imaging it from external media. The classic pull-and-image method simply does not work. The Mac is instead acquired live and logically, on the running, unlocked machine, which is where its data is readable (§5).

What is the single most important thing when seizing a Mac?

Keep it powered on and unlocked (§7, Example 1). A running, unlocked Apple Silicon Mac can be acquired; a switched-off, locked one may be an encrypted brick without the credentials. The reflex from old training, to power a machine down, is exactly wrong here. So the machine is kept awake and unlocked, prevented from locking or sleeping into a locked state, protected from remote wipe, and acquired as soon as possible while access lasts.

Is a live logical acquisition as good as a full image?

For a modern Mac it is the correct and defensible method, not a compromise (§5, Example 2). Because no physical image is obtainable, the live logical or targeted collection, taken from the unlocked machine, hashed, documented and validated, is the sound approach, and done properly it is as accountable and reproducible as a classic image. The rigour, integrity, documentation, validation, is unchanged; only the technique adapts to a machine whose data is readable only while it runs.

The Mac is locked and we do not have the password. Can you break in?

Honestly, usually not by direct attack on a powered-off Apple Silicon machine (§6, Example 3). The credible answer is not a promise to crack it but the lawful alternatives: obtain the password by cooperation or an order (guide 117), and reach the same data through the iCloud account and any backups, which often hold much of it (§8). A reputable expert states this limit plainly rather than overpromising, and pursues the routes that actually work.

If we cannot access the Mac, is the evidence lost?

Often not (§8, Examples 1 and 3). A Mac sits in a tightly integrated Apple estate: iCloud holds synced files, mail, messages and photos; the paired iPhone or iPad holds the same messages and libraries; and Time Machine or other backups hold prior states. Reached through the account or the other devices by consent or lawful process, these frequently hold much of the same evidence. The Mac being inaccessible is a setback, not usually the end of the enquiry.

Does this apply to older Intel Macs too?

Partly (§3). Older Intel Macs may have removable storage and different boot behaviour, so some classic techniques can still apply, though FileVault encryption and the T-series security chips on later Intel models bring similar constraints. Apple Silicon machines are the fullest expression of the new reality, soldered, hardware-encrypted, secure-booted, but the direction of travel is the same, and every Mac is assessed on its specific model, chip and configuration.

§ 14 · REFERENCE

Glossary

Apple Silicon
Apple's own M-series Mac chips, with integrated secure storage.

Soldered storage
Flash storage fixed to the board; not removable.

Hardware encryption
Storage encrypted by the hardware, on by default.

Secure Enclave
A secure subsystem holding keys and handling authentication.

Secure boot
A locked startup that blocks external or modified boot media.

Live acquisition
Collecting data from a running, unlocked machine.

Logical acquisition
A file-level collection rather than a physical image.

Memory capture
Preserving volatile RAM contents while the machine runs.

Time Machine
Apple's backup system holding prior states of the Mac.

iCloud
Apple's cloud, holding synced copies of much Mac data.

Sources and authoritative references

The Apple 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 (Apple Silicon and Intel Mac acquisition, live and logical collection, 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 (live acquisition of encrypted machines 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 (Secure Enclave, secure boot, storage encryption and data protection on Apple Silicon): support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (integrity and method in live acquisition): gov.uk, FSR Code · ISO/IEC 27037 (identification, collection, acquisition and preservation, including live systems): iso.org, 27037
- 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 macOS and Apple Silicon forensics as at August 2026. Apple hardware, security architecture and operating systems change frequently, and the feasibility and method of any acquisition depend on the specific model, chip, OS version and machine state; a locked, powered-off machine may be inaccessible without credentials. 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

Mac work at the laboratory starts with the advice that most often decides the outcome, given before the machine is touched: keep it powered on and unlocked, prevent it from locking or being remotely wiped, and secure the credentials while access lasts, because a switched-off Apple Silicon Mac can become an encrypted brick (Example 1, §7). Acquisition is then performed the modern way, live and logically on the running, unlocked machine, a targeted collection of the relevant user and system data with a memory capture, hashed and documented so it is as accountable and reproducible as any classic image, because no physical image of the soldered, hardware-encrypted storage is obtainable (Example 2, §5). Where the machine is locked and credentials are withheld, the honest limit is stated plainly rather than overpromised, and the lawful routes are pursued: cooperation or an order for the password (guide 117), and the iCloud, paired-device and backup estate that so often holds the same evidence (Example 3, §8). The acquisition and its limits are reported clearly under CPR Part 35 or CrimPR Part 19. This guide opens the Apple block, and the encryption, file-system and artefact guides that follow build on it. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the first message about any modern Mac is the urgent one: do not switch it off.

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