COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iOS Full-File-System vs Logical Acquisition

How Deep the Extraction Goes, and Why It Matters for What You Will Find

Not all iPhone extractions are equal. A logical acquisition collects the data the phone is willing to hand over through its normal interfaces, the messages, photos, contacts and app data a backup would contain, and it is quick, safe and often sufficient. A full-file-system acquisition goes deeper, capturing the underlying file system and reaching data a logical extraction never sees: far more app data, system databases, location and activity records, and crucially deleted and unallocated content. The difference is not academic. Two examinations of the same phone can reach very different conclusions depending on the depth of extraction, and a party relying on a shallow acquisition may genuinely, and wrongly, believe that evidence is not there. Which method is possible depends on the device, its iOS version and its state, and each has its place. This guide sets out for UK lawyers what logical and full-file-system acquisitions are, what each does and does not reach, when each is available, and why the depth of extraction must be understood and stated.

⏱ 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. Choosing and performing the right iOS extraction, logical for what the phone hands over, full-file-system for the deeper record including deleted data, is central to its mobile work. The laboratory matches the method to the device and its state, states plainly the depth achieved and what it does and does not reach, and reports under CPR Part 35 and CrimPR Part 19, so that a conclusion is never mistaken for completeness when only a shallow extraction was possible.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | LOGICAL & FULL-FILE-SYSTEM EXTRACTION | EXTRACTION-DEPTH ASSESSMENT | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: iOS extractions differ in depth, a logical acquisition collects what the phone hands over through normal interfaces, while a full-file-system acquisition reaches the deeper file system including far more app data, system records and deleted content, so the method used can change what is found and must always be understood and stated.

Logical (§3): quick and safe, collecting the messages, photos, contacts and app data the phone exposes, roughly what a backup holds, often sufficient. **Full-file-system (§4):** deeper, capturing the underlying file system and reaching data logical never sees, extensive app databases, system and location records, and deleted and unallocated content. **What each reaches (§5):** logical gives the readily available data; full-file-system adds the hidden, system-level and deleted material, so a shallow extraction can miss evidence that exists. **Availability and choice (§6):** which method is possible depends on the device, iOS version and state, and the depth achieved is stated plainly. **Deployment (§7):** matching the method to the matter, and never mistaking a logical extraction's silence for proof that evidence is absent.

- **Depth changes the answer:** the same phone can yield different conclusions by extraction depth.
- **Logical is what the phone hands over:** messages, photos, contacts, app data, quick and safe.
- **Full-file-system goes deeper:** system records, more app data, and deleted content.
- **Shallow can miss real evidence:** absence in a logical extraction is not proof of absence.
- **State the depth:** which method was used, and what it reaches, is always made clear.

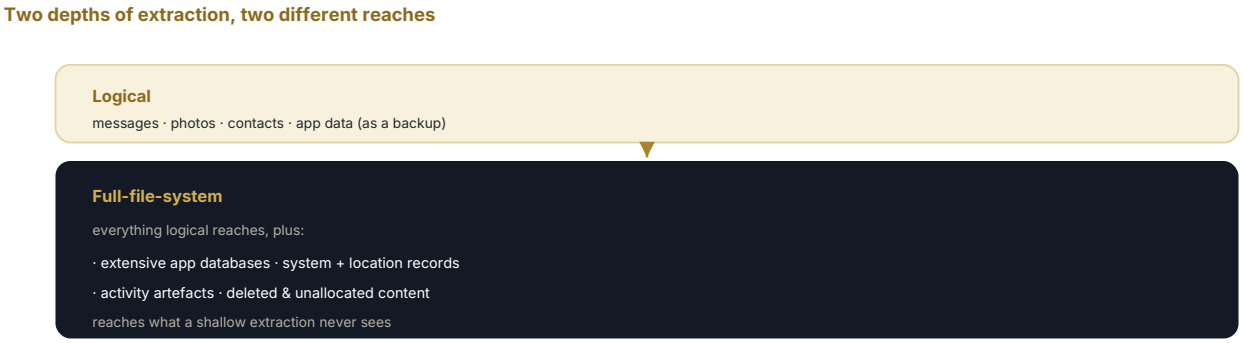

Figure 1 - logical acquisition reaches the data the phone hands over; full-file-system reaches that and the deeper system, app and deleted content a shallow extraction never sees.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: depth changes the answer

