COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Mac Evidence in Litigation

APFS, FileVault, Time Machine, iCloud and the Artefacts of macOS

Macs are everywhere the disputes are: design studios, agencies, executive suites, founder laptops. They are examined less often than Windows machines, and misexamined more often, because their architecture differs at every layer: the APFS file system with its snapshots and clones, FileVault encryption on by default, Apple Silicon hardware that changes how acquisition works, Time Machine's versioned history, and iCloud woven through the user's files, messages and photographs. This guide explains what a Mac records, how examiners acquire and read it, where the Windows instincts mislead, and how Mac evidence wins and loses cases in practice.

⏱ Estimated reading time: 27 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, examining Windows, macOS, mobile and cloud sources under one methodology. Mac examinations run weekly through the laboratory: founder and executive devices, creative-industry disputes, exfiltration and forgery questions, reported under CPR Part 35 and CrimPR Part 19. Its eDiscovery arm, **e-discovery.uk**, integrates Mac-derived evidence into disclosure-scale review.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | MACOS & APPLE SILICON ACQUISITION | DELETED DATA RECOVERY | CPR PART 35 EXPERT REPORTS | COURT-EXPERIENCED EXPERT WITNESSES

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: RICH EVIDENCE, DIFFERENT RULES

A Mac records its user's life as thoroughly as any Windows machine: files opened, applications run, devices connected, networks joined, websites visited, messages synchronised: but through its own architecture, and that architecture changes the practicalities at every step. **Acquisition first:** FileVault full-disk encryption is on by default and Apple Silicon binds storage to the specific machine, so the credential and recovery-key work of this series' encryption guide is not an edge case on Macs; it is the front door, and imaging without the password or recovery key yields ciphertext. **Deletion second:** the APFS file system snapshots itself and shares storage between cloned files, so deleted material often survives in local snapshots and version histories even as classic unallocated-space carving gives little on Apple's SSDs: recovery routes shift from carving to snapshots, Time Machine and iCloud. **Artefacts third:** macOS keeps its own families: Spotlight metadata, FSEvents (a rolling journal of file-system changes), quarantine records for downloads, KnowledgeC/Biome pattern-of-life databases, unified logs, recent-items and connection records: unfamiliar names doing familiar evidential work. **And the cloud throughout:** iCloud Drive, Desktop and Documents sync, Messages, Photos and device backups mean the Mac's story is routinely half local, half server-side, and complete answers collect both. The strategic point for lawyers is simple: instruct examiners who work in this architecture natively: Windows habits applied to a Mac miss evidence that exists and claim evidence that does not.

- **Credentials before everything:** the user password or FileVault recovery key (personal, corporate MDM escrow, or iCloud-stored) determines whether there is an examination at all; secure them at preservation, per guide 33's disciplines.
- **Local snapshots are the quiet archive:** APFS snapshots (taken automatically around updates and by Time Machine's local machinery) preserve point-in-time volume states, and with them files deleted since: the first place a Mac examiner looks for the recently destroyed.
- **FSEvents remembers operations:** a rolling record of created, modified, renamed and deleted paths, persisting after the files themselves are gone: the Mac's answer to "what happened in that folder that week".
- **Attribution has the same layers as ever:** accounts, sessions, fast user switching and shared studio machines: the account-versus-human discipline of the Windows guide applies unaltered.
- **USB and external media are recorded here too:** mounted-volume artefacts, recent-items volume references and log entries do the data-theft work, with per-artefact semantics an examiner states honestly.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the Mac is not a Windows machine in nicer clothes

The commonest Mac-evidence failure in litigation is imported instinct. A party's IT team, or a generalist provider, treats the founder's MacBook like an office Dell: pull the drive, image it, carve the unallocated space, quote the registry. Each step misfires: the drive is soldered and encrypted, so pulling it yields nothing; the "image" without credentials is ciphertext; there is no registry; and carving Apple's encrypted SSD storage returns fragments of nothing. The report that follows either overclaims ("no deleted files were recoverable, therefore none existed") or underdelivers, and the other side's Mac-literate expert dismantles it by pointing at the snapshot, the FSEvents journal and the iCloud version history the examination never opened.

