COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iPhone Forensics: The Defensible Mobile Evidence Bundle

Bringing the Whole iPhone Block Together: From Seizure to a Bundle That Survives Challenge

The preceding fifteen guides each examined one part of the iPhone: its acquisition, its backups, its messages, photos, health, apps, location, calls, activity databases, deleted data, secure messengers, the Watch, the account behind it, and the phone as an instrument of harm. This capstone brings them together into the thing a case actually needs: a single, coherent, defensible mobile evidence bundle. A bundle is defensible not because any one source is strong but because the sources converge, the weakest link has been found and addressed, the chain from seizure to report is unbroken, and every conclusion is stated at the confidence the evidence supports. This guide sets out for UK lawyers how the iPhone's many sources are assembled into one bundle, how it is built from seizure through acquisition, analysis and corroboration to reporting, how it is tested against the challenges it will face, and how it is presented so that it survives them.

⏱ Estimated reading time: 26 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. Building defensible mobile evidence bundles is the culmination of its iPhone work: assembling the phone's many sources, device, backups, account, Watch and estate, into one converging, corroborated account, tested against the challenges it will face, with an unbroken chain from seizure to report and every conclusion stated at honest confidence. The bundle is reported under CPR Part 35 and CrimPR Part 19 and built to survive scrutiny.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | DEFENSIBLE MOBILE EVIDENCE BUNDLES | CONVERGENCE & WEAKEST-LINK TESTING | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: the iPhone's many sources, device, backups, account, Watch and estate, become useful only when assembled into one coherent, defensible bundle, defensible not because any single source is strong but because the sources converge, the weakest link is found and addressed, the chain from seizure to report is unbroken, and every conclusion is stated at honest confidence.

The sources (§3): the block established the device (acquired at the right depth), backups, the iCloud account, the Watch and paired estate, and the many data types within them, messages, photos, health, apps, location, calls, activity and deleted data. **Building it (§4):** from seizure (decisive) through acquisition, analysis and corroboration to a report, each step preserving the chain. **Convergence and weakest link (§5):** a finding rests on sources agreeing, and the bundle is only as strong as its weakest link, which is found and shored up. **Testing (§6):** the bundle tested against the challenges it will face before it is served. **Deployment (§7):** presented so that it survives challenge, at honest confidence, under CPR Part 35 or CrimPR Part 19.

- **Many sources, one bundle:** the block's parts assembled into a single coherent account.
- **Seizure to report:** an unbroken chain from the decisive first moments to the final report.
- **Convergence carries weight:** findings rest on sources agreeing, not on one alone.
- **Find the weakest link:** the bundle is as strong as its weakest element, so it is found and fixed.
- **Test before serving:** the bundle is challenged internally before it faces the other side.

