



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

macOS System Artefacts

Unified Logs, Activity Databases and the Detailed Record of What Was Done, and When

Beneath the documents and messages, a Mac keeps a remarkably detailed record of its own use: which applications ran and when, which files were opened, what was searched for, when the device woke and slept, what was connected, and much more. These system artefacts, the unified logs, the activity databases such as the one often called KnowledgeC, Spotlight and its metadata, the record of recent items and quick-look thumbnails, and many others, together reconstruct user activity with a precision that surprises those new to Mac forensics. They answer the questions that matter most in disputes: not just what a file contains, but whether and when someone opened it, used an application, searched for a term or was active at the machine. This guide sets out for UK lawyers what the principal macOS system artefacts are, what each reliably shows, how they are combined into a defensible activity timeline, and how their meaning, and their limits, including log rotation and honest interpretation, are handled in evidence.

© 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. macOS system-artefact analysis is where its Mac work turns storage into a record of behaviour: the unified logs, activity databases, Spotlight metadata, recent items and related artefacts that show what was done on a Mac and when. The analysis reconstructs user activity into defensible timelines, interpreted with an understanding of what each artefact does and does not prove, and reported under CPR Part 35 and CrimPR Part 19 with limits such as log rotation stated plainly.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

UNIFIED LOGS & ACTIVITY DATABASES

ACTIVITY TIMELINE RECONSTRUCTION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: the Mac remembers what was done
03	The principal system artefacts
04	What each artefact reliably shows
05	Building the activity timeline
06	Interpretation, log rotation and honest limits
07	Deployment: proving activity, use and presence
08	Source architecture: where else the evidence lives
09	Worked examples
10	Common mistakes and technical limitations
11	Questions to ask · Suggested wording
12	Checklist and red flags · When to involve a digital forensic expert
13	Frequently asked questions
14	Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

The headline point: a Mac keeps a detailed record of its own use, in unified logs, activity databases, Spotlight and many other artefacts, that reconstructs what applications ran, what files were opened, what was searched and when the user was active, answering the who-did-what-when questions at the heart of disputes, provided each artefact is interpreted for what it truly shows.

The artefacts (§3): the unified logs (a vast system-wide event record), activity databases such as the one often called KnowledgeC, Spotlight and its metadata, recent items, quick-look thumbnails and related records. **What each shows (§4):** each artefact reliably evidences particular things, application use, file access, searches, device wake and sleep, connections, and each is read for its specific meaning, not stretched. **The timeline (§5):** the artefacts combined, on a normalised clock, into an activity timeline that reconstructs user behaviour far more richly than any single record. **Interpretation and limits (§6):** artefacts are interpreted honestly, distinguishing activity from mere presence of a file, and their limits, above all log rotation, which ages older entries out, are stated. **Deployment (§7):** proving whether and when a file was opened, an application used, a search made or the user active, as corroborated activity evidence.

- **The Mac remembers use, not just content:** artefacts record what was done, not only what files exist.
- **Many artefacts, specific meanings:** logs, activity databases and Spotlight each show particular things reliably.
- **Activity timelines are powerful:** combined on one clock, artefacts reconstruct user behaviour in detail.
- **Log rotation is the key limit:** older log entries age out, so prompt preservation matters and gaps are stated.
- **Interpret honestly:** activity is distinguished from a file merely being present, at honest confidence.