Run natively, the same machine is generous. macOS is, if anything, a more compulsive note-taker than Windows: its pattern-of-life databases log application usage in sessions, its file-system journal records operations by path, its download quarantine remembers where files came from, and its cloud entanglement means many "deleted" items persist server-side with version trails. The evidence is there; it is simply filed under different names, behind a locked front door whose key must be obtained first. This guide is the map: enough architecture for a lawyer to instruct intelligently, scope realistically and cross-examine the other side's Mac claims with confidence.

§ 0 3 · THE FRONT DOOR

Acquisition: FileVault, Apple Silicon and getting the data at all

- **FileVault is the default state:** modern Macs encrypt the system volume as standard; without the user password, a FileVault recovery key, or (on managed fleets) the MDM-escrowed institutional key, the disk's contents are unreadable. The preservation moment is therefore also the credential moment: obtain and verify keys while goodwill and memory exist, per guide 33.
- **Apple Silicon changes the mechanics:** on M-series machines storage is integral and cryptographically tied to the hardware, so acquisition proceeds through the machine itself: booted acquisition modes, target-disk-style transfers over cable, or agent-based logical collection: producing decrypted logical images when credentials are supplied. The classic remove-and-write-block ritual belongs to older hardware; the modern method is different and, properly logged and hashed, no less defensible.
- **Full versus logical, honestly framed:** what is captured is typically the decrypted logical file system (files, metadata, snapshots, system databases): which is where essentially all macOS evidence lives: rather than raw sectors of an encrypted SSD whose "unallocated space" is cryptographic noise by design. The method record states what was taken and why it is complete for the questions asked.
- **Live opportunities matter more, not less:** a powered-on, logged-in Mac is unlocked evidence: the guide 33 calculus (photograph state, assess, acquire while access exists, capture volatile data) applies with force, because power-off on a credential-less Mac may close the estate permanently.
- **MDM fleets are the corporate blessing:** managed Macs escrow FileVault keys and support remote lock and inventory; establishing MDM status early converts many locked-device problems into administrative retrievals: a first-day question for client IT.

§ 0 4 · DELETION, REWRITTEN

APFS: snapshots, clones and what deletion means now

- **Snapshots preserve the past wholesale:** APFS can freeze a volume's entire state instantly; macOS does so automatically around system updates and via Time Machine's local snapshot machinery (typically hourly while a backup drive is unavailable, retained on a rolling basis and pruned under storage pressure). A file deleted on Tuesday commonly persists, intact with metadata, in Monday's snapshot: mounted and examined like any volume.
- **Clones complicate copies:** APFS clones share storage between a file and its duplicates until one changes, which affects how examiners interpret timestamps, sizes and "copies" of documents: a semantics layer the report must handle correctly in forgery and backdating disputes.
- **Carving gives way to structure:** with encrypted SSD storage, traditional unallocated-space carving yields little; deleted-data recovery on Macs is structural: snapshots first, then Time Machine's history (§6), then application-level versions (macOS's document versioning keeps per-file edit histories for many apps), then iCloud's server-side copies and versions (§7). The recovery conversation with the examiner is about which of these doors this machine and this timing leave open.
- **The metadata layer persists regardless:** FSEvents records (created, renamed, deleted paths with approximate times), Spotlight database remnants and application records prove that named files existed and what happened to them: so, as on Windows, mass deletion is provable as an event even where content is gone, with all the adverse-inference consequences this series' examples keep illustrating.
- **Timing rules recovery:** snapshots rotate and prune; the difference between instructing this week and next month is often the difference between mounting Monday's volume and reading about it in FSEvents. Preserve fast, image fast.