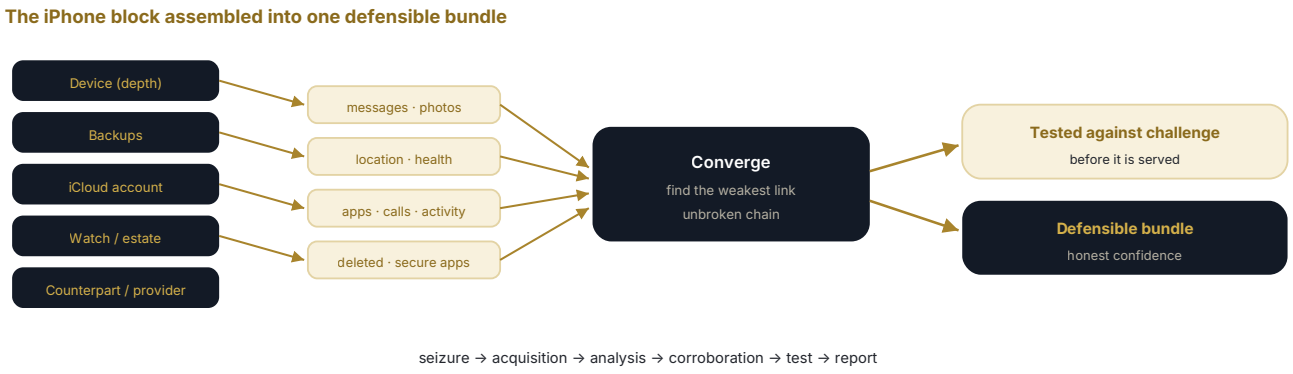

Figure 1 - the block's sources and data types converge into one bundle whose weakest link is found and chain kept unbroken, tested against challenge before it is served, and presented at honest confidence.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: many sources, one bundle

Over the preceding fifteen guides this block has taken the iPhone apart. It has examined how the phone is acquired and why seizure is decisive (guide 145), how the depth of extraction governs what is seen (146), how backups hold the phone's contents and sometimes more (147), and then each of the great evidence types in turn: messages (148), photos and their metadata (149), health and motion (150), the apps (151), location (152), calls and contact metadata (153), the activity databases (154), deleted data and SQLite (155), secure messengers (156), the Watch and paired devices (157), the iCloud account behind everything (158), and finally the phone as an instrument of harm (159). Each guide is a lens on one part. But a case does not need fifteen separate lenses; it needs one picture. This capstone is about turning the parts into the whole: a single, coherent, defensible mobile evidence bundle.

What makes a bundle defensible is worth stating plainly, because it is not what people often assume. It is not that any one source is overwhelmingly strong; a single source, however striking, is always open to challenge. It is that the sources converge, that a finding is supported by several independent sources agreeing, so that undermining one does not topple the conclusion. It is that the weakest link has been found and addressed, because a bundle, like a chain, is only as strong as its weakest element, and the other side will look for exactly that element. It is that the chain from seizure through acquisition, analysis and corroboration to the report is unbroken and documented, so the evidence's provenance cannot be attacked. And it is that every conclusion is stated at the confidence the evidence actually supports, neither overstated, which invites collapse under cross-examination, nor understated, which throws away value. The bundle, in short, is built to survive challenge, and the surest way to achieve that is to challenge it oneself before it is served. This guide sets out how the iPhone's many sources are assembled into one bundle, how it is built from seizure to report, how convergence and the weakest link are handled, how it is tested, and how it is presented so that it survives.

§ 0 3 · THE SOURCES

The sources the iPhone block established

- **The device, at the right depth:** the phone acquired lawfully, preserved from seizure (guide 145), and extracted at a depth sufficient for the matter, since logical silence is not absence (guide 146): the primary source, properly reached.
- **The backups:** iTunes/Finder and iCloud backups holding the phone's contents and earlier states, an encrypted local backup holding more (guide 147), so backups are first-class sources: the preserved copies.
- **The account behind the device:** the iCloud account aggregating all devices and often holding more and older data than any one, reached lawfully and with ADP accounted for (guide 158): the real store.
- **The Watch and paired estate:** the Apple Watch for stronger attribution and its own data, and the paired iPad, Mac and iCloud as a redundant, corroborating estate (guide 157): the wider estate.
- **The data types within them:** messages (148), photos (149), health (150), apps (151), location (152), calls and metadata (153), activity databases (154), deleted data (155) and secure messengers (156), each recovered and read by its own discipline: the evidence within.

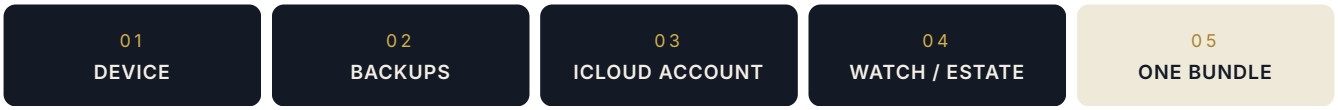

Figure 2 - the block's sources, device, backups, account, Watch and estate, each with its data types and discipline, assembled into one bundle.

