COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Apple Mail Archives and Email Threading on macOS

Reconstructing the True Conversation from the Local Store and the Headers

Email remains the backbone of business evidence, and on a Mac, Apple Mail keeps a rich local archive of it: whole mailboxes downloaded and stored, complete with the technical headers that record how each message really travelled. For the lawyer, two things matter. First, the local archive frequently holds more than the live server, older mail, deleted messages, and the full headers that a simple print or forward strips away. Second, email is a conversation, and reconstructing the true thread, who said what, in what order, with which replies and forwards, from the message headers rather than from a party's tidy presentation, is often where the real story emerges, and where selective disclosure and doctored threads are exposed. This guide sets out for UK lawyers where Apple Mail keeps its archive, what the headers reveal, how a genuine thread is reconstructed and authenticated, and how email evidence is interpreted honestly and set in the wider estate.

⏱ 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. Email work on the Mac recovers the rich local Apple Mail archive, reads the technical headers that record how messages truly travelled, and reconstructs genuine threads from the header data rather than from a party's presentation, exposing selective disclosure and doctored chains. The analysis authenticates each message, sets the email in the wider estate, and is reported under CPR Part 35 and CrimPR Part 19 with the meaning and limits of headers explained.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | MAIL ARCHIVE & HEADER ANALYSIS | THREAD RECONSTRUCTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: Apple Mail keeps a rich local archive that often holds more than the live server, and email is a conversation whose true thread must be reconstructed from the technical headers rather than a party's presentation, which is where selective disclosure and doctored chains are exposed.

Where it lives (§3): Apple Mail stores whole mailboxes locally, with full messages, attachments and technical headers, frequently retaining more than the server, older, deleted and complete-header versions. **What headers reveal (§4):** the headers record how a message actually travelled, its true sender, route, timing and threading identifiers, information a print or forward strips away. **Thread reconstruction (§5):** the genuine conversation, who said what, in what order, with which replies and forwards, is rebuilt from the header threading data, not from a tidy presentation. **Authentication and limits (§6):** each message is authenticated from its headers, doctored or fabricated threads are exposed, and headers are read for what they reliably show. **Deployment (§7):** exposing selective disclosure, proving the real chain, and setting the email in the wider estate.

- **The thread is the evidence:** email is a conversation, and the true order and authorship matter.
- **The local archive holds more:** Apple Mail often retains older, deleted and full-header mail the server lacks.
- **Headers record the truth:** sender, route, timing and threading, stripped away by a print or forward.
- **Rebuild from headers, not presentation:** the genuine chain comes from the technical data.
- **Expose doctoring:** selective disclosure and fabricated threads are caught by header analysis.

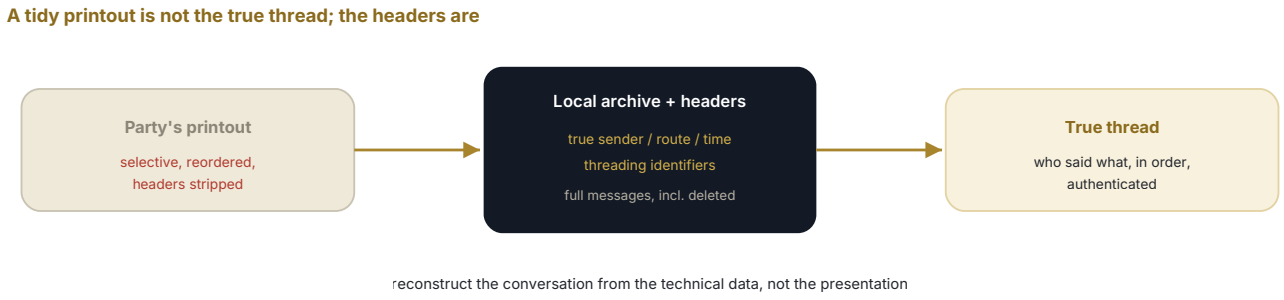

Figure 1 - a party's printout is selective and header-stripped; the true thread is rebuilt from the local archive and the technical headers that record how each message really travelled.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the thread is the evidence

Email is still the spine of business evidence, and it is rarely a single message. It is a conversation: an exchange of replies and forwards, often across many participants and over time, in which the meaning depends on who said what, in what order, and in response to what. That structure, the thread, is frequently the real evidence, and it is exactly what a party's presentation can distort. A printed-out email, a forwarded chain, a pasted excerpt, is easy to make selective: to drop the inconvenient reply, to reorder, to quote out of sequence, and, in the worst cases, to fabricate. And the very act of printing or forwarding strips away the technical information that would reveal the truth.