§ 0 5 · THE ARTEFACT MAP

The macOS artefact map: what the system records

QUESTION	PRINCIPAL MACOS ARTEFACTS
What files were opened?	Recent items and per-application recents; document-interaction records in the pattern-of-life databases (KnowledgeC/Biome); Spotlight metadata including use dates; application state and saved sessions
What happened in the file system?	FSEvents journal: creations, modifications, renames and deletions by path over a rolling window; APFS metadata; document versions database
What programs ran, when?	KnowledgeC/Biome application-usage sessions (start, end, focus); launch services and login items; unified logs; crash and diagnostic reports
Who logged in, when, how?	Unified log authentication events; login window records; fast-user-switching traces; screen lock/unlock events; remote access (SSH, screen sharing) log entries
What devices and volumes connected?	Mounted-volume records and mount-point artefacts; recent items referencing external volume names; unified log USB and disk-arbitration entries; Time Machine records of participating drives
What networks and locations?	Known Wi-Fi networks with connection history; network configuration records; captive-portal and hotspot traces; per-app network usage in usage databases
Where did files come from?	Quarantine database: per-download origin URL, timestamp and downloading application, persisting after the file's deletion: the provenance artefact of malware, leak and IP cases
What was browsed and searched?	Safari history, downloads and cache (plus Chrome/Firefox as on Windows); Spotlight search history; Siri and suggestion caches
What was said and shared?	Messages database (iMessage/SMS synced from the phone), Mail stores, FaceTime call records, AirDrop transfer traces in unified logs, Continuity/Handoff artefacts

Two families deserve emphasis. The **pattern-of-life databases** (KnowledgeC and its Biome successors) log application usage as timed sessions, device lock state, and interaction events: on contested-hours questions ("was anyone using this machine at 02:00?") they are frequently decisive. The **quarantine database** answers provenance: every browser and AirDrop download's source URL and moment, surviving the file's deletion: in exfiltration reversed (what arrived) and IP contamination cases, it is the artefact the matter turns on.

§ 0 6 · THE VERSIONED PAST

Time Machine: the versioned past

- **What it holds:** a Time Machine backup drive contains periodic snapshots of the user's world going back months or years: hourly for the last day, daily for the last month, weekly beyond: each browsable as the volume stood at that moment. For litigation this is a documentary time series: the contract folder as it was before the dispute; the design files' evolution; the week the "long-standing" document first appeared.
- **Deleted and edited material persists:** files removed from the Mac remain in every backup taken while they existed; documents edited retain their earlier states in earlier backups: the natural home of forgery, backdating and destruction questions.
- **Backups are exhibits:** the drive (or network backup store) is preserved, imaged and examined under the same custody as the Mac; its own records (backup times, participating machine, interruptions) are evidence about the user's habits and about gaps: the backup that stopped the week the trouble started is a finding in itself.
- **Ask for it by name:** preservation notices and disclosure requests that say "the computer" collect one point in time; adding "and any Time Machine or other backup drives, network backup locations and their contents" collects the time series: the single highest-yield sentence in Mac-related correspondence.

§ 0 7 · THE OTHER HALF

iCloud: the half of the Mac that lives elsewhere

- **Sync is the default posture:** iCloud Drive with Desktop and Documents sync means many users' working folders exist as a mirrored pair (local and server); Messages, Photos, Notes, Contacts, Calendars, Safari data and passwords sync likewise; and iPhone backups may sit in the same account: the Mac examination that ignores iCloud examines half a user.
- **Two evidential gifts:** server-side persistence (files deleted locally often persist in iCloud's recently-deleted areas and version histories, on iCloud's own timetable) and cross-device reach (the phone's messages readable via the Mac's synced database; the tablet's files in the same drive).
- **Two complications:** access and law. Access: iCloud collection requires the account credentials and second factor (or Apple's lawful-process routes in criminal contexts), and "optimised storage" means some local files are placeholders whose substance is server-side only: collection must fetch, not just copy stubs. Law: the account is the individual's; corporate authority over a personal iCloud is not assumed, and the consent/compulsion framework of this series' personal-accounts and BYOD guides applies.
- **Collect both halves deliberately:** the protocol names the Mac, its snapshots and backups, and the iCloud account's relevant services, with the legal basis per source: the pairing that turns "his laptop" into the user's actual documentary estate.

§ 0 8 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DESIGN FILES AND THE LOCAL SNAPSHOT

A departing creative director wiped his project folders the night before returning his MacBook, confident that emptied trash meant gone. The laboratory's first stop was APFS local snapshots: an automatic snapshot from thirty-one hours earlier held the entire folder tree intact: files, metadata, and the client-name subfolders whose existence he had denied. FSEvents corroborated the deletion sequence (paths and evening timestamps), and the quarantine database showed the same files had been downloaded to his personal Mac at home a week earlier via a file-transfer service, whose URL it had kept. The injunction application exhibited the snapshot listing beside his denial; undertakings followed within the week.