§ 0 4 · BUILDING THE BUNDLE

Building the bundle: seizure to report

- **Seizure and preservation:** the decisive first moments, keeping the device from locking, from the network and from remote wipe, and minimising use so remnants survive (guides 145, 155), so what can ever be recovered is not lost at the start: the foundation laid.
- **Lawful acquisition at depth:** the device, backups, account and estate acquired lawfully, with passcode and consent or process, at the depth the matter needs, with integrity preserved by hashing and documentation (guides 2, 3, 117): the sound acquisition.
- **Analysis by discipline:** each data type analysed by its own discipline from the block, messages, photos, location, apps and the rest, so each is read correctly rather than naively (§3): the disciplined analysis.
- **Corroboration and timeline:** the findings corroborated across sources and placed on a single normalised timeline (guides 96, 108, 130), so the bundle tells one coherent story: the converging account.
- **The report:** the findings reported under CPR Part 35 or CrimPR Part 19, with method, chain, corroboration, limits and confidence stated (guide 100), so the bundle is accountable: the defensible report.

§ 0 5 · CONVERGENCE AND THE WEAKEST LINK

Convergence and the weakest link

- **Convergence carries weight:** a finding resting on several independent sources agreeing, a message, a location, an activity record, a counterpart copy, so that undermining one does not topple it (guide 130): the converging finding.
- **Find the weakest link:** the bundle examined for its weakest element, an uncorroborated source, a coarse location, an assumed attribution, a gap from rotation, since the other side will find it (guide 130): the vulnerability found.
- **Shore it up or state it:** the weak link strengthened by further corroboration where possible, and otherwise its weakness stated honestly so it does not surprise (guide 100): the vulnerability addressed.
- **Attribution as a common weak link:** the device-to-person inference a frequent weakest point, strengthened by the Watch, activity patterns and corroboration and stated at its true strength (guides 105, 157): the attribution shored up.
- **Gaps as gaps:** gaps from rotation, overwriting, ephemerality or an unworn Watch stated as gaps, never as absences, so the bundle does not overclaim (guides 154, 155, 156): the honest gaps.

§ 0 6 · TESTING THE BUNDLE

Testing the bundle against challenge

- **Challenge it yourself first:** the bundle attacked internally as the other side would, before it is served, so weaknesses are found in private rather than in court (guide 100): the internal cross-examination.
- **Test the chain:** the chain from seizure to report checked for any break, undocumented step or integrity gap, since a broken chain undermines everything (guides 2, 3): the chain tested.
- **Test the interpretations:** each interpretive step, a field meaning, a timestamp, an activity event, validated rather than assumed, especially for cryptic sources (guides 151, 154): the readings tested.
- **Test the alternatives:** alternative explanations considered and, where possible, excluded or acknowledged, so the conclusion is not merely the first that fitted (guide 100): the alternatives faced.
- **Test the confidence:** each conclusion checked against the evidence for overstatement or understatement, so the stated confidence is the confidence the evidence supports (guide 100): the calibration tested.

§ 0 7 · DEPLOYMENT

Deployment: presenting a bundle that survives

- **One coherent story:** the bundle presented as a single, coherent account on a timeline, not a pile of disconnected findings, so the tribunal can follow it (guides 96, 130): the narrative bundle.
- **Convergence made visible:** the corroboration shown, so the reader sees that each finding rests on sources agreeing, not on one source (§5): the visible strength.
- **Limits stated up front:** the gaps, weak links and limits stated openly, so they cannot be sprung as surprises and the honesty itself builds credibility (§5, §6): the candid limits.
- **Method and chain shown:** the method, extraction depth, chain of custody and integrity documented, so provenance is unassailable (guides 2, 3): the accountable method.
- **Honest confidence throughout:** every conclusion at the confidence the evidence supports, under CPR Part 35 or CrimPR Part 19, so the bundle bends but does not break under challenge (guide 100): the bundle that survives.

