COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Time Machine and macOS Backup Analysis

The Second Machine That Remembers What the First One Deleted

Time Machine is Apple's built-in backup system, and for the lawyer it is one of the most valuable sources on the whole Apple estate. It keeps regular, versioned backups of a Mac to an external drive or network location, preserving the state of the machine at many points across weeks, months or years. That makes a Time Machine backup a second machine that remembers what the first one deleted: a file erased from the Mac, a document altered after signing, a message or note removed, or system artefacts long since aged out by log rotation, may all survive intact in a backup taken before the change. Crucially, a Time Machine drive often sits outside the encryption and the anti-forensic reach of the live machine, so it can hold evidence even when the Mac itself is locked, wiped or unavailable. This guide sets out for UK lawyers how Time Machine and other macOS backups work, what they preserve, how prior states and deleted data are recovered from them, and how backup evidence is authenticated and interpreted honestly.

⏱ 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. Time Machine and backup analysis is one of the most productive parts of its Apple work: recovering deleted files, prior document versions and aged-out artefacts from versioned backups that often sit outside the encryption and reach of the live machine. The analysis authenticates and dates each recovered state and is reported under CPR Part 35 and CrimPR Part 19, so a backup becomes a reliable, dated record of what the Mac held at a known past moment.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | TIME MACHINE & BACKUP RECOVERY | PRIOR-STATE & VERSION ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: Time Machine keeps regular, versioned backups of a Mac, so a backup is a second machine that remembers what the first one deleted, preserving deleted files, earlier document versions and aged-out artefacts at many past points, often outside the encryption and reach of the live machine.

How it works (§3): Time Machine backs up the Mac at regular intervals to an external drive or network location, keeping many versioned snapshots over time, and other macOS and third-party backups do similar. **What it preserves (§4):** the state of the machine at each backup, files since deleted, documents before they were altered, messages, notes and system artefacts since aged out by log rotation. **Recovery (§5):** the specific prior state or deleted item extracted from the relevant backup, whole and datable, because a backup predating a change holds the thing intact. **Authentication (§6):** each recovered state authenticated and dated to its backup, and the backup's integrity established, so it is a reliable record of a known past moment. **Deployment (§7):** recovering the deleted file, proving the earlier version against a later edit, and restoring the aged-out log, often when the live Mac cannot supply them.

- **A second machine that remembers:** a Time Machine backup preserves the Mac's state at many past points.
- **It holds what was deleted:** files, versions, messages, notes and aged-out artefacts survive in backups.
- **Often outside the live machine's reach:** a backup drive may hold evidence even when the Mac is locked or wiped.
- **Dated and authenticatable:** each backup is a record of what the Mac held at a known time.
- **Interpret honestly:** a backup shows the state at its time, authenticated and dated to that moment.

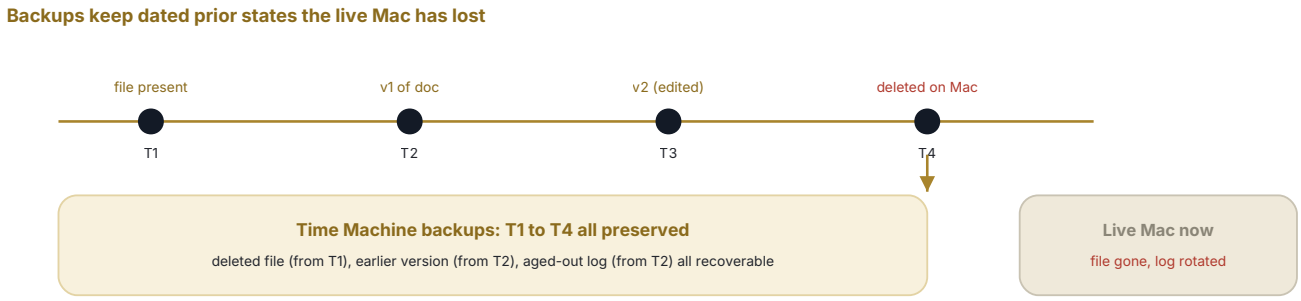

Figure 1 - a backup taken before a change holds the thing intact: the deleted file, the earlier document version and the aged-out log all survive in the Time Machine record even after the live Mac has lost them.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: a second machine that remembers

A backup exists to let a user recover from disaster, restore a lost file, roll back a bad change, rebuild a failed machine. For the forensic examiner and the lawyer, that same backup is something else: a preserved record of what the computer held in the past. Apple builds this in through Time Machine, which, once set up, automatically backs the Mac up at regular intervals to an external drive or a network location, and keeps many of those backups over time, so it holds the state of the machine not just as it is now but as it was hours, days, weeks and often months or years ago. Each backup is, in effect, a dated photograph of the Mac.