That technical information lives in two places on a Mac. Apple Mail keeps a local archive: whole mailboxes downloaded and stored on the machine, with the complete messages, their attachments, and, crucially, their full headers. The headers are the hidden part of every email, the record of how the message actually travelled, its true sender and route, its precise timing, and the identifiers that link it to the messages it replied to and that replied to it. From the local archive and these headers, an examiner can do what a party's presentation cannot: recover the complete messages, including older and deleted ones the live server may no longer hold, and reconstruct the genuine thread from the threading identifiers rather than from anyone's tidy account of it. This is where selective disclosure is exposed, a reply that was quietly omitted reappears, an out-of-order excerpt is put back in sequence, and a doctored or fabricated chain is caught by headers that do not add up. The discipline is to work from the archive and the headers, to reconstruct and authenticate the true conversation, and to read the headers honestly for what they show. This guide sets out where Apple Mail keeps its archive, what the headers reveal, how the real thread is rebuilt, and how email evidence is interpreted.

§ 0 3 · WHERE THE ARCHIVE LIVES

Where Apple Mail keeps its archive

- **Local mailbox stores:** Apple Mail downloading and storing whole mailboxes on the Mac, so complete messages, with attachments and full headers, sit locally, often a fuller record than the live server holds (guide 135): the local email archive.
- **Full messages and headers:** each stored message retaining its complete content and its technical headers, the information a print or forward discards, so the archive preserves what a presentation strips away (§4): the complete, header-bearing message.
- **Older and deleted mail:** the local store frequently retaining email since deleted from the server or the visible mailbox, and deleted items recoverable from remnants and snapshots (guides 4, 132): the mail that outlived deletion.
- **Attachments preserved:** the attachments to messages stored alongside, with their own metadata (guide 138), so the full content of an exchange, not just its text, is preserved: the attachments retained.
- **On the decrypted device and estate:** the archive recovered from the acquired, decrypted Mac (guides 131, 133), and corroborated across iCloud, paired devices, backups and the mail server (guides 135, 137), integrity preserved (guides 2, 3): the sound, corroborated basis.

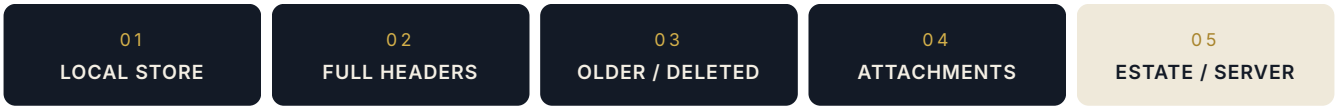

Figure 2 - Apple Mail's local archive holds complete, header-bearing messages, including older and deleted mail, corroborated across the estate and the server.

§ 0 4 · WHAT THE HEADERS REVEAL

What the headers reveal

- **True sender and route:** the headers recording the actual originating sender and the servers a message passed through, so the real source and path of an email, not just the display name, can be established (guide 129): the who-really-sent-it answer.
- **Precise timing:** the header timestamps recording when a message was sent and handled at each hop, so its true timing, reconciled for time zones (guide 108), can be established against any claimed date: the when answer.
- **Threading identifiers:** the message and reference identifiers that link a message to the one it replied to and the ones that replied to it, the technical basis for rebuilding the true thread (§5): the conversation's wiring.
- **Recipients and distribution:** the full set of recipients, including copied and blind-copied parties where recorded, so who actually received a message can be established, sometimes contradicting a party's account (§7): the who-received-it answer.
- **Authenticity signals:** the headers carrying signals, authentication results, server records, that bear on whether a message is genuine, so a fabricated or altered email can often be exposed (§6, guide 126): the genuineness signals.

