COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iMessage, SMS and Messaging Apps on iOS

Where the Conversations Really Live, and Why Deletion, Edits and Encryption Change What You See

Messaging is where the most important evidence on a phone usually sits. On an iPhone the conversations run through several channels at once: Apple's own iMessage and the ordinary SMS text service, both handled by the Messages app, and a crowd of third-party apps, WhatsApp, Signal, Telegram, Messenger and more, each storing its data differently. For the lawyer, three realities shape what can be recovered and how far it can be trusted. Deleted messages frequently survive in the app databases, in backups and across the estate, so a party's deletions rarely erase the record. Messages can be edited or unsent, so what appears now may not be what was originally sent. And some apps are end-to-end encrypted, which limits interception but not necessarily recovery from the endpoints. This guide sets out for UK lawyers where iOS messaging data lives, what survives deletion, how edits, unsending and encryption affect the evidence, and how messaging is recovered, attributed 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. Messaging recovery is central to its mobile work: extracting iMessage, SMS and third-party app conversations from the phone's databases, recovering deleted messages from remnants, backups and the estate, and interpreting edits, unsending and end-to-end encryption honestly. The analysis attributes conversations with care and is reported under CPR Part 35 and CrimPR Part 19, so the record a party believes they have erased or altered is recovered and read for what it truly shows.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | IMESSAGE, SMS & APP MESSAGING | DELETED-MESSAGE RECOVERY | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: an iPhone carries conversations across iMessage, SMS and many third-party apps, each storing data differently, and three realities govern the evidence, deleted messages frequently survive, messages can be edited or unsent, and some apps are end-to-end encrypted, which limits interception but not recovery from the endpoints.

Where it lives (§3): iMessage and SMS in the Messages app database, and third-party apps (WhatsApp, Signal, Telegram, Messenger) each in their own stores, all on the phone and often in backups and the estate. **What survives (§4):** deleted messages frequently persist in app database remnants, recently-deleted areas, backups and counterpart devices, so deletion rarely erases the record. **Edits and encryption (§5):** messages can be edited or unsent, so the current view may differ from what was sent, and end-to-end encryption limits interception in transit but not recovery from the sender's or recipient's device. **Attribution (§6):** conversations attributed to accounts and people with care, and interpreted honestly. **Deployment (§7):** recovering and proving conversations, including deleted and altered ones, across the estate.

- **Many channels, one phone:** iMessage, SMS and third-party apps each store messaging differently.
- **Deleted often survives:** messages persist in databases, backups, snapshots and counterpart devices.
- **Edits and unsending matter:** the current view may not be what was originally sent.
- **Encryption limits interception, not endpoints:** end-to-end apps are still recoverable from the device.
- **Attribute with care:** a message is from an account; tying it to a person needs corroboration.

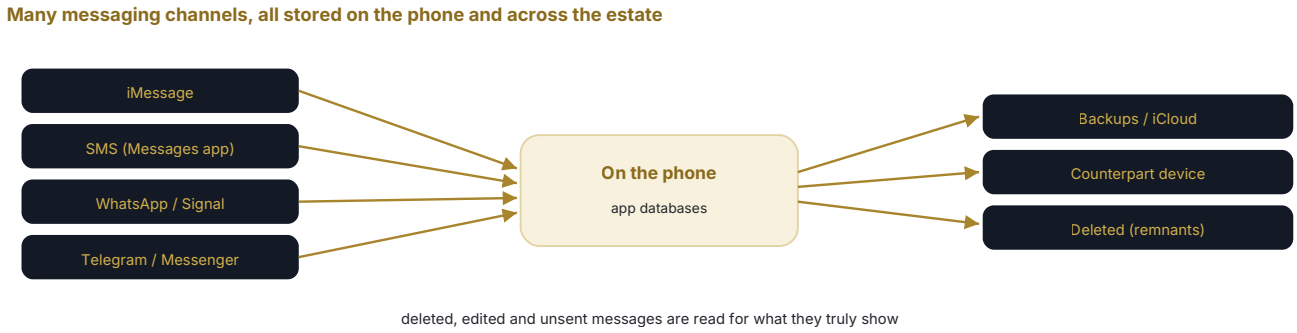

Figure 1 - iMessage, SMS and third-party apps each store conversations on the phone, replicated across backups, iCloud and counterpart devices, so deletion rarely erases the record.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: many channels, one phone

When a dispute turns on what someone said, the messages are usually the heart of it, and on an iPhone those messages do not travel through a single channel. Apple's own iMessage service and the ordinary SMS text service are both handled by the Messages app, which stores them together in its own database. Alongside that sit a crowd of third-party messaging apps, WhatsApp, Signal, Telegram, Messenger and others, each of which keeps its own data in its own way. So the first task is simply to recognise that a person's conversations are spread across several channels, each with different storage, different features and different recovery characteristics, and that examining one while ignoring the others can miss most of the story.