The evidential power of this is hard to overstate. Whatever a party has done to the live Mac, deleted a file, altered a document after signing, removed a message or a note, or simply let time and log rotation age out the system artefacts (guide 134), the backup taken before that change still holds the thing intact. A Time Machine backup is, quite literally, a second machine that remembers what the first one deleted. And there is a further, crucial point: the backup usually lives on a separate drive or server, outside the live machine. That means it often sits outside the encryption, the sync and the anti-forensic reach of the Mac itself, so it can hold recoverable evidence even when the live Mac is locked, wiped, or otherwise unavailable (guides 131, 133, 110). The tasks, then, are to find the backups, to recover the specific prior state or deleted item from the right one, and to authenticate and date each recovered state so it stands as a reliable record of what the Mac held at a known past moment. This guide sets out how Time Machine and other macOS backups work, what they preserve, how the past is recovered from them, and how backup evidence is authenticated and interpreted honestly.

§ 0 3 · HOW BACKUPS WORK

How Time Machine and macOS backups work

- **Regular, automatic backups:** Time Machine, once configured, backs the Mac up at regular intervals to a designated external drive or network location, without user intervention, so backups accumulate as a matter of routine (§2): the automatic historian.
- **Versioned over time:** many backups retained across a long period, hourly, daily and weekly, thinned over time, so the machine's state is preserved at numerous past points, not just the latest (§4): the many dated states.
- **Efficient storage of versions:** backups storing changes efficiently so that unchanged data is shared between versions while changed and deleted data is preserved from the point it existed, so each version can be reconstructed (§5): the space-saving that still keeps the past.
- **Local snapshots too:** Time Machine also keeps local snapshots on the Mac itself (guide 132) when the backup drive is absent, a related source, though the external backups are the fuller and more independent record (§8): the on-machine complement.
- **Other backups:** iCloud backup, disk clones and third-party backup tools providing further preserved states, each examined where present, so all backup sources are considered, not Time Machine alone (§8): the wider backup estate.

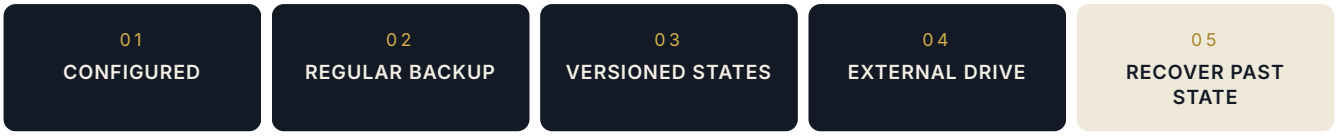

Figure 2 - Time Machine backs the Mac up regularly to an external drive, keeping many versioned states, so any preserved past state can be recovered from the backup.

§ 0 4 · WHAT BACKUPS PRESERVE

What backups preserve

- **Deleted files:** a file deleted from the live Mac surviving intact in any backup taken before the deletion, so deletion from the machine is not deletion from the record (guide 4): the erased file, still present in the backup.
- **Earlier document versions:** the state of a document at each backup preserved, so a version before a later alteration can be recovered and compared, exposing edits and backdating (guide 109): the prior version kept.
- **Messages, notes and mail:** earlier states of Mail, Messages and Notes stores (guide 135) preserved in backups, so deleted communications survive in a backup predating their removal (§7): the communications the backup retained.
- **System artefacts before rotation:** unified logs, activity databases and other artefacts (guide 134) preserved in backups from before log rotation aged them out, so activity history lost on the live machine survives in a backup (§7): the aged-out record recovered.
- **Application and system state:** the broader state of applications, settings and the system at each backup preserved, so the machine as it was at a past moment can be examined as a whole (§5): the whole machine, dated.