§ 0 8 · THE WHOLE ESTATE

Source architecture: the whole iPhone estate

Per this series' source-architecture discipline, and as the capstone of the block: the iPhone is never examined in isolation, because the whole estate is what makes a bundle both complete and resilient. The device holds the primary data, at the depth it was acquired. But the backups (guide 147) hold earlier states and, if encrypted, more; the iCloud account (guide 158) aggregates all devices and often holds more and older data, and survives a lost or wiped phone; the Watch (guide 157) gives stronger attribution and its own data; the paired iPad and Mac (guides 131, 135) hold synced copies; the counterparts hold their side of every communication; the app providers and carriers hold records by disclosure; and independent sources, CCTV, ANPR, transactions, corroborate from outside the estate entirely. The discipline is to map the whole estate at the outset, to reach each source lawfully, and to build the bundle from their convergence, so that no finding depends on one source and no lost or locked device ends the enquiry. When the phone is gone, the account and backups reconstruct it; when attribution is weak, the Watch and patterns strengthen it; when a source is coarse or gapped, another sharpens or fills it; and the bundle that results is one no single challenge can bring down.

EVIDENCE	DEVICE	BACKUPS	ICLOUD ACCOUNT	WATCH / PAIRED	COUNTERPART / PROVIDER	INDEPENDENT
Communications	Y: at depth	Y: earlier states	Y: if synced	Y: synced	Y: their side / records	n/a
Location / movement	Y: multi-source	In backup	Some synced	Y: Watch motion	Carrier cell (area)	Y: CCTV / ANPR
Activity / presence	Y: activity dbs	Earlier (pre-rotation)	Some	Y: worn (stronger)	App / provider logs	Y: sightings
Deleted / altered	Remnants	Y: pre-deletion	Y: earlier states	Device remnants	Y: their copy	n/a
Attribution	Device-level	Account-level	Account / devices	Y: wrist (stronger)	Counterpart naming	Y: person visible

Fallback strategy in one line: map the whole estate at the outset, reach every source lawfully, and build the bundle from convergence, so that no finding depends on one source and no lost or locked device ends the enquiry.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE BUNDLE THAT CONVERGED WHERE ONE SOURCE WOULD HAVE FAILED

A matter required proving that a person had been at a place, doing a thing, at a time, and had then tried to conceal it. No single source could carry it: the §3 location was partly coarse, the messages had been deleted, and attribution was contested. The §4 bundle was built from convergence: §5 Significant Locations and a photo geotag placed the phone (guide 152), the §3 Watch's worn heart-rate data strengthened attribution (guide 157), the §3 deleted messages were recovered from SQLite remnants and a pre-deletion backup (guides 155, 147), the §3 activity databases showed the phone in use (guide 154), and the §8 counterpart's device corroborated the conversation. The §5 weakest link, the coarse location, was shored up by the geotag and the Watch. The bundle stood where any one source would have fallen. The lesson is §5's: a defensible bundle rests on sources converging, so that a finding supported by location, attribution, recovered messages, activity and a counterpart survives the undermining of any one of them, which is why the whole estate is assembled rather than one striking source relied on.

EXAMPLE 2 · THE WEAKEST LINK FOUND BEFORE THE OTHER SIDE FOUND IT

A bundle looked strong until it was §6 tested internally as the other side would test it. The §5 weakest link emerged: a key conclusion rested on an §6 assumed meaning of a field in an unfamiliar app (guide 151), and on an attribution that was really only device-level (guide 105). Found in private, both were addressed: the field's meaning was validated against the provider's records, and the attribution was strengthened with the Watch and activity patterns (guide 157) and then stated at its true, more modest strength. Had these emerged in cross-examination, the bundle might have collapsed; found first, they were fixed or honestly stated. The lesson is §6's: the surest way to build a bundle that survives challenge is to challenge it oneself before it is served, finding the weakest links, an assumed interpretation, an overstated attribution, in private, and shoring them up or stating them honestly, so that nothing is sprung on the bundle in court.