Three realities then shape what can be recovered and how far it can be trusted, and each must be understood. First, deletion is rarely final. Messages a party has deleted frequently survive, in the free space and remnants of the app databases, in recently-deleted areas, in backups and snapshots (guides 132, 147), and on the devices of the people they were talking to. A deleted conversation is very often recoverable. Second, messages are no longer fixed once sent. Modern messaging supports editing and unsending, so what appears in a conversation now may not be what was originally sent, and an apparent history may have been altered, which the analysis must account for rather than take at face value. Third, encryption changes what is possible but not always in the way people assume. Several apps are end-to-end encrypted, which means the messages cannot readily be intercepted in transit, but that is a limit on interception, not on recovery: the messages are still present, decrypted, on the sender's and recipient's own devices, and can usually be recovered from those endpoints. The discipline, then, is to cover all the channels, to recover deleted material, to interpret edits and unsending honestly, to understand what encryption does and does not prevent, and to attribute conversations to people with care. This guide sets out where iOS messaging lives, what survives, how edits and encryption affect the evidence, and how it is recovered and read.

§ 0 3 · WHERE IT LIVES

Where iOS messaging data lives

- **iMessage and SMS together:** the Messages app storing both Apple's iMessage and ordinary SMS texts in a single local database, with participants, timing and attachments, so the core conversation record sits in one place on the phone (§5): the Messages store.
- **Third-party app stores:** WhatsApp, Signal, Telegram, Messenger and others each keeping their own databases and media on the phone, so every installed messaging app is examined, not just Messages (guide 146's completeness point): the app-by-app record.
- **Attachments and media:** the images, videos, voice notes and files sent in conversations stored alongside or within the app data, so the full content, not just the text, is recovered (guide 138): the media of the conversation.
- **Depth matters:** the completeness of a given app's history depending on extraction depth (guide 146), so a full-file-system acquisition often reaches app data a logical extraction misses: the depth-dependent record.
- **On the decrypted device and estate:** the messaging data recovered from the acquired, decrypted phone and corroborated across backups, iCloud and counterpart devices (guides 147, 130), integrity preserved (guides 2, 3): the sound, corroborated basis.

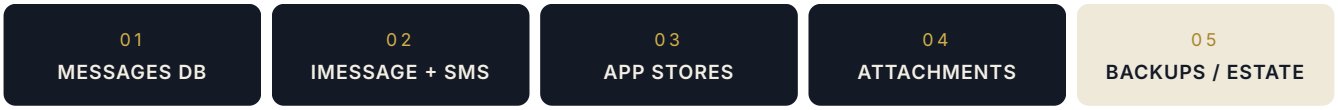

Figure 2 - iOS messaging spans the Messages database (iMessage and SMS) and each third-party app's own store, with attachments, all corroborated across the estate.

§ 0 4 · WHAT SURVIVES DELETION

What survives deletion

- **Deleted messages in databases:** deleted messages frequently persisting in the free pages and remnants of the app databases, so a conversation a party deleted can often be reconstructed from the database itself (guide 4): the message that outlived deletion.
- **Recently-deleted areas:** Messages and some apps retaining recently-deleted items for a period before final removal, an easy and reliable recovery source (§7): the grace-period copy.
- **Backups and snapshots:** backups and APFS snapshots (guides 132, 147) preserving earlier states, so messages deleted since a backup survive intact within it, and a backup can be compared to date a deletion (guides 109, 137): the preserved prior state.
- **The counterpart device:** the other party to a conversation holding their copy, so a message deleted on one phone survives on the other, reachable by disclosure (guide 130): the other side of the exchange.
- **Depth reaches more:** a full-file-system extraction reaching deleted app data a logical extraction never sees, so a matter turning on deleted messages needs the deeper method (guide 146): the deletion divide.