§ 0 5 · RECOVERING PRIOR STATES

Recovering prior states and deleted data

- **Acquire the backup soundly:** the Time Machine drive or backup location acquired forensically, with integrity preserved and, where it is unencrypted, imaged directly, so the backup is examined without altering it (guides 2, 3): the backup preserved as evidence.
- **Identify the right version:** the backup that predates the change or deletion in issue identified from the versioned history, so the recovery draws on the state that still holds the thing intact (§4): the correct dated state chosen.
- **Extract the item whole:** the deleted file, earlier version, communication or artefact extracted intact from that backup, a whole object rather than a carved fragment, with its metadata (guide 132): the past recovered complete.
- **Compare across versions:** successive backups compared to show how a file, document or artefact changed over time, bracketing when a change or deletion occurred (guides 96, 109): the change dated by comparison.
- **Handle backup encryption:** where a Time Machine backup is itself encrypted, access obtained by the backup password or lawful means (guides 117, 133), and any residual inaccessibility stated honestly, though many backup drives are unencrypted (§6): the encrypted backup addressed lawfully.

§ 0 6 · AUTHENTICATION AND HONEST LIMITS

Authentication, dating and honest limits

- **Date to the backup:** each recovered state dated to the backup it came from, so a file or version is shown to have existed on the Mac at that backup's known time, a reliable dated checkpoint (guide 96): the recovered thing anchored in time.
- **Authenticate the backup:** the backup's integrity and provenance established, whose Mac, which drive, how acquired, so the recovered material is shown to be a genuine, unaltered record (guides 2, 3): the backup itself proved sound.
- **State at the time, not now:** a backup shows the machine as it was at the backup time, not necessarily its later state, so the finding is expressed as existence at that moment, not current presence (guide 4): the honest temporal framing.
- **Gaps between backups:** events between two backups not directly captured, so the record is a series of dated states with intervals, and conclusions respect what falls between (guide 100): the interval acknowledged.
- **Attribution unchanged:** the backup preserves account activity, so attributing recovered material to a person still needs care, exactly as on the live machine (guide 105): the who-question kept honest.

§ 0 7 · DEPLOYMENT

Deployment: the deleted file, the earlier version, the aged-out log

- **Recovering the deleted file:** a file a party deleted from the Mac recovered whole from a backup predating the deletion, in fraud, IP and employment matters, and dated to that backup (guides 4, 98): the vanished file restored and dated.
- **Proving the earlier version:** a document's state before a later alteration recovered from a backup and compared with the version relied on, exposing backdating or editing (guide 109): the alteration proved by the backup.
- **Restoring the aged-out log:** system artefacts and activity records that log rotation removed from the live Mac recovered from a backup taken while they still existed, so the activity history extends further back (guide 134): the lost log recovered.
- **Reaching evidence past a locked or wiped Mac:** the backup drive, sitting outside the live machine, yielding evidence when the Mac is locked, wiped or unavailable, so the enquiry survives the loss of the device (guides 110, 131): the record the device could not deny.
- **Corroborated, dated presentation:** the recovered material authenticated, dated to its backup and corroborated across the estate, presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the backup evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a Time Machine backup is itself one of the most important "where else the evidence lives" answers for the whole Apple estate, and it in turn sits among other backup and prior-state sources. The live Mac holds the current data and its APFS snapshots (guide 132). But the Time Machine drive holds many dated prior states on separate, often unencrypted, media outside the machine; iCloud backup and iCloud-synced data hold cloud copies and some prior versions; disk clones and third-party backup tools hold further preserved states; the paired iPhone and iPad hold their own data and backups; and a corporate backup or archiving system holds managed copies. The discipline is to treat the backups as first-class sources, not afterthoughts, so that what is deleted, altered or aged out on the live machine is recovered from the backup that predates the change, and so that a locked or wiped Mac does not end the enquiry when a backup drive survives. When the live file is gone, the Time Machine backup holds it; when the Mac is inaccessible, the external backup and iCloud carry the record; and when a single backup has a gap, another backup source or a snapshot fills it.