Many artefacts reconstruct one activity timeline

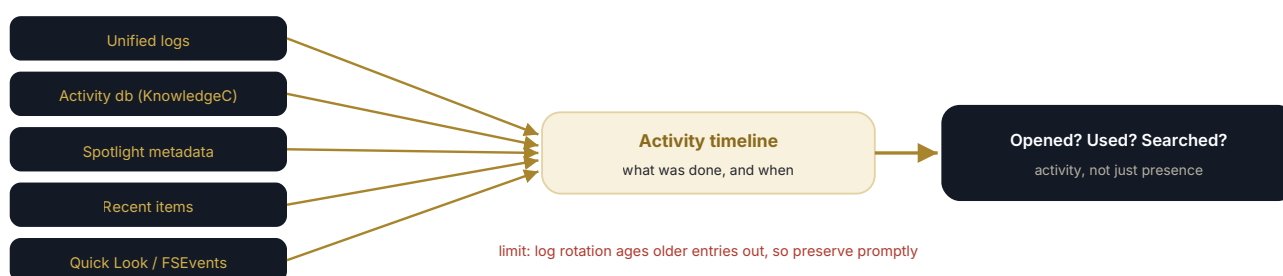


Figure 1 - the principal macOS system artefacts feed one normalised activity timeline that answers whether and when files were opened, applications used and searches made, subject to log rotation.

The problem in plain English: the Mac remembers what was done

Most people, and many lawyers, think of the evidence on a computer as its contents: the documents, the emails, the photos. But a huge part of what makes computer evidence powerful is not the content at all; it is the record the machine keeps of its own operation. A Mac, in the ordinary course of running, continually notes what it is doing: which applications launch and quit, which documents are opened and by what, what the user searches for, when the machine wakes, sleeps and is used, what devices and networks it connects to, and a great deal more. This information lives in system artefacts, structured records maintained by macOS for its own purposes, that a forensic examiner can read to reconstruct not just what was on the machine but what was done with it, and when.

This matters because the decisive question in a dispute is often about activity rather than mere presence. It is one thing to show that a confidential file existed on a departing employee's Mac; it is far more telling to show that they opened it, copied it to a USB drive, and searched for related terms, on a particular evening, using the machine themselves. The content shows what; the system artefacts show whether, when and how it was used. The principal artefacts, the unified logs, the activity databases such as the one often referred to as KnowledgeC, Spotlight and its metadata, the lists of recent items, the thumbnails generated when files are previewed, and others, each capture particular kinds of activity, and combined on a common timeline they reconstruct user behaviour with real precision. But they must be read correctly: each artefact means a specific thing, activity is not the same as a file merely being present, and the records have limits, above all log rotation, whereby older entries are aged out to save space, so a gap in the record is not the same as an absence of activity. This guide sets out the artefacts, what each shows, how they build a timeline, and how their meaning and limits are handled honestly.

§ 0 3 · THE ARTEFACTS

The principal system artefacts

- **The unified logs:** a vast, system-wide stream of events from the operating system and applications, recording an enormous range of activity in detail, the richest single source of what the machine was doing, though subject to rotation (§6): the firehose of system events.
- **Activity databases (KnowledgeC and related):** databases that record user and device activity, application usage, device wake and sleep, and interactions over time, often the clearest record of when the machine and its apps were actually used (§4): the usage record.
- **Spotlight and its metadata:** the system-wide search index and the metadata store that records information about files, including timestamps and attributes, valuable both for what files exist and for search-related activity (§4): the index that knows the files.
- **Recent items and application state:** the lists of recently opened documents and applications, and saved application state, showing what the user opened and worked with recently (§4): the trail of recent use.
- **Quick Look, FSEvents and related traces:** thumbnails generated when files are previewed, the file-system event record, and other traces that evidence files having been seen or changed, corroborating activity (§4): the supporting traces.

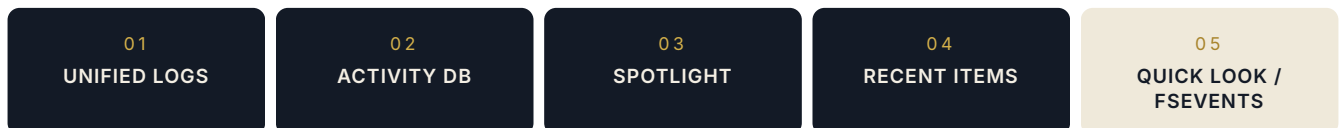


Figure 2 - the principal macOS system artefacts, from the system-wide unified logs to the specific traces of preview and file-system change, each contributing to the activity picture.