§ 0 5 · EDITS, UNSENDING AND ENCRYPTION

Edits, unsending and end-to-end encryption

- **Editing changes the record:** Messages and some apps allowing a sent message to be edited, so the current text may differ from the original, and traces of the earlier version may survive in the database and be recoverable (guide 4): the edited message read carefully.
- **Unsending removes from view:** a sender able to unsend a message, removing it from the visible conversation, though remnants of an unsent message may persist in the database or on the counterpart device (§4): the unsent message that may still be traced.
- **End-to-end encryption limits interception:** apps like Signal, WhatsApp and iMessage encrypting messages so they cannot readily be intercepted in transit, a limit on interception, not on the messages themselves (§2): the in-transit protection.
- **The endpoints still hold the messages:** the messages present, decrypted, on the sender's and recipient's own devices, so end-to-end encryption does not prevent recovery from those endpoints (guide 133's on-device theme): the endpoint recovery.
- **Ephemeral and disappearing messages:** some apps offering disappearing messages that limit what survives, an honest limit, though traces, notifications and counterpart copies may remain (guide 100): the vanishing message and its limits.

§ 0 6 · ATTRIBUTION AND HONEST LIMITS

Attribution, interpretation and honest limits

- **Account, not person:** a message coming from an account or number, so attributing it to a person needs care, especially where a device or account may be shared (guide 105): the who-sent-it question kept honest.
- **Reconstruct the true conversation:** messages reassembled into their conversations with participants, timing and reply structure, so the exchange reads as it happened, not as fragments or a party's arrangement (guides 96, 143): the conversation restored.
- **Edits and unsending flagged:** the record read with an understanding of edits and unsending, so an altered history is not taken at face value and any recovered original is distinguished from the current text (§5): the honest reading of an editable record.
- **Deletion in context:** a deletion established and dated, and its significance assessed, routine or deliberate, and against any duty to preserve (guides 4, 110): the deletion read in context.
- **State confidence plainly:** content, timing, attribution and completeness expressed at the confidence the recovered data supports, distinguishing established fact from inference (guide 100): the honest messaging account.

§ 0 7 · DEPLOYMENT

Deployment: recovering and proving conversations

- **Proving what was said:** recovered conversations establishing the content of communications in contract, fraud, employment, harassment and family matters, including messages a party deleted and believed gone (guides 4, 98): the communication proved.
- **Proving timing and sequence:** the metadata dating messages and placing them in sequence, so who said what, when, and in what order is established on a timeline (guides 96, 130): the chronology of the exchange.
- **Exposing deletion and alteration:** deleted or edited messages recovered against a party's account or disclosure, so a pruned or altered chain is corrected and the selectivity exposed (guides 98, 143): the concealment undone.
- **Reaching end-to-end apps from the device:** conversations in encrypted apps recovered from the endpoints where interception was impossible, so encryption does not shield the record (§5): the encrypted app opened at the device.
- **Corroborated, honest presentation:** the conversations corroborated across the phone, backups, iCloud and counterpart devices, and presented at honest confidence with attribution stated, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the messaging evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a conversation on an iPhone exists in more than one place, which is exactly why deletion, unsending and encryption so rarely erase it. The phone holds the Messages database and each app's store, including deleted remnants. But backups (iTunes/Finder and iCloud, guide 147) hold copies and prior states, and an encrypted backup holds more; iCloud holds synced Messages and app data; the paired Mac and iPad (guides 131, 135) hold the same conversations through continuity and sync; APFS snapshots (guide 132) hold earlier states; the counterpart devices of the other parties hold their side of every exchange; and the app providers and carriers hold their own limited records. The discipline is to reconstruct a conversation across all available copies, so that a message deleted, unsent or edited on one device is caught by its presence, or its earlier form, in another, and so that an end-to-end-encrypted app, impervious to interception, is still recovered from an endpoint. When a message is deleted from the phone, the counterpart, a backup or a snapshot holds it; when a conversation is unsent, the counterpart device or a remnant may retain it; and the multiple copies together reconstruct the genuine exchange.