EVIDENCE	LIVE MAC	TIME MACHINE DRIVE	APFS SNAPSHOTS	ICLOUD BACKUP / SYNC	CLONES / 3RD-PARTY BACKUP	DELETED / RECOVERABLE
Deleted files	Free-space remnants	Y: whole, dated	Y: whole, at time	Recently deleted	Y: if backed up	Y (multiple routes)
Earlier versions	COW remnants	Y: many versions	Y: at snapshot	Version history	Backup versions	Y
Communications	Live stores	Y: earlier stores	Y: snapshot state	Synced copies	Backup copies	Y (guide 135)
System artefacts	Subject to rotation	Y: pre-rotation	Y: at snapshot	Limited	Backup copies	Y (guide 134)
Access when Mac locked	n/a (locked)	Y: if unencrypted	On device only	Via account	Y: separate media	Backup / account

Fallback strategy in one line: treat the backups as primary sources; when the live Mac has deleted, altered, aged out or locked away the evidence, the Time Machine drive and other backups usually hold it, dated and intact.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DELETED FILE THE BACKUP DRIVE KEPT

A party deleted a decisive document from his Mac and, being careful, used the machine enough afterwards to overwrite the free-space remnants, so live recovery was uncertain. The §7 Time Machine analysis made it moot: an external backup drive held many dated backups, and one taken weeks before the deletion contained the document whole, with its metadata (guide 4). The §6 dating anchored it, the file was shown to have existed on the Mac at that backup's known time, and a later backup showed it gone, bracketing the deletion (guide 109). The backup drive, sitting outside the live machine, had quietly preserved what he had erased. The lesson is §2's: a Time Machine backup is a second machine that remembers what the first one deleted, so a file removed from the Mac, even where live recovery is defeated by overwriting, is routinely recovered whole and dated from a backup taken before the deletion.

EXAMPLE 2 · THE EARLIER VERSION THAT EXPOSED THE BACKDATING

A contract was produced bearing a certain date, and the other side suspected it had been altered later. The §5 and §7 version comparison across Time Machine backups resolved it: successive backups preserved the document at several points, and a backup taken after the purported date held a materially different, earlier version than the one produced, showing that a clause had been changed after the date the document claimed (guide 109). The §6 authentication established the backups' integrity, and each version was dated to its backup, so the timeline of the changes was reliable. The backup history, not the live file, told the true story of the document. The lesson is §4's: because backups preserve a document's state at many points, comparing versions across them can prove when, and how, a document was altered, and expose backdating that the final file conceals, with each version reliably dated to its backup.

EXAMPLE 3 · THE LOCKED MAC AND THE BACKUP THAT ANSWERED

A key Mac was recovered locked and powered off, and, without credentials or a recovery key, was inaccessible by direct means (guide 133). The §7 and §8 estate approach turned to the backups: a Time Machine drive found with the machine was unencrypted, and it held many dated states of the Mac, from which the relevant files, communications and even aged-out system artefacts (guide 134) were recovered, entirely independently of the locked machine. The §6 dating and authentication made the recovered material a reliable record of what the Mac had held at known past times. The device being closed had not closed the enquiry. The lesson is §2's and §8's: a Time Machine backup often sits outside the encryption and reach of the live machine, so it can yield evidence even when the Mac itself is locked, wiped or unavailable, making the backup drive one of the first things to look for when a device is inaccessible.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Ignoring backups:** the biggest miss, examining only the live Mac and overlooking the Time Machine drive that holds what the Mac deleted (Examples 1 and 3, §2).
- **Not looking for the backup drive:** failing to locate and preserve the external backup, especially when the Mac is locked or wiped (Example 3, §8).
- **Treating a backup as current:** reading a backup as the machine's present state rather than its state at the backup time (§6).
- **Not dating recovered items:** recovering material without anchoring it to its backup's known time (§6).
- **Missing version comparison:** not comparing successive backups to date a change or deletion (Example 2, §5).
- **Altering the backup:** examining the backup drive without preserving its integrity first (§5).
- **Overlooking other backups:** considering only Time Machine and missing iCloud, clones and third-party backups (§8).
- **Attributing carelessly:** recovered account activity attributed to a person without corroboration (§6).

Technical limitations

- **Only what was backed up survives:** a backup holds what existed at its time; data created and deleted between backups may not be captured: the interval limit (§6).
- **Backups can be encrypted:** an encrypted Time Machine backup needs the password or lawful access (§5, guide 133).
- **Backups are thinned:** older backups are pruned over time, so how far back the record reaches is bounded (§3).
- **No backup, no history:** if Time Machine was never configured, this source is absent, and others are relied on (§8).
- **Attribution still needs care:** a backup preserves account activity, not proof of who performed it (§6, guide 105).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is there a Time Machine or other backup of the Mac, and where is the backup drive or location, so it can be preserved as a priority?
- Might a deleted file, earlier version or aged-out record survive in a backup predating the change?
- If the Mac is locked or wiped, is there a backup that could hold the evidence independently?