§ 0 5 · RECONSTRUCTING THE THREAD

Reconstructing the true thread

- **Rebuild from threading identifiers:** the genuine conversation reconstructed from the header identifiers that link replies and forwards, so the true structure, not a party's arrangement, is established (§4): the thread wired back together.
- **Restore the true order:** the messages placed in their real chronological and reply order from the headers, so an out-of-sequence or reordered presentation is corrected (guide 96): the order put right.
- **Recover omitted messages:** replies and forwards omitted from a party's disclosure recovered from the archive and slotted into the thread, so a selectively pruned chain is completed (§7): the missing links restored.
- **Reconcile across mailboxes and parties:** the thread reconciled across the sender's and recipients' mailboxes and the estate, so each participant's copy corroborates the whole and gaps are exposed (guide 130): the thread cross-checked.
- **Present the genuine conversation:** the reconstructed thread presented as the true exchange, with each message authenticated and sourced, so the court sees the real conversation, not a curated version (§6): the honest thread.

§ 0 6 · AUTHENTICATION AND HONEST LIMITS

Authentication, doctored threads and honest limits

- **Authenticate from headers:** each message authenticated from its headers and the archive, so a genuine email is distinguished from an altered or fabricated one (guide 126): the genuineness established.
- **Expose doctored threads:** a fabricated or altered chain exposed where the headers do not add up, inconsistent identifiers, impossible timing, missing routing, so a doctored thread is caught (§4): the fabrication detected.
- **Headers can, rarely, be forged:** headers strong evidence but interpreted in context, since they can in unusual cases be forged or altered, so authenticity rests on the whole record, not one header alone (guide 126): the careful reading.
- **Display versus reality:** the display name and quoted text distinguished from the true header data, since a spoofed sender or a doctored quote is revealed only by the headers (guide 129): the appearance separated from the fact.
- **State findings honestly:** the thread, timing, authorship and authenticity expressed at the confidence the headers and archive support, distinguishing established fact from inference (guide 100): the honest email account.

§ 0 7 · DEPLOYMENT

Deployment: selective disclosure and the real chain

- **Exposing selective disclosure:** a party's pruned or reordered chain corrected by the reconstructed thread, so omitted replies and true sequence are restored and the selectivity exposed (§5): the curation undone.
- **Proving the real chain:** the genuine conversation established from the archive and headers, so what was actually said, by whom and when, is proved against a distorted account (guide 96): the true exchange proved.
- **Detecting fabricated email:** a fabricated or altered message exposed by header analysis, so a forged email offered as evidence is caught (guides 126, 129): the forgery detected.
- **Recovering deleted mail:** email a party deleted recovered from the local archive, remnants and snapshots, so a message believed gone is restored to the thread (guides 4, 132): the deleted mail recovered.
- **Honest, corroborated presentation:** the thread authenticated, sourced across the estate and presented at honest confidence, with headers explained, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the email evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the Apple Mail archive on a Mac is one copy of an email conversation that exists across many mailboxes and systems, and reconstructing and authenticating a thread depends on corroborating across them. The Mac holds the local archive, the full headers and deleted remnants. But iCloud and the paired devices (guide 135) hold synced copies of the same mail; the mail server holds its own copy and server-side logs that corroborate routing and timing; each other participant's mailbox holds their side of the thread, sender, recipients, copied parties; backups and snapshots (guides 132, 137) hold earlier states, including messages since deleted; and the wider estate ties the email to the events it concerns. The discipline is to reconstruct the thread not from one mailbox but across all available copies, so that an omitted or altered message in one is caught by its presence, or absence, in another, and so that headers are corroborated by server logs and counterpart copies. When a party has pruned their disclosure, the counterpart's mailbox or the server holds the missing messages; when mail has been deleted, the archive, a backup or a snapshot preserves it; and the multiple copies together authenticate the genuine thread and expose the doctored one.