EVIDENCE	THE PHONE	BACKUPS (INCL. ENCRYPTED)	ICLOUD / SYNC	PAIRED MAC / IPAD	COUNTERPART DEVICE	DELETED / RECOVERABLE
iMessage / SMS	Y: Messages db	Y: in backup	Y: if synced	Y: same threads	Y: their copy	Often (guide 4)
App messages	Y: app stores	Varies / more if encrypted	Varies	Some synced	Y: their copy	Often (remnants)
Attachments / media	Y: stored	Y: in backup	Y: synced	Y: synced	Y: their copy	Varies
Edited / original	Current + remnants	Earlier state in backup	Synced current	Device copy	Their received version	Original may survive
Unsent / deleted	Remnants	Pre-deletion backup	n/a	Device remnants	Y: often retained	Y (multiple routes)

Fallback strategy in one line: reconstruct the conversation across the estate; when a message is deleted, unsent or edited on the phone, the counterpart device, a backup, a snapshot or iCloud usually holds it or its earlier form.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DELETED CONVERSATION THE DATABASE KEPT

A party deleted an incriminating iMessage conversation before their phone was examined and assumed it was gone. The §4 recovery proved otherwise: the deleted messages survived in the free pages and remnants of the Messages database and were reconstructed in full, with participants, timing and attachments (guide 4), and the §8 estate corroborated them, the same conversation was present in an encrypted backup (guide 147) and on the counterpart's device. The §6 attribution was handled with care and was clear on the account. The deletion had not erased the record. The lesson is §4's: deleted messages frequently survive in the app databases, in backups and on counterpart devices, so a conversation a party deletes is very often recoverable and reconstructable against their expectation, provided the phone and estate are preserved before the remnants are overwritten.

EXAMPLE 2 · THE EDITED MESSAGE AND THE ORIGINAL BENEATH IT

A message relied on by one party appeared, in the current conversation, to say something helpful to them. The §5 edit analysis changed the picture: the message had been edited after sending, and a trace of the original text survived in the database (guide 4), showing that the original had said something materially different. The §8 counterpart device held the originally-received version, corroborating the recovered original. The §6 interpretation distinguished the current text from the recovered original and stated both at honest confidence. What the current view showed was not what had first been sent. The lesson is §5's: messages can be edited after sending, so the current text may not be the original, and recovering the earlier version from the database or the counterpart device, and distinguishing it from the current text, is essential to an honest account of what was actually said.

EXAMPLE 3 · THE END-TO-END APP OPENED AT THE ENDPOINT

Key conversations had taken place in an end-to-end-encrypted app, and one party argued that the encryption meant they could not be produced. The §5 endpoint principle answered this: end-to-end encryption prevents interception in transit, but the messages sit decrypted on the participants' own devices, and a §3 extraction of the app's store on the phone recovered the conversations in full (guide 133). The §8 estate corroborated them from the counterpart device. The encryption had protected the messages in transit but not on the endpoints where they lived. The lesson is §5's: end-to-end encryption limits interception, not recovery from the device, so conversations in encrypted apps are routinely recovered from the sender's or recipient's own phone, and a claim that encryption shields the record from disclosure misunderstands what that encryption actually protects.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Examining only one channel:** looking at Messages while ignoring the third-party apps that hold much of the conversation (§2, §3).
- **Assuming deletion is final:** treating a deleted conversation as gone, ignoring databases, backups and counterpart devices (Example 1, §4).
- **Taking the current text at face value:** not accounting for edits and unsending that changed the record (Example 2, §5).
- **Thinking encryption blocks recovery:** assuming an end-to-end app cannot be produced, when the endpoints hold the messages (Example 3, §5).
- **Shallow extraction missing app data:** a logical extraction relied on where a full-file-system one was needed for deleted app messages (§4, guide 146).
- **Attributing to a person carelessly:** a message from an account treated as certainly from an individual on a shared device (§6).
- **Not corroborating across the estate:** a conversation rested on one device when the counterpart or a backup would confirm it (§8).
- **Ignoring attachments:** recovering text but not the media that is often the point of the exchange (§3).

Technical limitations

- **Recovery is not guaranteed:** remnants may be overwritten with use, so prompt preservation matters (§4, guide 132).
- **Disappearing messages limit survival:** ephemeral messages may leave little, though traces and counterpart copies can remain (§5).
- **Edits can obscure history:** an original may not always be recoverable, so the current text is read with that caveat (§5).
- **Account is not identity:** the record shows account activity; attributing it to a person needs care (§6, guide 105).
- **Apps evolve rapidly:** messaging apps and their storage change constantly, so behaviour is checked per app and version (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which channels carry the relevant messages, iMessage, SMS, or which third-party apps, so all of them are examined?
- Might messages have been deleted, edited or unsent, and has the phone and estate been preserved promptly?
- Is the deeper extraction needed for deleted app data, and is the counterpart device available?