Ask your opponent

- Please preserve and disclose all Time Machine and other backups of the device at Schedule 1, including the backup drive or location, without alteration.
- For any document, communication or file in issue, please confirm whether earlier or deleted versions survive in a backup, and provide them.
- Please confirm the backup configuration, the media used and the period covered.

Ask your eDiscovery / forensic provider

- What do the backups hold, and can the deleted or earlier material be recovered and dated from them?
- Can version comparison across backups date a change or deletion?
- If the Mac is inaccessible, does a backup hold the evidence independently, and is it encrypted?

SUGGESTED WORDING · INSTRUCTION FOR A BACKUP ANALYSIS

> "We instruct you to locate, preserve and analyse the Time Machine and other backups of the device at Schedule 1, relevant to Schedule 2. Please: (1) identify and forensically preserve all backups, the Time Machine drive or location, iCloud backups, disk clones and any third-party backups, imaging them without alteration and addressing any backup encryption by lawful means; (2) from the versioned history, recover intact any deleted files, earlier document versions, communications (Mail, Messages, Notes) and system artefacts (including those aged out by log rotation) relevant to the matter, with their metadata; (3) date each recovered state to the backup it came from and compare successive backups to establish when a change or deletion occurred, bracketing it between dated states; (4) authenticate each backup's integrity and provenance, and where the live Mac is locked, wiped or unavailable, recover the evidence from the backup independently; and (5) express findings as existence at the backup's time rather than current presence, respect the intervals between backups, attribute account activity to a person only with corroboration, and state confidence honestly."

§ 12 · QUICK CONTROL

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

The backup-analysis checklist

- ☐ Time Machine and other backups located and preserved without alteration
- ☐ Backup drive secured, especially where the Mac is locked or wiped
- ☐ Backup encryption addressed by lawful means
- ☐ Correct version predating the change identified
- ☐ Deleted files and earlier versions recovered whole
- ☐ Aged-out system artefacts recovered from pre-rotation backups
- ☐ Successive backups compared to date changes and deletions
- ☐ Each recovered state dated to its backup and authenticated
- ☐ Findings framed as existence at the backup time; intervals respected
- ☐ Attribution handled with care; confidence stated honestly

Red flags

- Only the live Mac examined; backups ignored: Examples 1 and 3.
- No search for the backup drive when the Mac is inaccessible: Example 3.
- A backup read as the current state rather than a past one: §6.
- Recovered items not dated to their backup.
- No version comparison to date a change: Example 2.
- The backup examined without preserving its integrity.
- iCloud, clones and third-party backups overlooked.

When to involve a digital forensic expert

Early, and as a matter of routine wherever a deletion, alteration or inaccessible Mac is in play, because the backup is so often the source that holds what the live machine cannot: the expert locates and forensically preserves the Time Machine and other backups, recovers intact the deleted files, earlier versions, communications and aged-out artefacts from the state that predates the change, and dates each to its backup as a reliable checkpoint (Examples 1 and 2, §5). Version comparison across backups brackets when a change or deletion occurred (Example 2), and, crucially, where the Mac is locked, wiped or unavailable, the backup drive, often unencrypted and outside the machine's reach, yields the evidence independently (Example 3, §8). Each backup is authenticated, findings are framed honestly as existence at the backup's time with intervals respected, and everything is reported under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, backup analysis treats Time Machine as the first-class source it is: the second machine that remembers what the first one deleted, and often the one place the evidence still lives when the live Mac has lost, altered or locked it away.

§ 13 · COMMON QUESTIONS

Frequently asked questions

A file was deleted from the Mac. Can a backup still have it?

Very often yes (§4, Example 1). Time Machine keeps regular, versioned backups, so a file deleted from the live Mac survives intact in any backup taken before the deletion, complete with its metadata, and can be dated to that backup's known time. This holds even when live recovery is defeated by overwriting, because the backup preserved the file independently. A Time Machine backup is a second machine that remembers what the first one deleted, which makes it one of the most valuable sources on the estate.