EXAMPLE 3 · THE LOST PHONE AND THE BUNDLE BUILT FROM THE ESTATE

The central phone was lost before it could be examined, and it seemed the case had lost its evidence with it. The §8 estate discipline rebuilt the bundle without it: the §3 iCloud account held recent backups and synced photos and messages (guide 158), the §3 Watch held health, message and location data (guide 157), the paired Mac held synced conversations (guide 135), the §8 counterparts held their side of the communications, and carrier records supplied the call pattern (guide 153). Assembled and §4 placed on one timeline, these reconstructed most of what the lost phone would have shown, and the §7 report stated honestly what the estate could and could not replace. The bundle was built from the estate around the missing device. The lesson is §8's: because the whole estate is mapped and reached, a lost, wiped or locked phone does not end the enquiry, the account, backups, Watch, paired devices, counterparts and providers together reconstruct the bundle, with what the estate cannot replace stated honestly.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Relying on one striking source:** the cardinal error, resting a case on a single source that a challenge can topple (Example 1, §5).
- **Not finding the weakest link:** serving a bundle without having tested it as the other side will (Example 2, §6).
- **Losing the chain at seizure:** letting the phone lock, wipe or be used so that the foundation is lost (§4, guide 145).
- **Shallow extraction:** building on a logical extraction whose silence is mistaken for absence (§3, guide 146).
- **Ignoring the estate:** examining the device alone, and giving up when it is lost (Example 3, §8).
- **Overstating attribution:** presenting device-level attribution as person-level (§5, guide 105).
- **Presenting gaps as absences:** treating rotation, overwriting or ephemerality as proof nothing happened (§5).
- **Overstating or understating confidence:** conclusions not calibrated to the evidence (§6, §7).

Technical limitations

- **No bundle is unassailable:** it is built to survive challenge, not to be beyond it: the honest premise (§2).
- **Gaps are real:** rotation, overwriting and ephemerality leave genuine gaps that are stated (§5).
- **Attribution has limits:** device to person is an inference, strengthened but never certain (§5).
- **Depth and access constrain:** what was acquired, and lawfully reachable, bounds the bundle (§3).
- **The platform evolves:** every source in the block changes with iOS, so the bundle is current-aware (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What is the whole estate, phone, backups, account, Watch, paired devices, and has it all been preserved from the outset?
- Which findings does the case depend on, and are they corroborated by more than one source?
- What are the likely challenges, attribution, deletion, interpretation, and have we tested the bundle against them?

Ask your opponent

- Please preserve and disclose the whole estate at Schedule 1: the device, all backups, the iCloud account and its device records, the Watch and paired devices.
- Please disclose the method, extraction depth and chain of custody of any mobile evidence you rely on.
- Please identify the sources corroborating each finding you rely on, and any gaps or limits.

Ask your eDiscovery / forensic provider

- Does each key finding rest on converging sources, and what is the weakest link?
- Is the chain from seizure to report unbroken and documented?
- Has the bundle been tested against the challenges it will face, and is every conclusion at honest confidence?

SUGGESTED WORDING · INSTRUCTION FOR A DEFENSIBLE MOBILE EVIDENCE BUNDLE

> "We instruct you to build a defensible mobile evidence bundle from the iPhone estate at Schedule 1 relevant to Schedule 2. Please: (1) map and preserve the whole estate from the outset, the device (kept from locking, the network and remote wipe, with use minimised), all backups, the iCloud account and its device records, the Watch and paired devices, and identify counterparts, providers and independent sources; (2) acquire each source lawfully and at a depth sufficient for the matter, with integrity preserved by hashing and documentation, so the chain from seizure to report is unbroken; (3) analyse each data type by its proper discipline and corroborate the findings across sources on a single normalised timeline, so that each key finding rests on convergence rather than one source; (4) identify the bundle's weakest links, including attribution, interpretation and gaps, and shore them up with further corroboration or state them honestly; (5) test the bundle internally against the challenges it will face before it is served, validating interpretations and considering alternatives; and (6) report under CPR Part 35 or CrimPR Part 19 with method, chain, corroboration, limits and confidence stated, presenting one coherent account at the confidence the evidence supports."