EXAMPLE 2 · THE BACKDATED AGREEMENT AND THE TIME MACHINE SERIES

A consultancy dispute turned on a signed letter agreement said to date from March 2023. The counterparty's Mac was imaged with its Time Machine drive. The document existed in no backup before February 2026, three weeks before proceedings; the February version's document-versions history showed its date field edited twice in one sitting; and the pattern-of-life database put the drafting application in active use on the claimed author's account that evening. The Mac's own time series had preserved not only the forgery but its rehearsal, and the claim was discontinued after the expert reports were exchanged.

EXAMPLE 3 · THE GENERALIST REPORT AND THE EMPTY UNALLOCATED SPACE

An opponent's expert, examining a founder's MacBook with Windows-era habits, reported that "forensic carving of unallocated space recovered no deleted documents; the alleged files therefore never existed." Our review report explained the architecture: on FileVault-encrypted SSD storage, carving free space recovers ciphertext fragments by design, so the null result was inevitable and meaningless: and then examined the layers the first report had skipped: two local snapshots, the FSEvents journal and the iCloud Drive version history, which together evidenced the files' creation, their ten-day life and their deletion two days after the letter of claim. The court preferred the architecture-literate analysis in terms; the costs of the first report were, in every sense, thrown away.

§ 0 9 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Powering off the logged-in Mac** without credentials in hand: the front door locked from inside, per guide 33.
- **Imaging without the key:** ciphertext acquired, examination impossible, and the schedule discovering it late.
- **Windows habits transplanted:** Example 3's carving fallacy; registry-shaped questions; unallocated-space conclusions on encrypted SSDs.
- **Snapshots and versions unexamined:** the recently-deleted evidence sitting one mount command away, missed.
- **The backup drive left on the desk:** "the computer" collected, the time series abandoned: §6's highest-yield sentence unwritten.
- **iCloud treated as out of scope:** placeholder stubs collected as if substantive; server-side versions and the phone's synced messages never fetched.
- **Slow instruction:** snapshots pruning, unified logs rolling, iCloud retention windows passing while the letter before action is polished.
- **Shared-studio attribution shortcuts:** the account/human conflation, unchanged from the Windows guide and just as fatal.

Technical limitations

- **No key, no content:** FileVault without credentials or escrow defeats examination of the protected volume; the honest report says so and pivots to the sources that remain (backups, iCloud, other devices).
- **Artefact horizons:** FSEvents is a rolling window; unified logs rotate quickly; pattern-of-life databases span weeks to months; snapshots prune under pressure: every finding carries its horizon, and absence beyond it proves nothing.
- **OS churn:** Apple changes artefact formats and locations frequently; findings are version-specific, tooling must be current, and yesterday's blog post is not a methodology.
- **Privacy engineering constrains:** some data classes are protected even from local examination without the user's unlock (per-app protections, secure enclave material); the examiner reports what the platform permits, not what folklore promises.
- **Cloud data is on Apple's terms:** iCloud content, versions and deleted-item retention follow Apple's mechanisms and timetables, and advanced user-enabled protections can place content beyond any collection without the user's devices and codes: a scoping fact, established early.

§ 10 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the Mac powered on and logged in now? Who holds the password, and is the fleet MDM-managed with FileVault key escrow?
- Where are the backups: Time Machine drives, network backup locations, and how far back do they run?
- What iCloud account is signed in, what syncs (Drive, Desktop and Documents, Messages, Photos), and who controls the credentials?

Ask your opponent

- Please preserve and disclose, in addition to the Mac itself: all Time Machine and other backup drives and locations; all APFS local snapshots (which we ask you not to prune or reduce); and the associated iCloud account's Drive contents, versions and recently-deleted items.
- Please state whether FileVault is enabled and confirm that credentials or recovery keys will be made available for examination under the agreed protocol.
- Please identify all user accounts on the machine and all persons with access in the relevant period.

Ask your eDiscovery / forensic provider

- What is your acquisition route for this hardware generation, and what will the image actually contain?
- Which artefact families and horizons apply to our questions on this machine's OS version?
- How will you collect the iCloud half: mechanism, legal basis, and handling of placeholder files?