Can backups prove a document was altered after it was dated?

Frequently (§5, Example 2). Because backups preserve a document's state at many points, comparing successive versions across them can show that the document changed, and when. If a backup taken after the document's purported date holds an earlier, different version than the one produced, that exposes a later alteration or backdating (guide 109). Each version is dated to its backup and the backups are authenticated, so the timeline of the changes is reliable, the backup history, not the final file, tells the true story.

The Mac is locked and we cannot access it. Does that end things?

Often not, look for the backup (§8, Example 3). A Time Machine backup usually lives on a separate drive or server, outside the live machine, and is frequently unencrypted, so it can hold the evidence even when the Mac itself is locked, wiped or unavailable (guides 131, 133). Recovering files, communications and even aged-out artefacts from the backup, independently of the device, can carry the matter forward. When a device is inaccessible, the backup drive is one of the first things to look for.

Can a backup recover system logs that have rotated away?

Yes, that is one of its great strengths (§4, §7, guide 134). The unified logs and some activity artefacts rotate, ageing older entries out of the live Mac. But a backup taken while those entries still existed preserves them, so activity history lost on the live machine can be recovered from a pre-rotation backup, extending how far back the record reaches. This is often the only way to reach older activity, which is why backups are examined whenever the relevant period predates the surviving live logs.

How reliable is a backup as evidence of timing?

Reliable, when authenticated and properly framed (§6). Each recovered item is dated to the backup it came from, so it is shown to have existed on the Mac at that backup's known time, a dependable dated checkpoint. The important discipline is that a backup shows the state at its time, not the machine's later state, and events between two backups are not directly captured, so conclusions respect the intervals. Authenticated and framed this way, backups give some of the most reliable dating available.

What if there is no Time Machine backup?

Then other sources are relied on (§8). If Time Machine was never configured, that particular record is absent, but the estate offers alternatives: APFS local snapshots on the Mac (guide 132), iCloud backup and synced data, disk clones, third-party backups, and the paired devices. A thorough analysis considers all backup and prior-state sources, not Time Machine alone. Where none exists, the live-machine recovery and the wider estate carry the enquiry, with the absence of a backup simply noted.

§ 14 · REFERENCE

Glossary

Time Machine
Apple's built-in versioned backup system.

Backup
A preserved copy of a machine's state at a point in time.

Versioned backup
Backups kept at many past points over time.

Backup drive
The external drive or location holding the backups.

Prior state
The machine as it was at a past backup.

Version comparison
Comparing backups to date a change or deletion.

Local snapshot
An on-Mac Time Machine snapshot (see guide 132).

iCloud backup
A cloud backup of a device's data.

Dated checkpoint
A backup used to prove existence at its time.

Encrypted backup
A backup needing a password to access.

Sources and authoritative references

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

- cflab.uk, digital forensics services (Time Machine and backup recovery, prior-state and version analysis, 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 (backup preservation and recovery 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 support and Platform Security guide (Time Machine, local snapshots, backup encryption and iCloud backup): support.apple.com, Platform Security · support.apple.com, Time Machine
- Forensic Science Regulator, Code of Practice v2 (integrity, authentication and dating): gov.uk, FSR Code · ISO/IEC 27037: 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

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Backup analysis at the laboratory treats Time Machine as the first-class source it is, often the one place the evidence still lives. The backups, the Time Machine drive, iCloud backups, disk clones and third-party tools, are located and forensically preserved without alteration, and any backup encryption is addressed by lawful means (guides 117, 133). From the versioned history, the specific state that predates the change in issue is identified, and the deleted file, earlier document version, communication or aged-out system artefact is recovered intact with its metadata (Examples 1 and 2). Successive backups are compared to date a change or deletion, bracketing it between dated states and exposing backdating (guide 109), and each recovered item is dated to its backup and the backup authenticated, so it stands as a reliable record of what the Mac held at a known past time. Crucially, where the live Mac is locked, wiped or unavailable, the backup drive, frequently unencrypted and outside the machine's reach, yields the evidence independently, so a closed device does not close the enquiry (Example 3). Findings are framed honestly as existence at the backup's time, with intervals respected and attribution handled with care, and reported under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding point is simple: whatever a party did to the live Mac, the backup taken beforehand usually still remembers it, dated and intact.

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