§ 12 · QUICK CONTROL

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

The defensible-bundle checklist

- ☐ Whole estate mapped and preserved from the outset
- ☐ Device kept unlocked, off the network, use minimised at seizure
- ☐ Every source acquired lawfully at sufficient depth
- ☐ Chain from seizure to report unbroken and documented
- ☐ Each data type analysed by its proper discipline
- ☐ Findings corroborated and placed on one normalised timeline
- ☐ Each key finding rests on converging sources
- ☐ Weakest links identified and shored up or stated
- ☐ Bundle tested internally against likely challenges
- ☐ Report states method, chain, limits and honest confidence

Red flags

- A case resting on a single striking source: Example 1.
- A bundle served without internal testing: Example 2.
- The chain broken at seizure or an undocumented step.
- A shallow extraction's silence read as absence.
- The estate ignored, or the enquiry abandoned when the phone is lost: Example 3.
- Device-level attribution presented as person-level.
- Gaps presented as absences; confidence miscalibrated.

When to involve a digital forensic expert

From the very first moments, because the bundle's foundation is laid at seizure and cannot be relaid, and throughout, because assembling the iPhone's many sources into one defensible whole is expert work at every step: the expert maps and preserves the whole estate from the outset, acquires each source lawfully and at sufficient depth with an unbroken, documented chain (§4), analyses each data type by its proper discipline from the block, and builds the bundle from convergence so that no key finding rests on one source (Example 1, §5). The weakest links, attribution, assumed interpretations, gaps, are found and shored up or stated honestly, and the bundle is tested internally against the challenges it will face before it is served, so nothing is sprung on it in court (Example 2, §6). Where the phone is lost, wiped or locked, the bundle is rebuilt from the estate (Example 3, §8), and the whole is reported under CPR Part 35 or CrimPR Part 19 as one coherent account at honest confidence. This guide closes the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, defensible-bundle work turns the fifteen lenses of this block into one picture, built from convergence, tested against challenge, and presented with the candour that lets it survive.

§ 13 · COMMON QUESTIONS

Frequently asked questions

What makes a mobile evidence bundle "defensible"?

Four things together (§2). Convergence: each key finding rests on several independent sources agreeing, so undermining one does not topple it. The weakest link found and addressed: the bundle is only as strong as its weakest element, so that element is identified and shored up or stated honestly. An unbroken chain: provenance from seizure to report is documented and intact. And honest confidence: every conclusion is stated at the level the evidence supports. A bundle with these qualities is built to survive challenge, which is the point; no single strong source achieves that on its own.

Why not just rely on the strongest piece of evidence?

Because a single source, however striking, is always open to challenge (§5, Example 1). If a case rests on one source, an attack on that source, its attribution, its interpretation, its integrity, brings the whole case down. If the same finding is supported by location, activity, recovered messages, the Watch and a counterpart's copy, undermining any one of them leaves the conclusion standing. So the bundle is deliberately built from convergence across the whole estate, and the strongest single source is used as one converging element rather than the sole support.

What do you mean by "the weakest link"?

The element of the bundle most vulnerable to challenge (§5, Example 2). It is often attribution, the inference from a device's data to a particular person, or an assumed interpretation of a cryptic source, or a gap from rotation or overwriting, or a coarse location presented too precisely. Because the other side will look for exactly this, it is found first, internally, and then either strengthened with further corroboration or stated honestly at its true weight, so that it is never sprung as a surprise that unravels the bundle in court.

How is the bundle tested before it is served?

By challenging it as the other side would (§6). The chain from seizure to report is checked for breaks; each interpretive step, a field meaning, a timestamp, an activity event, is validated rather than assumed; alternative explanations are considered and excluded or acknowledged; and each conclusion is checked for overstatement or understatement against the evidence. Weaknesses found in this internal cross-examination are fixed or honestly stated, so the bundle that is served has already survived the challenges it is likely to face.