EVIDENCE	MAC MAIL ARCHIVE	ICLOUD / PAIRED DEVICES	MAIL SERVER / LOGS	COUNTERPART MAILBOXES	BACKUPS / SNAPSHOTS	DELETED / RECOVERABLE
Message content	Y: full, local	Y: synced	Server copy	Y: their copy	Y: earlier state	Often (guide 4)
Headers / routing	Y: full headers	Y: synced	Y: server logs	Their headers	Earlier headers	With message
Thread structure	Y: identifiers	Synced	Server threading	Their thread	Earlier thread	Reconstructable
Recipients / distribution	Y: headers	Synced	Delivery logs	Y: who received	Earlier state	n/a
Deleted messages	Remnants	Recently deleted	Server retention	Their copy	Y: in backup	Y (multiple routes)

Fallback strategy in one line: reconstruct and authenticate the thread across all copies, the archive, server logs, counterpart mailboxes and backups, so an omitted, altered or deleted message in one is caught by another.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE REPLY THAT HAD BEEN QUIETLY DROPPED

A party disclosed an email chain that appeared to support their case, but the §5 thread reconstruction told the full story. Working from the §3 local Apple Mail archive and the §4 threading identifiers in the headers, the true conversation was rebuilt, and it contained a reply, omitted from the party's disclosure, that materially changed the meaning of the exchange. The omitted message was recovered from the archive and, per §8, corroborated in a counterpart mailbox and a backup. The §6 authentication confirmed the genuineness of the full thread. The party's curated chain had concealed the very message that mattered. The lesson is §2's: email is a conversation, and a party's presentation can quietly omit the inconvenient reply, but reconstructing the true thread from the local archive and the header identifiers restores the omitted messages and exposes the selectivity, so the court sees the real exchange rather than a pruned version of it.

EXAMPLE 2 · THE FABRICATED EMAIL CAUGHT BY ITS HEADERS

An email was produced that, on its face, supported a party's claim. The §6 authentication tested it rather than accepting it, and the §4 headers did not add up: the threading identifiers were inconsistent with the messages it purported to reply to, the routing was absent or impossible, and the timing conflicted with the server records (guides 126, 129). Corroboration across the §8 estate, the counterpart's mailbox and the mail server, held no trace of the message. The email was a fabrication, exposed not by its content, which looked plausible, but by the technical headers that a forger had not been able to make consistent. The lesson is §6's: a fabricated or altered email is caught by header analysis, because the headers record how a message truly travelled and a forgery rarely produces consistent, corroborated routing, threading and timing, so authenticating from the headers and the estate exposes a forged chain that a printout alone would never reveal.

EXAMPLE 3 · THE FULL HEADERS THE PRINTOUT HAD STRIPPED

A dispute turned on who had really sent a message and when. The party relied on a printout showing a particular display name and date, but the §4 header analysis of the archived message revealed the truth: the true originating sender and route differed from the display name (a spoofed or misattributed sender), and the precise header timing, reconciled for time zones (guide 108), differed from the printed date. The §3 local archive preserved the full headers that the printout had stripped away, and the §6 findings were stated at honest confidence and corroborated with server logs (§8). The reality, hidden in the headers, was not what the printout showed. The lesson is §4's: printing or forwarding an email strips away the headers that record how it truly travelled, so relying on a printout can mislead as to sender, timing and threading, and it is the full headers in the local archive, read carefully, that reveal what actually happened.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Trusting a party's presentation:** accepting a printed or forwarded chain as the true thread without reconstructing it (Example 1, §2).
- **Relying on printouts:** using header-stripped printouts that hide the true sender, timing and threading (Example 3, §4).
- **Not authenticating:** failing to test a produced email against its headers and the estate, missing a fabrication (Example 2, §6).
- **Ignoring the local archive:** relying on the server while overlooking the fuller local store (§3).
- **Missing omitted messages:** not recovering the replies a party pruned from the chain (Example 1, §5).
- **Reading display over headers:** taking the display name and quoted text as the truth rather than the header data (§6).
- **Not corroborating across mailboxes:** resting on one mailbox when counterparts and the server would confirm or refute (§8).
- **Overstating header certainty:** treating headers as infallible when they can, rarely, be forged (§6).

Technical limitations

- **Headers can be forged:** strong but not infallible, so authenticity rests on the whole corroborated record (§6, guide 126).
- **Printouts lose the evidence:** printing and forwarding strip headers, so native messages are needed (§4).
- **Deletion recovery is not guaranteed:** remnants may be overwritten, so prompt preservation matters (§3, guide 132).
- **Timing needs reconciliation:** header timestamps span time zones and must be normalised (§4, guide 108).
- **Mail apps evolve:** Apple Mail and its stores change across versions, checked per version (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Do we have the native email with full headers, or only printouts or forwards, so we know whether the true thread can be reconstructed?
- Is the concern a selectively disclosed chain, a disputed sender or timing, or a possible fabrication?
- Has the Mac and the estate been preserved promptly, so deleted mail and full headers survive?

