Mobile Phone Forensics

Mobile phone forensics is governed by extraction level, encryption state, and app architecture. This guide explores these gates, alongside deleted data, preservation, and common mistakes, helping UK lawyers navigate mobile and messaging evidence in litigation.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/mobile-phone-forensics

MOBILE PHONE FORENSICS · A GUIDE FOR UK LAWYERS Mobile Phone Forensics Extraction Levels, Encryption, App Evidence, Deleted Data and the Honest Limits of the Most Personal Device in the Case COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the witness with a lock on its mouth 03 Extraction levels: what each route actually yields 04 Encryption and device state: the access question 05 App evidence: where it lives, how it dies 06 Deleted data on modern phones: the honest position 07 Preservation and handling: before anyone touches it 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: MOBILEEVIDENCEISGOVERNEDBYTHREEGATES: EXTRACTION LEVEL, ENCRYPTIONSTATE, ANDAPPARCHITECTURE: AND STRATEGY IS SET BY WHICH GATESOPEN

§ 02 · FIRST PRINCIPLES The problem in plain English: the witness with a lock on its mouth

§ 03 · GATEONE Extraction levels: what each route actually yields LEVEL WHAT IT YIELDS · WHAT IT MISSES

§ 04 · GATETWO Encryption and device state: the access question

§ 05 · GATETHREE App evidence: where it lives, how it dies

§ 06 · THEHONESTLINE Deleted data on modern phones: the honest position

§ 07 · BEFOREANYONETOUCHESIT Preservation and handling: before anyone touches it

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE HANDSET CLOUD COMPUTER COUNTERPART O PER AT OR / DELETED / (BY LEVEL) ACCOUNT BACKUPS DEVICES PROVIDER RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THELEVELTHATCHANGEDTHEANSWER EXAMPLE2 · THEREBOOTTHATCLOSEDTHEGATE EXAMPLE3 · THEENSEMBLETHATOUTRANTHEWIPE

§ 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 · MOBILELIMBFORTHEPRESER VAT I ON INSTRUCTION

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

§ 13 · COMMON QUESTIONS Frequently asked questions Can the laboratory get into a locked phone? Do we need the phone at all if everything syncs to the cloud? How long does mobile exam in at i on take and what does it cost? The other side's expert says deleted messages are unrecoverable. Do we accept that? What about the privacy of everything else on the phone? Company phone, personal phone, or both: what should the scope chase?

§ 14 · REFERENCE Glossary TRIM 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 the laboratory get into a locked phone?

The only honest answer is conditional: it depends on the model, OS and patch level, the device's state (AFU/ BFU), the credentials position and the legal basis: five facts a first call establishes, against a capability frontier that moves monthly. Sometimes yes, quickly; some time s yes, expensively; some time s no, and the ensemble becomes the strategy. What no competent practice offers is the unconditional yes: guide 147 takes the full question.

Do we need the phone at all if everything syncs to the cloud?

Usually both, deliberately: the cloud carries breadth (and survives device loss), while the device carries what never synced: FFS-level app internals, deleted-record layers, system and location artefacts, and the local truth against which cloud copies are compared. Where only one is reachable, the other's absence is stated as a limitation. The comparison itself: device against cloud twin: is frequently the finding (deletions dated by divergence).

How long does mobile exam in at i on take and what does it cost?

Scoped work is days-to-weeks: capability check and preservation immediately; extraction hours-to-days once access exists; analysis scaling with apps and issues, not gigabytes. The budget-killers are avoidable: access adventures on hostile devices, full extractions where targeted scopes serve, and mythology-driven recovery quests past §6's line. Fixed-fee phases: preserve, assess, extract, analyse: keep the spend tied to decisions.

The other side's expert says deleted messages are unrecoverable. Do we accept that?

Ask the level question first: unrecoverable at logical extraction is a statement about the surface, not the phone (Example 1). Then the architecture questions: which app, what deletion behaviour, what cloud twin and backups exist, what do counterpart devices hold. Acceptance is some time s right: §6's honest line runs both ways: but only after the report states level, database-layer analysis and the ensemble position. The request wording in §11 extracts exactly that.

What about the privacy of everything else on the phone?

Central, not peripheral: phones hold whole lives, and UK practice: the college extraction guidance, UK GDPR minimisation, proportionality under PD 57AD: expects targeted scopes, staged review, and handling that separates the relevant from the merely present. Targeted extraction, examiner-side filter in g and protocol-agreed scopes are standard tools; "image everything and browse" is neither lawful practice nor good strategy. The specification carries the privacy architecture.

Company phone, personal phone, or both: what should the scope chase?

Follow the apps, not the ownership labels: work Whats App lives on personal handsets, personal Gmail on corporate ones, and the issues decide which stores matter. Corporate devices add MDM records and policy powers (guide 160); personal devices add the BYOD consent-and-proportionality track (guides 68 and 171). The per-app map across both, drawn early, is the scoping answer: and the ecosystem freeze covers which ever devices it names.