SMS And IMessage Evidence

This guide explores the complexities of SMS and iMessage evidence, detailing message databases, cloud sync, and deleted layers. It covers timestamps, attribution, and recovery realities, offering insights for UK litigators, in-house counsel, and investigators.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/sms-and-imessage-evidence

SMS & I MESSAGE EVIDENCE · A GUIDE FOR UK LAWYERS SMS and i Message Evidence Message Databases, Cloud Sync, Deleted Threads, Timestamps and Attribution on the Phone's Native Channels COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES MESSAGE-DATABASE FORENSICS CLOUD & BACKUP ARCHAEOLOGY CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: two services in one inbox 03 The stores: message databases and their deleted layers 04 iMessage's ecosystem: sync, devices and backup lineages 05 SMS's ecosystem: carriers, o per at or records and RCS 06 Deletion and recovery: windows, propagation, realities 07 Timestamps, attribution and authentication 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 THE HEADLINE POINT: ONEINBOX, TWOARCHITECTURES: ANDTHEARCHITECTURE DECIDESWHERETHEEVIDENCELIVESANDHOWITDIES

§ 02 · FIRST PRINCIPLES The problem in plain English: two services in one inbox

§ 03 · THESTORES The stores: message databases and their deleted layers

§ 04 · THEAPPLEECOSYSTEM iMessage's ecosystem: sync, devices and backup lineages

§ 05 · THECARRIERSIDE SMS's ecosystem: carriers, o per at or records and RCS

§ 06 · GONE, ANDBACK Deletion and recovery: windows, propagation, realities

§ 07 · STANDINGUP Timestamps, attribution and authentication 63) applied natively: the checkmate for contested threads.

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE DEVICE DEVICES (SYNC/ PRIMARY PEER ICLOUD (FFS) (MAC, IPAD) BACKUPS) COMPUTER COUNTERPART DELETED / BACKUPS + O PER AT OR RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEMACTHATREMEMBEREDTHERESIGNATION EXAMPLE2 ·

THEWINDOWTHATCAUGHTTHEWEEKENDEDIT EXAMPLE3 · THEOPERATORRECORDSTHATOUTLIVEDBOTHPHONES

§ 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 · N AT IVE - CHANNELLIMBFORTHEPRESER VAT I ON LETTER

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

§ 13 · COMMON QUESTIONS Frequently asked questions Can deleted texts be recovered? Can we get message content from the phone companies? Someone unsent a message. Is it gone? How do we prove who actually sent a text from a shared or accessible phone? The thread mixes green and blue bubbles. Does the analysis change mid-conversation? What single step best protects a native-channel case this week?

§ 14 · REFERENCE Glossary RCS. Sources and authoritative references 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides 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 deleted texts be recovered?

Walk the ladder: the recently-deleted window (about 30 days: routinely yes); the database layer at FFS (yes while unvacuumed); backup lineages bracketing the deletion (yes where habits existed); out-of-sync peers (Example 1's answer); counterpart devices (their copy, regardless). A disciplined deleter can defeat all five: rarely does: and the deletion's own chronology survives in any event. The realistic answer, most cases: substantially, if extraction moves early.

Can we get message content from the phone companies?

No: UK operators retain traffic data (numbers, times, cell context) on limited schedules, not content: Example 3 shows what the traffic spine can none the less prove. Content lives at the ends: devices, backups, counterparts: and for i Message the o per at or holds nothing at all (Apple-carried, not carrier-borne). The advice pairing: o per at or requests early for events; device work for words.

Someone unsent a message. Is it gone?

Rarely cleanly: the unsend window is short; recipients on older systems keep the message outright; not if i c at i on residue captures first lines; the sender's own store carries the unsend event with residue; and any backup or peer syncing before the unsend holds the original. The feature is loud: the attempt is usually easier to prove than the message would have been to deny: the delete-for-everyone lesson of guide 63, restated for the native channel.

How do we prove who actually sent a text from a shared or accessible phone?

The ladder's fourth rung, built not assumed: device-side context (unlock methods and their users, usage artefacts around the sending, location consistency), account context (who else knew the passcode: the pool named honestly), style and content coherence, and the surrounding conduct. Sometimes the summit is reached; some time s the honest finding is number-and-device level with the pool stated: guide 255 takes the full question, and this series' standing rule applies: the report claims the rung, never the assumption.

The thread mixes green and blue bubbles. Does the analysis change mid-conversation?

Yes, message by message: the store's service flags classify each record, and each class carries its own transit posture, provider shadow and recovery ecosystem: an o per at or record exists for the green message and not its blue reply; the blue message syncs to the Mac and the green may not. The unified exam in at i on handles this natively: the point for lawyers is not to argue channel-specific propositions ("the o per at or will confirm it") across a mixed thread unclassified.

What single step best protects a native-channel case this week?

The pairing this guide keeps repeating: early FFS extraction (the window and vacuum clocks) plus the o per at or request (the retention clock): the two moves with genuine stopwatches. Everything else: census, lineages, counterparts: improves with time or at least survives it; those two only decay. If the matter has texts at its centre and neither is in motion, that is today's work. cflab. u k · e-disc ove r y. u k