§ 0 4 · WHAT EACH SHOWS

What each artefact reliably shows

- **Application use and timing:** the activity databases and logs showing which applications ran, when, and for how long, so the use of a particular app at a particular time can be established (guide 96): the when-was-this-app-used answer.
- **File access:** recent items, quick-look thumbnails, file-system events and log entries together evidencing that a particular file was opened, previewed or accessed, and when, activity beyond mere existence (§2): the was-this-file-opened answer.
- **Searches and queries:** Spotlight and related artefacts evidencing what was searched for, revealing intent and interest that content alone does not (guide 125's search-as-signal theme, applied to the Mac): the what-was-sought answer.
- **Device use, wake and sleep:** the activity databases recording when the machine was awake, asleep and in use, so periods of actual user presence at the device can be reconstructed (§5): the when-was-it-in-use answer.
- **Connections and devices:** logs and artefacts evidencing connected USB devices, networks and peripherals, so, for example, the attachment of an external drive at a given time can be shown (guide 110's exfiltration context): the what-was-connected answer.

§ 0 5 · THE ACTIVITY TIMELINE

Building the activity timeline

- **Combine the artefacts:** the several artefacts brought together, so application use, file access, searches, device use and connections are seen as one sequence of activity rather than as isolated records (guide 96, guide 130): the reconstruction from many sources.
- **Normalise the clocks:** the artefacts' timestamps reconciled to a common time base, accounting for time zones and any drift, so events from different artefacts align truly (guides 108, 130): the alignment that makes the timeline sound.
- **Corroborate across artefacts:** a given activity confirmed by more than one artefact, a file open shown by recent items, a thumbnail and a log entry together, so the finding rests on convergence, not a single record (guide 124): the cross-checked event.
- **Tie to content and the estate:** the activity timeline married to the documents and messages it concerns, and to the wider estate (guide 131, §8), so behaviour and content tell one story (guide 130): the timeline made meaningful.
- **Reconstruct behaviour:** the result a detailed account of what the user did on the machine and when, opened this, searched that, connected a drive, was active at these times, far richer than content alone (§7): the behaviour reconstructed.

Interpretation, log rotation and honest limits

- **Log rotation ages entries out:** the central limit, that the unified logs and some artefacts retain only a limited window before older entries are overwritten, so activity from further back may simply not be recorded, and a gap is not proof of inactivity (guide 100): the limit that governs how far back one can see.
- **Preserve promptly:** because of rotation, the sooner the machine is acquired the more history survives, so prompt preservation directly affects how much of the past the artefacts can show (guides 131, 95): the preservation consequence.
- **Activity is not presence:** an artefact showing a file was opened is different from the file merely existing, and the finding states which it is, activity evidence read as activity, not overstated (guide 4): the crucial distinction.
- **Each artefact means a specific thing:** artefacts interpreted for their precise meaning, a thumbnail means a preview, a recent-items entry means an open, a log line means a specific event, not stretched into general claims (guide 100): the discipline of precise reading.
- **Attribution to the person:** activity attributed to a user account and, with care, to a person, since the machine may be shared and an account is not automatically an individual (guide 105): the who-was-at-the-keyboard question kept honest.

