MacOS System Artefacts

macOS system artefacts provide a detailed record of user activity, answer in g who-did-what-when questions in disputes. This guide covers principal artefacts, activity timeline reconstruction, interpretation, and common limitations for UK legal professionals.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/macos-system-artefacts

MACOSSYSTEMARTEFACTS · A GUIDE FOR UK LAWYERS macOS System Artefacts Unified Logs, Activity Databases and the Detailed Record of What Was Done, and When COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM 19 with limits such as log rotation stated plainly. ACTIVIT Y TIMELINE RECONSTRUCTION CPR PART 35 EXPERT REPORT S 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

§ 01 · ORIENTATION Executive summary and many other artefacts, that reconstructs what applications ran, what files were opened, what was searched and when the user was active, answer in g the who-did-what-when questions at the heart of disputes, provided each artefact is interpreted for what it truly shows.

§ 02 · FIRST PRINCIPLES The problem in plain English: the Mac remembers what was done

§ 03 · THEARTEFACTS The principal system artefacts UNIFIED LOGS ACTIVITY DB SPOTLIGHT RECENT ITEMS QUICK LOOK / FSEVENTS

§ 04 · WHATEACHSHOWS What each artefact reliably shows

§ 05 · THEACTIVITYTIMELINE Building the activity timeline

§ 06 · INTERPRETATIONANDHONESTLIMITS Interpretation, log rotation and honest limits

§ 07 · DEPLOYMENT Deployment: proving activity, use and presence

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE MACHINE / IPHONE / DEVICE MAC LIVE ICLOUD / AGED-OUT / ARTEFACTS ACCOUNT RECOVERABLE TIME PAIRED MANAGED- BACKUPS IPAD CONSOLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEOPENEDFILEANDTHECONNECTEDDRIVE EXAMPLE2 · THEGAPTHATWASROTATION, NOTINNOCENCE EXAMPLE3 · THESEARCHESTHATSHOWEDINTENT

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTION FOR A SYSTEM - ARTE FAC TANA LY SIS

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The system-artefact checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can you tell whether someone actually opened a file, not just that it was there? What is Knowledge C and why is it useful? There are no log entries for the period we care about. Does that clear our opponent? Can the artefacts show what someone searched for? How urgent is preserving the Mac for this kind of evidence? Do the artefacts prove who was using the machine?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 confidential it y 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 Knowledge C 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. cflab. u k · e-disc ove r y. u k

Source: https://e-discovery.uk/library/macos-system-artefacts. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.