What if the phone itself is lost or wiped?

The bundle is rebuilt from the estate (§8, Example 3). Because the whole estate is mapped from the outset, a lost, wiped or locked phone does not end the enquiry: the iCloud account and backups reconstruct much of its contents, the Watch and paired devices hold synced and independent data, the counterparts hold their side of communications, and providers and carriers hold records. Assembled on one timeline, these often reconstruct most of what the phone would have shown, with what the estate cannot replace stated honestly, so the case proceeds around the missing device.

Why does seizure matter so much to the final bundle?

Because the foundation is laid, or lost, in the first moments and cannot be relaid (§4, guide 145). A phone that locks, is wiped remotely or is used heavily before it is preserved may lose the passcode-dependent access, the recoverable remnants and the activity records that the rest of the bundle depends on, and no later expertise can recover what those first moments destroyed. So the chain begins at seizure, keeping the device unlocked, off the network and unused, and every subsequent step preserves it, which is why the expert is involved from the very start rather than after the damage is done.

§ 14 · REFERENCE

Glossary

Evidence bundle
The assembled, coherent body of mobile evidence.

Defensible
Built to survive challenge, not beyond it.

Convergence
Several independent sources agreeing on a finding.

Weakest link
The bundle's most vulnerable element.

Chain of custody
The documented provenance from seizure to report.

Extraction depth
How much of the device an acquisition reaches.

Estate
The device, backups, account, Watch and paired devices.

Normalised timeline
Findings aligned on one common clock.

Internal testing
Challenging the bundle before it is served.

Honest confidence
Conclusions at the level the evidence supports.

Sources and authoritative references

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

- cflab.uk, digital forensics services (defensible mobile evidence bundles, convergence and weakest-link testing, 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, Phase 06 · Analysis and Phase 08 · Presentation (assembling and presenting corroborated evidence as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis · e-discovery.uk/edrm/presentation
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (validation, corroboration, disclosure of limits and honest reporting) and ISO/IEC 27037 (identification, collection, acquisition and preservation): gov.uk, FSR Code · iso.org, 27037
- NPCC / ACPO Good Practice Guide for Digital Evidence (principles for seizure and handling): npcc.police.uk · Apple Platform Security guide: support.apple.com, Platform Security
- CPR Part 35 and CrimPR Part 19 (expert evidence) · PD 57AD and CPR Part 31 · UK GDPR: justice.gov.uk, Part 35 · justice.gov.uk, CrimPR Part 19 · justice.gov.uk, PD 57AD · ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Defensible-bundle work at the laboratory turns the fifteen lenses of the iPhone block into one picture, built to survive challenge. From the first moments, the whole estate is mapped and preserved, the device kept from locking, the network and remote wipe with use minimised (guides 145, 155), and the backups, iCloud account, Watch and paired devices identified alongside counterparts, providers and independent sources (guides 147, 158, 157). Each source is acquired lawfully and at a depth sufficient for the matter, with integrity preserved by hashing and documentation so the chain from seizure to report is unbroken (guides 2, 3, 146). Each data type, messages, photos, health, apps, location, calls, activity, deleted data and secure messengers, is analysed by its proper discipline, and the findings are corroborated across sources and placed on a single normalised timeline so that every key finding rests on convergence rather than one source (Example 1). The weakest links, attribution, assumed interpretations, gaps, are found and shored up or stated honestly, and the bundle is tested internally against the challenges it will face before it is served (Example 2); where the phone is lost, wiped or locked, the bundle is rebuilt from the estate (Example 3). The whole is reported under CPR Part 35 or CrimPR Part 19 as one coherent account, with method, chain, corroboration, limits and confidence stated. This guide closes the iPhone and iPad block; the series turns next to Android. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle of the whole block is distilled here: many sources, converging, tested and candidly presented, make one bundle that survives.

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