

WhatsApp Evidence

WhatsApp evidence presents unique challenges due to its architecture, encryption, and deletion features. This guide explores databases, backups, linked devices, and the implications of 'for-me' and 'for-everyone' deletion, offering insights into authentication and preservation for UK legal professionals.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30. <https://e-discovery.uk/library/whatsapp-evidence>

WHATSAPP EVIDENCE · A GUIDE FOR UK LAWYERS WhatsApp Evidence Databases, Backups, Deleted Messages, Groups and Linked Devices: the App That Runs UK Business on the Side COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
BACKUP & DELETED-DATA ANALYSIS CPR PART 35 EXPERT REPORT S FULL
CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: encrypted in transit, every where at rest 03 The architecture: databases, media, backups, linked devices 04 Deletion: for-me, for-everyone, and what each leaves 05 Groups: multiplied evidence, multiplied duty 06 Disappearing messages and the preservation race 07 Authentication: threads, exports and the screenshot problem 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: WHATSAPP 'SENCRIPTIONGUARDSTHEWIRE, NOT THE END S: ANDLITIGATIONLIVESATTHEENDS

§ 02 · FIRST PRINCIPLES The problem in plain English: encrypted in transit, every where at rest

§ 03 · THEARCHITECTURE The architecture: databases, media, backups, linked devices COMPONENT WHAT IT HOLDS · WHAT MATTER S

§ 04 · WHATDELETIONLEAVES Deletion: for-me, for-everyone, and what each leaves

§ 05 · GROUPS Groups: multiplied evidence, multiplied duty

§ 06 · THERACE Disappearing messages and the preservation race

§ 07 · ISITREAL? Authentication: threads, exports and the screenshot problem

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE BACKUP PRIMARY COMPUTER LINKED COUNTERPART DELETED / DEVICE (FFS) BACKUPS DEVICES PARTICIPANTS RECOVERABLE CLOUD LINEAGE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEDELETE - FOR - EVERYONETHATDATEDITSELF EXAMPLE2 · THEGROUPTHATOUTVOTEDTHEWIPEDPHONE EXAMPLE3 ·

THESCREENSHOTTHREADTHATNEVEREXISTED

§ 10 · WHERE IT GOES WRONG 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 · WHAT SHOULD BE FOR THE PRESERVATION LETTER

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The
Whats App checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can Whats App itself give us the
messages? Messages were deleted months ago. Realistic prospects? Are Whats App messages
even admissible: aren't they hearsay? The other side produced a chat export. Do we accept it?
Our client screenshot everything and deleted the originals "to save space". How bad? Do we
need every group member's phone?

§ 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. INSTRUCT THE LAB
NEW ENQUIRIES EMAIL - DISCOVERY

Questions and answers

Can Whats App itself give us the messages?

No: end-to-end encryption means the provider holds no readable content, and legal process against the platform yields account, registration and group metadata at most. The content routes are the ends: devices, backups and participants: which is why this guide is an architecture map rather than a subpoena template. Business API deployments (companies running Whats App through business tooling) are the exception worth checking: their message flows may be archived enterprise-side.

Messages were deleted months ago. Realistic prospects?

Decomposed, per §4: for-me deletions: good prospects via database layer (if extraction comes before vacuum), backups and counterparts; for-everyone: placeholders plus any backup or not if i c at i on residue pre-window, plus counterpart copies where the window missed; vacuumed and unbacked: the honest no, with the deletion's own record remaining. The single best predictor is backup lineage: a weekly cloud backup habit means the question is usually "which set", not "whether".

Are Whats App messages even admissible: aren't they hearsay?

They are documents, disclosed and admitted like any other, with hearsay rules apply in g to their contents as they would to a letter: the practical battleground is authenticity and completeness, not admissibility: which is why §7's workups matter more than evidence-law anxiety. Present threads threaded, sourced and complete (selective quotation invites the completeness attack), with the extraction pedigree stated: the presentation disciplines of guide 56 §13 apply.

The other side produced a chat export. Do we accept it?

As a start, not an end: exports are editable text artefacts. The §11 request asks for the underlying extraction and source-device access; the comparison (export against extracted store, and against your client's own copy of the thread) is quick and decisive; and divergences: messages present in one, absent in the other: are findings, not formalities. Accept nothing contested on format alone.

Our client screenshot everything and deleted the originals "to save space". How bad?

Recoverable, usually: the screenshots become leads; the database layer may retain the deleted records if extraction moves fast; backups predating the clear-out likely hold the threads; and counterparts hold their ends regardless. The honest account of the deletion goes in the file now: innocent housekeeping explained early reads entirely differently from the same facts excavated by the other side later. Then the ordinary machinery runs.

Do we need every group member's phone?

Rarely: two or three independent, cooperative members' extractions converging at record level authenticate a thread to the standard courts need (Example 2 used four of eleven); the selection favours members with long tenure, intact stores and backup habits. The full membership matters for preservation (letters) and for divergence analysis where deletion dating is itself in issue: collection scales to the questions, per the proportionality dial this series

runs every where. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd
·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 15 of 17

Source: <https://e-discovery.uk/library/whatsapp-evidence>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.