Ask your opponent

- Please preserve and disclose the messaging data on the device at Schedule 1, across iMessage, SMS and all third-party apps, including deleted, edited and unsent messages, and any backups, iCloud data and paired devices.
- Please confirm whether relevant messages have been deleted, edited or unsent, and when, and disclose any recovered originals.
- Please confirm the accounts and numbers involved and their attribution.

Ask your eDiscovery / forensic provider

- What conversations, across all channels, does the phone hold, including deleted and edited ones?
- How is the record corroborated across backups, iCloud and counterpart devices, and any deletion or edit assessed?
- What can and cannot be recovered, including end-to-end and ephemeral apps, and at what confidence?

SUGGESTED WORDING · INSTRUCTION FOR AN IOS MESSAGING ANALYSIS

> "We instruct you to recover and analyse the messaging on the device at Schedule 1, relevant to Schedule 2, across all channels. Please, on the acquired, decrypted device and preserving integrity: (1) recover the Messages database (iMessage and SMS) and the stores of all third-party messaging apps (including WhatsApp, Signal, Telegram and Messenger), with attachments, obtaining the extraction depth needed to reach deleted app data; (2) recover deleted, edited and unsent messages from database remnants, recently-deleted areas, backups and APFS snapshots, and distinguish any recovered original from the current text; (3) reconstruct each conversation with participants, timing and reply structure, and treat end-to-end-encrypted apps as recoverable from the device notwithstanding that they resist interception; (4) attribute conversations to accounts and, with corroboration, to people, and assess any deletion, edit or unsend in context and against any duty to preserve; and (5) corroborate across backups, iCloud, paired and counterpart devices, and state content, timing, attribution and completeness at honest confidence, noting the limits of ephemeral messaging."

§ 12 · QUICK CONTROL

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

The iOS messaging checklist

- ☐ All channels identified: iMessage, SMS and every third-party app
- ☐ Phone and estate preserved promptly; remnants intact
- ☐ Messages database and app stores recovered, with attachments
- ☐ Extraction depth sufficient for deleted app data
- ☐ Deleted, edited and unsent messages recovered
- ☐ Recovered originals distinguished from current text
- ☐ End-to-end apps recovered from the endpoint
- ☐ Conversations reconstructed and corroborated across the estate
- ☐ Deletion, edits and unsends assessed in context
- ☐ Attribution handled with care; confidence stated honestly

Red flags

- Only one channel examined; third-party apps ignored: §3.
- A deleted conversation assumed gone: Example 1.
- The current text taken as the original despite editing: Example 2.
- An end-to-end app treated as unrecoverable: Example 3.
- A shallow extraction relied on for deleted app data.
- An account message attributed to a person without corroboration.
- Attachments or counterpart devices overlooked.

When to involve a digital forensic expert

Whenever messaging matters, and promptly, because deleted remnants are overwritten and app data is depth-dependent: the expert recovers the Messages database and every third-party app store, with attachments, at the depth needed to reach deleted material (§3, guide 146), and reconstructs deleted, edited and unsent messages from remnants, backups and snapshots, distinguishing any recovered original from the current text (Examples 1 and 2, §4, §5). End-to-end-encrypted apps are recovered from the endpoints, where the messages sit decrypted, so encryption does not shield the record (Example 3). Conversations are attributed with care, assessed in context, corroborated across the phone, backups, iCloud and counterpart devices, and reported at honest confidence under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, messaging work recovers the conversations that decide so many cases across every channel a phone carries, so that a party's deletions, edits and unsending, and even end-to-end encryption, rarely manage to keep the true exchange from the court.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Someone deleted a conversation. Can it be recovered?

Frequently yes (§4, Example 1). Deleted messages often persist in the free pages and remnants of the app databases, in recently-deleted areas, in backups and snapshots, and on the counterpart's device. So a conversation a party deleted can usually be reconstructed, with participants, timing and attachments, provided the phone and estate are preserved before the remnants are overwritten. A full-file-system extraction reaches deleted app data a logical one cannot, so the deeper method is used where deletion is in issue.

A message was edited. Can you see the original?

Often yes (§5, Example 2). Because editing changes a sent message, the current text may differ from the original, but a trace of the earlier version frequently survives in the database and can be recovered, and the counterpart's device may hold the originally-received version. The analysis distinguishes the current text from any recovered original and states both at honest confidence. So an edited message is not simply taken at face value; the original is sought and, where found, presented alongside the current text.

The messages are in an end-to-end-encrypted app. Doesn't that stop recovery?