Ask your opponent

- Please disclose the native email messages, with full headers, for the chain relied on, not printouts or forwards, across the Mac, iCloud, paired devices and server.
- Please confirm and disclose all messages in the thread, including replies and forwards, and any deleted messages.
- Please confirm the true sender, recipients and timing of the messages in issue.

Ask your eDiscovery / forensic provider

- What does the local archive hold, including deleted mail and full headers, beyond the party's presentation?
- What does the reconstructed thread show about order, authorship and omitted messages?
- Are the produced messages authentic, and does the estate corroborate them?

SUGGESTED WORDING · INSTRUCTION FOR A MAIL ARCHIVE AND THREADING ANALYSIS

> "We instruct you to recover and analyse the Apple Mail archive on the device at Schedule 1 and to reconstruct and authenticate the email thread(s) at Schedule 2. Please, on the acquired, decrypted device and preserving integrity: (1) recover the local Mail store, including full messages, attachments, technical headers, and older and deleted mail from remnants and snapshots; (2) read the headers to establish the true sender, route, precise timing (reconciled for time zones), recipients and threading identifiers of each message; (3) reconstruct the genuine thread from the threading identifiers, restoring the true order and any replies or forwards omitted from a party's presentation, and reconcile it across the sender's and recipients' mailboxes and the estate; (4) authenticate each message from its headers and the corroborating record, exposing any doctored or fabricated chain where the headers do not add up, while recognising that headers can rarely be forged and must be read in context; and (5) distinguish display data from the true header data, and state thread, timing, authorship and authenticity at honest confidence, working from native messages rather than printouts."

§ 12 · QUICK CONTROL

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

The Mail archive and threading checklist

- ☐ Mac and estate preserved promptly; deleted mail and headers intact
- ☐ Local Mail archive recovered, with full headers and attachments
- ☐ Older and deleted mail recovered from remnants and snapshots
- ☐ True sender, route, timing and recipients read from headers
- ☐ Thread reconstructed from threading identifiers
- ☐ True order restored; omitted replies and forwards recovered
- ☐ Thread reconciled across mailboxes and the estate
- ☐ Each message authenticated; doctored or fabricated chains exposed
- ☐ Display data distinguished from true header data
- ☐ Findings stated at honest confidence, from native messages

Red flags

- A party's printout accepted as the true thread: Example 1.
- Reliance on header-stripped printouts: Example 3.
- A produced email not authenticated against its headers: Example 2.
- The local archive and deleted mail overlooked.
- Omitted replies not recovered.
- Display name and quoted text taken as the truth.
- Headers treated as infallible or not corroborated.

When to involve a digital forensic expert

Whenever an email chain matters and there is any question of selectivity, sequence, authorship or authenticity, because the true thread is reconstructed from technical data a party's presentation strips away: the expert recovers the rich local Apple Mail archive, with full messages, headers, attachments and deleted mail (§3), reads the headers to establish the true sender, route, timing and recipients (§4), and rebuilds the genuine thread from the threading identifiers, restoring the true order and the replies a party omitted (Example 1, §5). Each message is authenticated from its headers and the corroborating estate, so a doctored or fabricated chain is exposed where the headers do not add up (Example 2, §6), and display data is never mistaken for the true header data (Example 3). The thread is reconciled across mailboxes, server logs and backups (§8), and reported at honest confidence, from native messages rather than printouts, under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, Mail archive and threading work recovers the true conversation from the local store and the headers, exposing the selective disclosure, the doctored chain and the fabricated email that a tidy printout is designed to hide.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Why not just rely on the printed email chain?

Because a printout hides the very evidence that matters (§4, Example 3). Printing or forwarding an email strips away its headers, the record of how it truly travelled, so a printout can mislead as to the real sender, the precise timing and the thread structure, and it is easy to make a printed chain selective or reordered. The native messages, with their full headers, preserved in Apple Mail's local archive, are what allow the true sender, timing and conversation to be established, so native email, not printouts, is worked from.

What are email headers, and why do they matter?