Deployment: proving activity, use and presence

- **Proving a file was opened:** artefacts establishing that a party opened or accessed a document, and when, in confidentiality, IP and employment matters where use, not mere possession, is the issue (guides 4, 110): the access proved, not assumed.
- **Proving application and device use:** the use of a particular application, or the connection of an external drive, at a particular time shown, evidencing exfiltration, tampering or activity relevant to the dispute (guide 110): the action evidenced.
- **Establishing user presence:** the activity databases reconstructing when the machine was actually in use, supporting or undermining accounts of where a person was and what they were doing (guides 96, 124): the presence at the device shown.
- **Revealing intent through searches:** what was searched for on the machine evidencing interest and intent that content alone does not carry (guide 125): the intent glimpsed through activity.
- **Corroborated, honest activity evidence:** the activity findings corroborated across artefacts and the estate, and presented at honest confidence with limits like rotation stated, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the behaviour proved defensibly.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the system artefacts on one Mac are a rich record of activity, but similar activity records exist across the Apple estate, and corroborating across them strengthens the account and covers the gaps that log rotation leaves. The Mac holds its unified logs, activity databases, Spotlight metadata and related traces. But a paired iPhone or iPad holds its own activity records for the same user's behaviour on those devices; iCloud and account records hold sign-ins, some usage and synced-app activity; Time Machine and other backups hold older states of the artefacts from before rotation aged them out; and a managed device's administrative console holds usage and access logs centrally (guides 111 to 114). The discipline is to treat the Mac's artefacts as one activity source among several, so that activity is corroborated across devices and, crucially, so that history lost to log rotation on the live machine may survive in a backup taken earlier. When the live logs have rotated away, a Time Machine backup preserves the older entries; when activity on the Mac is denied, the paired device and account records corroborate or contradict; and the estate as a whole gives a fuller behavioural picture than any one device.

EVIDENCE	MAC LIVE ARTEFACTS	TIME MACHINE / BACKUPS	PAIRED IPHONE / IPAD	ICLOUD / ACCOUNT	MANAGED-DEVICE CONSOLE	AGED-OUT / RECOVERABLE
Application use	Y: activity db, logs	Y: earlier state	Device usage	Some app activity	Admin usage logs	Backup restores
File access	Y: recent items, logs	Y: earlier records	Shared files	iCloud access	Access logs	Backup / snapshot
Searches	Y: Spotlight	Backup copies	Device searches	Limited	n/a	Backup
Device use / presence	Y: activity db	Earlier data	Y: device activity	Sign-in times	Session logs	Backup
Connections (USB, net)	Y: logs	Earlier logs	Device connections	Limited	Network logs	Rotated (guide 100)

Fallback strategy in one line: corroborate activity across the estate, and where log rotation has aged out the live record, an earlier Time Machine backup, the paired device or the account often preserves what the Mac no longer holds.

Worked examples

EXAMPLE 1 · THE OPENED FILE AND THE CONNECTED DRIVE

A departing employee denied taking confidential files, admitting only that they had existed on his Mac. The §4 and §7 system artefacts told the fuller story: recent-items entries, a quick-look thumbnail and unified-log lines showed he had opened the specific files on a particular evening; and the logs showed an external USB drive connected minutes later (guide 110). The §5 activity timeline, with clocks normalised, placed the opens and the drive connection in a coherent sequence, and the §6 interpretation kept it honest, activity, not mere presence, and attributed to his account with care (guide 105). Content alone would have shown only that the files existed; the artefacts showed they were opened and a drive attached, when, and in what order. The lesson is §2's: the decisive evidence is often activity, not content, and macOS system artefacts routinely show whether and when a file was opened and a device connected, turning a bare denial into a documented sequence of actions.

EXAMPLE 2 · THE GAP THAT WAS ROTATION, NOT INNOCENCE

A party argued that the absence of any log entries for a certain earlier period proved nothing had happened then. The §6 log-rotation discipline corrected the inference: the unified logs retain only a limited window, and the period in question predated the surviving logs, so the silence was rotation, not proof of inactivity, and it would have been wrong to read the gap as an absence of activity (guide 100). Crucially, the §8 estate filled part of the gap: a Time Machine backup taken during the earlier period preserved artefacts since aged out of the live machine, and those older records showed the relevant activity after all. The honest reading of the gap, and the recovery of the older state from backup, together defeated the false inference. The lesson is §6's: log rotation means a gap in the record is not proof that nothing happened, the honest expert says so, preserves promptly to save what remains, and looks to earlier backups where the estate can restore what rotation has removed.