SUGGESTED WORDING · INSTRUCTION FOR A MAC EXAMINATION

> "Please acquire and examine [the MacBook], its local APFS snapshots, the Time Machine backup [drive/location], and, on the basis set out at [consent/order reference], the associated iCloud account's [Drive, Messages, and recently-deleted and version data], and report on: (1) the existence, movement, deletion and provenance of [file categories], including snapshot, backup and cloud versions and quarantine origin records; (2) application usage and user sessions in [period], with the evidential basis for attribution; (3) external volumes and transfer mechanisms (including AirDrop and file-transfer services) in the period; and (4) a consolidated timeline in UTC and local time, graded and sourced, stating each artefact's horizon and any limitations arising from encryption, pruning or platform protections. Please secure all credentials and recovery keys at the outset and confirm acquisition method suitability for the hardware before attendance."

§ 11 · QUICK CONTROL

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

The Mac evidence checklist

- ☐ Power state assessed and the logged-in opportunity used; credentials and FileVault recovery keys secured (user, MDM escrow, iCloud)
- ☐ Acquisition method matched to the hardware generation; what-was-captured stated in the method record
- ☐ APFS local snapshots enumerated and preserved before pruning; document versions examined
- ☐ Time Machine and network backups identified, preserved and imaged as exhibits in their own right
- ☐ iCloud scope defined with legal basis; placeholders fetched, versions and recently-deleted collected
- ☐ Artefact families mapped to the questions: pattern-of-life, FSEvents, quarantine, recents, mounted volumes, unified logs
- ☐ Attribution layered: accounts, sessions, fast switching, corroborating records
- ☐ Horizons stated per finding; absence-of-evidence claims bounded accordingly
- ☐ Timeline delivered graded, sourced, dual-clocked
- ☐ Opposing Mac reports reviewed for architecture literacy (the Example 3 test)

Red flags

- A Mac powered down "for safekeeping" with no password in hand.
- "We imaged it" with no answer to "and the FileVault key?".
- An expert report reasoning from unallocated-space carving on modern Apple hardware.
- Snapshots, versions or backups pruned, reformatted or "tidied" after the dispute arose.
- iCloud stubs produced as if they were the documents.
- Attribution by ownership on a studio machine.

When to involve a digital forensic expert

At the first hint a Mac matters, for the same perishable-evidence reasons as ever, plus the credential clock: the logged-in machine and the retrievable key are opportunities that close. For acquisition, non-negotiably: modern Apple hardware punishes improvisation, and the method record must survive scrutiny. For examination and reporting, where architecture literacy is the whole game: snapshots, versions, pattern-of-life and cloud layers read by someone who works in them weekly, reported under CPR Part 35 / CrimPR Part 19 with horizons stated. And whenever the other side files Mac findings: the gap between Windows-habit reports and macOS reality is, as Example 3 shows, among the most efficiently exploitable weaknesses in current digital-evidence practice.

§ 12 · COMMON QUESTIONS

Frequently asked questions

Are Macs harder to examine than Windows machines?

Different, and less forgiving of casual method: encryption-by-default and integrated hardware make acquisition a credentialed, planned exercise rather than a drive-pull, and the artefact families reward specialists. Once acquired with keys, a Mac is at least as evidentially rich as its Windows counterpart, and its snapshot and version machinery often makes recently-deleted material easier to recover, not harder. The practical translation: the difficulty premium is paid at instruction (choose Mac-literate examiners, secure credentials early), not at trial.

Can deleted files be recovered from a Mac?

Frequently, by structure rather than carving: APFS local snapshots (hours to weeks back), Time Machine's series (months to years), per-document version histories, and iCloud's server-side versions and recently-deleted areas. What has genuinely gone is content absent from all four layers, and even then the metadata journal usually proves the files existed and when they died. The governing variable is speed: snapshots prune and cloud windows close, so the recovery conversation is best had this week.

What if the employee will not give up the password?

Work the alternatives in order: MDM escrow on managed fleets (the employer's own key); the iCloud-stored recovery key where the account cooperates or is controlled; compulsion routes where orders are available (with the privilege-against-self-incrimination and s.49 RIPA considerations of the encryption guide in criminal contexts); and, in parallel, the sources that need no device key: Time Machine backups made while the disk was unlocked, iCloud server-side data, email and corporate systems. A locked Mac narrows the estate; it rarely empties it.