They are the hidden technical record in every email (§4). Headers record the true originating sender and the servers a message passed through, its precise timing at each hop, its full set of recipients, and the identifiers that link it to the messages it replied to and that replied to it. This is the information needed to establish who really sent a message, when, to whom, and where it sits in a conversation, and to authenticate it. Because a print or forward discards the headers, the archived native message is essential.

Can you rebuild the true conversation from a messy exchange?

Yes, from the threading identifiers (§5, Example 1). Every email carries identifiers linking it to the message it replied to and the ones that replied to it, so the genuine thread, who said what, in what order, with which replies and forwards, can be reconstructed from that technical wiring rather than from a party's arrangement. This restores the true sequence and, crucially, recovers replies a party may have omitted, so a selectively pruned or reordered chain is corrected and the real exchange revealed.

Can you tell if an email has been faked?

Often yes (§6, Example 2). A fabricated or altered email is caught by analysing its headers and corroborating across the estate: a forgery rarely produces consistent, corroborated routing, threading and timing, so inconsistent identifiers, impossible timing or absent routing, and the absence of any trace in counterpart mailboxes or server logs, expose it. Headers are strong but not infallible, since they can rarely be forged, so authenticity rests on the whole corroborated record, not a single header, but header analysis frequently reveals a fake a printout would hide.

Does the local archive have more than the server?

Frequently (§3). Apple Mail downloads and stores whole mailboxes locally, so the archive often retains email that has since been deleted from the server or the visible mailbox, along with the full headers and attachments, and deleted messages can be recovered from remnants and snapshots (guide 132). So the local archive is regularly a fuller record than the live server, which is why it is recovered and examined, and corroborated across iCloud, paired devices, backups and the server for the complete picture.

How quickly should we preserve the Mac and mailboxes?

Promptly (§3, §8). Deleted email survives in remnants and snapshots only until overwritten by continued use, server retention is finite, and synced copies can change, so the sooner the Mac, the estate and the relevant mailboxes are preserved, the more of the archive, its deleted mail and its full headers survive. Preserving the counterparts' mailboxes and the server logs early also secures the corroboration needed to reconstruct and authenticate the thread. As with Mac work generally (guide 131), speed protects the evidence.

§ 14 · REFERENCE

Glossary

Local mail archive
Whole mailboxes stored on the Mac by Apple Mail.

Header
The technical record of how an email travelled.

Threading identifier
Header data linking replies and forwards.

Thread
The genuine sequence of a conversation.

Routing
The servers a message passed through.

True sender
The actual originator, not the display name.

Selective disclosure
A pruned or reordered chain.

Doctored thread
An altered or fabricated chain.

Native message
The original email with headers, not a printout.

Authentication
Establishing whether an email is genuine.

Sources and authoritative references

The email-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 (Mail archive and header analysis, thread reconstruction, email authentication, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 05 · Processing and Phase 07 · Review (email threading and analysis as practised): e-discovery.uk/edrm/processing · e-discovery.uk/edrm/review
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- IETF RFC 5322 (Internet Message Format, email headers) and related standards: rfc-editor.org, RFC 5322 · Apple Platform Security guide: support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (authentication and honest reporting): 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

Email work at the laboratory recovers the true conversation from the technical data a party's presentation strips away. On the acquired, decrypted Mac (guides 131, 133), the rich local Apple Mail archive is recovered, with full messages, attachments and, crucially, the complete headers, including older and deleted mail from remnants and snapshots that the live server no longer holds (§3). The headers are read to establish the true originating sender and route, the precise timing reconciled for time zones, the full set of recipients, and the threading identifiers, so who really sent what, when and to whom is established, not the display name a printout shows (Example 3, §4). The genuine thread is reconstructed from those identifiers, restoring the true order and recovering the replies and forwards a party has omitted, so selective disclosure is exposed and the real exchange revealed (Example 1, §5). Each message is authenticated from its headers and corroborated across the estate, the counterpart mailboxes and the server logs, so a doctored or fabricated chain is caught where the headers do not add up (Example 2, §6). Everything is worked from native messages rather than printouts, distinguished display data from header fact, and reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide sits within the macOS user-data run of the Apple block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the governing point is that email is a conversation, and only the archive and the headers reveal what it truly was.

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