EXAMPLE 3 · THE SEARCHES THAT SHOWED INTENT

In a matter turning on a party's intentions, the content of their files was ambiguous, but the §4 Spotlight and activity artefacts were not: the record of what they had searched for on the Mac, and the applications they had used around the relevant time, revealed a clear pattern of interest and preparation that the documents alone did not convey (guide 125's search-as-signal principle). The §5 activity timeline placed the searches and app use in sequence with the events in issue, and the §6 interpretation was careful, searches evidence interest and activity, attributed to the account with care, not proof of a completed act. The behavioural record shifted the picture materially. The lesson is §4's: system artefacts capture activity that content cannot, and what a person searched for and did on a machine often reveals intent and preparation, so the artefacts answer questions, about why and with what purpose, that the documents leave open, provided they are read at honest confidence.

Common mistakes and technical limitations

Common mistakes

- **Looking only at content:** the biggest missed opportunity, examining documents while ignoring the artefacts that show they were opened and used (Example 1, §2).
- **Reading a log gap as inactivity:** treating the absence of entries as proof nothing happened, when it may be log rotation (Example 2, §6).
- **Confusing activity with presence:** a file existing mistaken for the file being used, or vice versa (§6).
- **Stretching an artefact's meaning:** a thumbnail or recent-items entry read as more than it shows (§6).
- **Not preserving promptly:** delay allowing log rotation to age out the very period in issue (Example 2, §6).
- **Ignoring clock normalisation:** artefacts combined without reconciling timestamps, creating false sequences (§5).
- **Assuming account equals person:** activity attributed to an individual without care on a possibly shared machine (§6, guide 105).
- **Not corroborating:** an activity finding rested on one artefact when others could confirm it (§5).

Technical limitations

- **Log rotation limits history:** older entries age out, so how far back the record reaches is bounded and gaps are not absences: the central limit (§6).
- **Artefacts have specific meanings:** each shows a particular thing and cannot be stretched into general claims (§6).
- **Activity is not identity:** artefacts show account activity; attributing it to a person needs care (§6, guide 105).
- **Interpretation needs expertise:** macOS artefacts are numerous, technical and easily misread (§4).
- **macOS evolves:** artefacts, their formats and retention change across OS versions, so behaviour is checked per version (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the question about activity, whether and when a file was opened, an app used, a search made, rather than only about content, so the system artefacts are engaged?
- Has the Mac been preserved promptly, before log rotation ages out the relevant period?
- Are there earlier backups (Time Machine) that might preserve artefacts since rotated away?

Ask your opponent

- Please preserve the Mac and its system artefacts (unified logs, activity databases, Spotlight, recent items and related traces) without continued use that may cause log rotation, and any Time Machine backups.
- Please disclose the activity records evidencing access to and use of the files and applications in issue, and connections of external devices.
- Please confirm the account under which relevant activity occurred and whether the machine was shared.

Ask your eDiscovery / forensic provider

- What do the artefacts show about whether and when the files were opened, apps used and searches made?
- How far back does the surviving record reach, given log rotation, and what fills any gap?
- How is the activity corroborated across artefacts and attributed to a person honestly?

SUGGESTED WORDING · INSTRUCTION FOR A SYSTEM-ARTEFACT ANALYSIS

"We instruct you to examine the macOS system artefacts on the device at Schedule 1 to reconstruct user activity relevant to Schedule 2. Please, on the acquired device and preserving integrity: (1) recover and analyse the principal artefacts, the unified logs, activity databases (including KnowledgeC and related), Spotlight and its metadata, recent items, quick-look thumbnails, file-system events and device-connection records; (2) establish whether and when the relevant files were opened or accessed, applications were used, searches were made, external devices were connected and the machine was in use, distinguishing activity from mere presence; (3) combine the artefacts into an activity timeline on a normalised clock, corroborating each finding across more than one artefact where possible; (4) address the limits honestly, in particular log rotation, stating how far back the surviving record reaches and treating gaps as rotation rather than proof of inactivity, and drawing on earlier backups where they preserve aged-out records; and (5) attribute activity to a user account and, with appropriate care, to a person, and state conclusions at honest confidence."