No, it stops interception, not recovery (§5, Example 3). End-to-end encryption means the messages cannot readily be intercepted in transit, but they sit decrypted on the sender's and recipient's own devices, so an extraction of the app's store on the phone recovers them in full. A claim that an encrypted app cannot be produced misunderstands what the encryption protects: the record lives, readable, at the endpoints, and is recovered from there like any other messaging.

Do we need to look at apps other than Messages?

Yes, always (§2, §3). People spread their conversations across iMessage, SMS and many third-party apps, WhatsApp, Signal, Telegram, Messenger, each storing data differently, so examining only the Messages app can miss most of the exchange. Every installed messaging app is recovered and examined, with its attachments. Which apps matter depends on the case, but the discipline is to cover all the channels a phone carries rather than assume the relevant messages are in one place.

Does a message prove who sent it?

It shows the sending account or number; attributing it to a person takes care (§6, guide 105). A device or account may be shared, so a message is attributed to the account first and to a person only with corroboration, other artefacts, the estate, surrounding evidence. Edits and unsending also mean an apparent history may be partial or altered. So content and attribution are stated at honest confidence, distinguishing what is certain from what is inferred, rather than assuming the account holder personally sent every message.

What about disappearing messages?

They limit what survives, and that is stated honestly (§5). Some apps offer disappearing or ephemeral messages designed to leave little behind, so recovery of their content may be limited, an honest limit rather than a guarantee of nothing. Even so, traces, notifications, remnants and the counterpart's copies can sometimes remain, so the possibility is examined rather than dismissed. Where ephemeral messaging genuinely leaves no recoverable content, that is acknowledged plainly rather than overstated in either direction.

§ 14 · REFERENCE

Glossary

iMessage
Apple's messaging service, handled by the Messages app.

SMS
Ordinary text messaging, also in the Messages app.

Messages database
The local store of iMessage and SMS.

Third-party app
WhatsApp, Signal, Telegram, Messenger and others.

End-to-end encryption
Encryption preventing interception in transit.

Endpoint
The sender's or recipient's device, where messages sit decrypted.

Edit / unsend
Changing or removing a sent message.

Ephemeral message
A disappearing message that limits survival.

Remnant
Deleted data recoverable from a database or free space.

Attribution
Linking a message to a real person.

Sources and authoritative references

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

- cflab.uk, digital forensics services (iMessage, SMS and app messaging recovery, deleted-message analysis, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 06 · Analysis (message recovery and reconstruction as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple Platform Security guide (iMessage and Messages data protection, end-to-end encryption): support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (recovery, interpretation and honest reporting): gov.uk, FSR Code · ISO/IEC 27037: iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35 · UK GDPR (proportionate handling of communications data): justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · ico.org.uk

DISCLAIMER

This publication provides general information about iOS messaging forensics as at August 2026. Messaging apps, their storage and their features change constantly, and the recoverability of deleted, edited or unsent messages depends on the device, the app, the extraction depth and the survival of remnants and backups; end-to-end encryption limits interception but not recovery from the endpoints, and ephemeral messaging may leave little. Communications data must be handled proportionately under the UK GDPR. 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

Messaging work at the laboratory recovers the conversations that decide so many cases, across every channel a phone carries and against a party's attempts to erase or alter them. On the acquired, decrypted device (guides 131, 133), the Messages database, iMessage and SMS together, and the stores of every third-party app, WhatsApp, Signal, Telegram, Messenger, are recovered with their attachments, at the extraction depth needed to reach deleted app data (guide 146). Deleted, edited and unsent messages are reconstructed from database remnants, recently-deleted areas, backups and snapshots, with any recovered original distinguished from the current text (Examples 1 and 2), and end-to-end-encrypted apps are recovered from the endpoints where the messages sit decrypted, because that encryption limits interception, not recovery from the device (Example 3). Every conversation is reconstructed with its participants, timing and reply structure, attributed to accounts and, with corroboration, to people, assessed in context for any deletion, edit or unsend, and corroborated across the phone, backups, iCloud, and paired and counterpart devices. Communications are handled proportionately under the UK GDPR and reported at honest confidence, with the limits of ephemeral messaging noted, under CPR Part 35 or CrimPR Part 19. This guide sits within the iPhone and iPad block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the recurring reassurance is that on an iPhone, who said what, and when, is far more often recoverable than a party's deletions, edits or encryption would suggest.

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