Do Macs record USB sticks the way Windows does?

They record external volumes: mount events in system records and logs, volume names and timestamps, recent items referencing files on named external volumes, and Time Machine's knowledge of participating drives: enough, in combination, to do the exfiltration work of the Windows guide's examples. The artefact set differs (no registry, different persistence and horizons), so the formulation is calibrated per machine; the strategic point stands: copying to external media leaves traces on Macs too, and the stick itself remains the delivery-up prize.

The user's iPhone matters too. Does the Mac help?

Often substantially: Messages sync places the phone's iMessage/SMS history in the Mac's database; iCloud Photos, Notes and Drive mirror across devices; Continuity features leave cross-device traces; and local iPhone backups may sit on the Mac, examinable as device backups. The Mac is not a substitute for mobile forensics (the phone guides in this series cover that), but it is regularly the lawful, available window onto phone content when the handset itself is missing, wiped or withheld: a scoping opportunity worth remembering at the preservation stage.

Our opponent's expert says nothing was recoverable. How do we test that?

Apply the Example 3 test through your own examiner: did the report state the acquisition method and what the image contained; enumerate and examine local snapshots, versions, backups and iCloud layers; use the metadata journal for existence-and-deletion findings; and state horizons rather than converting them into "never existed"? A Part 35 review answering those four questions either validates the null result or, in our experience more often, relocates it: from "nothing was there" to "nowhere examined held it", which is a different sentence with different consequences.

§ 13 · REFERENCE

Glossary

APFS
Apple's file system: snapshots, clones, encryption-native design.

Apple Silicon
M-series Macs with integrated, hardware-bound storage; acquisition through the machine.

Biome / KnowledgeC
Pattern-of-life databases: application sessions, device state, interaction events.

FileVault
Default full-disk encryption; the credential gate to everything.

FSEvents
Rolling journal of file-system operations by path: the what-happened-in-that-folder record.

Local snapshot
Automatic APFS point-in-time volume state; the first recovery stop for the recently deleted.

MDM escrow
Corporate device management holding FileVault recovery keys for managed fleets.

Quarantine database
Per-download provenance: source URL, time, application: surviving the file's deletion.

Time Machine
Versioned backup series: hourly/daily/weekly states of the user's world, browsable per moment.

Unified logs
macOS's high-volume, fast-rotating system logging: authentication, devices, operations.

Document versions
Per-file edit-history database kept by many macOS applications.

Optimised storage
iCloud feature replacing local files with placeholders; substance server-side, fetch on collection.

Sources and authoritative references

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

- cflab.uk, digital forensics services (macOS and Apple Silicon acquisition, snapshot and backup examination, deleted data recovery, CPR Part 35 / CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Collection and Phase 04 · Processing (Mac and iCloud sources integrated into disclosure pipelines): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance · Forensic Science Regulator statutory Code: gov.uk/forensic-science-regulator
- ISO/IEC 27037:2012 and ISO/IEC 17025: iso.org, 27037 · iso.org, 17025
- Apple, platform security and support documentation (FileVault, iCloud, Time Machine): support.apple.com, Platform Security
- CPR Part 35 and CrimPR Part 19: justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19

DISCLAIMER

This publication provides general information about macOS forensic evidence as at August 2026. Apple changes hardware, OS behaviour and iCloud features frequently; artefact behaviour is version-specific, and 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 runs through the laboratory weekly, on current tooling and current hardware: credentialed acquisition matched to the machine's generation, snapshot and Time Machine examination, pattern-of-life and provenance artefact analysis, iCloud collection on a recorded legal basis, and the graded, dual-clocked timeline reporting of the wider series, under CPR Part 35 and CrimPR Part 19. We advise at the preservation moment (the logged-in opportunity, the credential hunt, the backup-drive sentence in your notice), and we review opposing Mac reports for architecture literacy: Example 3's exercise, performed to order. Through **e-discovery.uk**, Mac and iCloud sources flow into disclosure-scale processing beside every other estate. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine, and urgent Mac preservation can usually be mobilised within days.

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