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

The system-artefact checklist

- ☐ Mac preserved promptly, before log rotation ages out the period in issue
- ☐ Unified logs, activity databases and Spotlight recovered
- ☐ Recent items, quick-look and file-system events analysed
- ☐ File opens, app use, searches and connections established
- ☐ Activity distinguished from mere file presence
- ☐ Artefacts combined on a normalised clock into a timeline
- ☐ Each finding corroborated across more than one artefact
- ☐ Log rotation addressed; gaps read honestly, backups used
- ☐ Activity attributed to account and person with care
- ☐ Conclusions stated at honest confidence with limits explained

Red flags

- Only content examined; activity artefacts ignored: Example 1.
- A log gap read as proof of inactivity: Example 2.
- Activity confused with mere file presence: §6.
- An artefact's meaning stretched beyond what it shows: §6.
- Delay allowing the relevant period to rotate away.
- Artefacts combined without clock normalisation.
- Account activity attributed to a person without care.

When to involve a digital forensic expert

Whenever the question is about activity rather than content, and promptly, because log rotation is quietly ageing out the record every day the machine runs (Example 2, §6): the expert recovers and interprets the many macOS artefacts, unified logs, activity databases, Spotlight, recent items and the rest, to show whether and when files were opened, applications used, searches made and devices connected (Examples 1 and 3, §4); combines them into a normalised, corroborated activity timeline that reconstructs behaviour far beyond what content shows (§5); and reads them honestly, distinguishing activity from presence, treating log gaps as rotation rather than innocence, drawing on backups to recover aged-out records, and attributing activity to a person with care (§6). The findings are corroborated across the estate and reported at honest confidence under CPR Part 35 or CrimPR Part 19 (§8). Prompt preservation directly determines how much survives. Through **cflab.uk** and **e-discovery.uk**, system-artefact work answers the questions that most often decide a case, not just what was on the Mac, but what was done with it, and when, drawn from the detailed record the machine keeps of its own use.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can you tell whether someone actually opened a file, not just that it was there?

Yes, that is exactly what system artefacts are for (§4, Example 1). Recent-items lists, quick-look thumbnails, file-system events and unified-log entries together can show that a specific file was opened or previewed, and when. This activity evidence is often far more telling than the mere existence of the file, especially in confidentiality and employment disputes where the issue is use, not just possession. The artefacts distinguish a file that sat unopened from one that was actively used.

What is KnowledgeC and why is it useful?

It is one of the macOS activity databases (§3, §4), a record of user and device activity, including application usage and when the device was awake and in use, over time. It is useful because it gives a clear, timestamped picture of when the machine and its applications were actually used, helping reconstruct user behaviour and presence at the device. Read alongside the unified logs and other artefacts, it is a valuable part of the activity timeline, interpreted, like all artefacts, for what it specifically shows.

There are no log entries for the period we care about. Does that clear our opponent?

Not necessarily, this is the log-rotation trap (§6, Example 2). The unified logs retain only a limited window, and older entries are aged out to save space, so an absence of entries for an earlier period may simply mean the logs have rotated, not that nothing happened. A gap is not proof of inactivity. An honest analysis says so, preserves promptly to save what remains, and looks to earlier Time Machine backups, which often preserve artefacts since rotated off the live machine.

Can the artefacts show what someone searched for?

Often yes (§4, Example 3). Spotlight and related artefacts can evidence what was searched for on the machine, which can reveal interest, intent and preparation that the content of files does not convey (guide 125). Combined with application-use records, this can be powerful behavioural evidence. It is interpreted carefully, a search shows interest and activity, attributed to an account with care, not a completed act, but what a person sought on a machine frequently illuminates why they were doing what they did.

How urgent is preserving the Mac for this kind of evidence?

Genuinely urgent (§6, Example 2). Because the unified logs and some artefacts rotate, ageing out older entries as the machine keeps running, every day of continued use can erode the record of the period in issue. Preserving the Mac promptly, and acquiring it quickly, maximises how far back the activity record reaches. As with Mac acquisition generally (guide 131), the sooner the machine is secured and examined, the more of its detailed activity history survives to be analysed.

Do the artefacts prove who was using the machine?

They show account activity; attributing it to a person takes care (§6, guide 105). The artefacts record what was done under a user account, but a machine may be shared, and an account is not automatically an individual. So activity is attributed to the account first, and to a person only with corroboration, other artefacts, the estate, surrounding evidence, and stated at honest confidence. This keeps the powerful activity record from being overstretched into an unsupported claim about exactly who was at the keyboard.

§ 1 4 · REFERENCE

Glossary

System artefact

A record macOS keeps of its own operation and use.

Unified logs

The system-wide stream of detailed OS and app events.

Activity database

A store of user/device activity (e.g. KnowledgeC).

KnowledgeC

A macOS database of app usage and device activity.

Spotlight

The system search index and file metadata store.

Recent items

Lists of recently opened documents and apps.

Quick Look

File preview, leaving thumbnail traces of viewing.

FSEvents

The file-system change event record.

Log rotation

Ageing out of older log entries to save space.

Activity timeline

Artefacts combined to reconstruct user behaviour.

Sources and authoritative references

The system-artefact 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 system-artefact analysis, activity-timeline reconstruction, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 06 · Analysis and Phase 07 · Review (activity reconstruction and interpretation as practised): e-discovery.uk/edrm/analysis · e-discovery.uk/edrm/review
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple Platform Security guide and developer documentation (unified logging, Spotlight and system services): support.apple.com, [Platform Security](https://support.apple.com/platform-security) · developer.apple.com, [unified logging](https://developer.apple.com/unified-logging)
- Forensic Science Regulator, Code of Practice v2 (interpretation, limits and honest reporting): gov.uk, [FSR Code](https://gov.uk/fsr-code) · ISO/IEC 27037: iso.org, [27037](https://iso.org/27037)
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad) · justice.gov.uk, [Part 31](https://justice.gov.uk/part-31) · justice.gov.uk, [Part 35](https://justice.gov.uk/part-35)

DISCLAIMER

This publication provides general information about macOS system artefacts as at August 2026. The artefacts, their formats and their retention change across operating-system versions, and their evidential meaning depends on correct interpretation; log rotation limits how far back the record reaches, and a gap is not proof of inactivity. Activity is recorded against user accounts and attributing it to a person requires care. 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

System-artefact work at the laboratory answers the questions that most often decide a case: not just what was on a Mac, but what was done with it, and when. The principal artefacts, the unified logs, the activity databases such as KnowledgeC, Spotlight and its metadata, recent items, quick-look thumbnails and file-system events, are recovered and analysed to establish whether and when files were opened, applications used, searches made, external devices connected and the machine actually in use (Examples 1 and 3). They are combined into an activity timeline on a normalised clock, with each finding corroborated across more than one artefact and tied to the content and the wider estate (guide 130). Interpretation is honest throughout: activity is distinguished from mere presence, log rotation is confronted so that gaps are read as rotation rather than innocence and earlier backups are used to recover aged-out records (Example 2), and activity is attributed to an account and to a person with appropriate care. Because rotation ages the record out with continued use, prompt preservation directly determines how much survives. Findings are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide closes the opening run of the Apple block, acquisition, file system, encryption and artefacts, that together define modern Mac forensics. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the enduring point is that a Mac keeps a detailed diary of its own use, and read correctly, that diary is often the most telling evidence of all.



I N S T R U C T T H E L A B

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