When someone says an iPhone was examined, the natural assumption is that everything on it was looked at. That is not how it works. An extraction reaches only as deep as the method allows, and there are, broadly, two depths. A logical acquisition collects the data the phone is willing to expose through its ordinary interfaces, essentially the material that would go into a standard backup: the messages, photos, contacts, call history and the app data that apps make available. It is fast, safe, and often enough to answer the question. A full-file-system acquisition goes much deeper, capturing the underlying file system of the device and reaching data that a logical extraction simply never touches: the full contents of app databases, system and diagnostic records, detailed location and activity data, and, importantly, deleted and unallocated content that the phone would never hand over voluntarily.

The reason this matters, and matters greatly, is that the depth of extraction can change the answer. Two examiners looking at the same phone can reach genuinely different conclusions, not because one is wrong, but because one had a deeper extraction than the other. A logical acquisition that finds no trace of a deleted message, or of a particular app's history, does not prove that the message or history never existed; it may simply mean the method did not reach that far. A party relying on a shallow extraction can therefore, in complete good faith, believe evidence is absent when a deeper extraction would have found it. This is why the depth of the acquisition must always be understood and stated, and why the choice of method matters. Which method is even possible depends on the device, its iOS version and its state, so the two are not always alternatives freely chosen; each has its place, and sometimes only the shallower is available. The discipline is to obtain the deepest extraction the device allows where the matter needs it, and to be clear about what depth was achieved and what it does and does not reach. This guide sets out the two methods, what each reaches, when each is available, and how the depth is communicated honestly.

§ 0 3 · LOGICAL ACQUISITION

Logical acquisition: what the phone hands over

- **The phone's own data:** a logical acquisition collecting the data the device exposes through its normal interfaces, roughly the contents of a standard backup, so it captures what the phone is willing to hand over (§5): the readily available data.
- **Core content:** messages, photos, contacts, call history, calendar and the app data apps make available, the everyday content that answers many questions, gathered quickly (guide 148): the core record.
- **Quick and safe:** the method fast and low-risk, requiring less of the device, so it is often the first and, for many matters, a sufficient extraction (§6): the low-cost option.
- **Widely available:** a logical acquisition possible on a wider range of devices and states than the deeper method, so it is frequently what can be done when full-file-system is not (§6): the broadly feasible method.
- **Its own limits:** a logical extraction not reaching the system-level, deep app and deleted data that lies beyond the phone's normal interfaces, so its silence is not proof of absence (§2): the boundary of the shallow method.

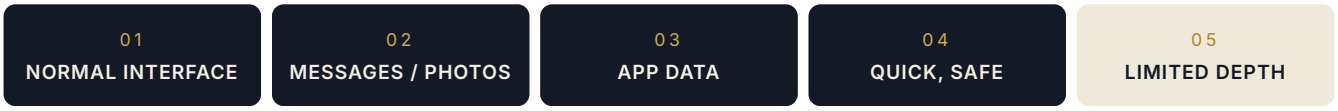

Figure 2 - the logical acquisition: fast, safe and widely available, capturing what the phone hands over, but limited to the readily available data.

§ 0 4 · FULL-FILE-SYSTEM ACQUISITION

Full-file-system acquisition: the deeper record

- **The underlying file system:** a full-file-system acquisition capturing the device's underlying file system, so it reaches data stored beyond the phone's normal interfaces, far more than a logical extraction (§5): the deep capture.
- **Extensive app data:** the full contents of app databases, including material apps do not expose to a backup, so the complete record of messaging and other apps is reached (guide 148): the full app record.
- **System, location and activity records:** system databases, detailed location history and activity artefacts (the iOS equivalents of guide 134's system record) reached, so the phone's own record of what was done and where is captured: the system-level record.
- **Deleted and unallocated content:** deleted data and unallocated space reached, so deleted messages, photos and records that a logical extraction never sees can be recovered (guide 4): the deleted data recovered.
- **More demanding and constrained:** the method requiring more of the device and available on a narrower range of models, iOS versions and states, so it is not always possible (§6): the deeper but more constrained option.

§ 0 5 · WHAT EACH REACHES

What each reaches, and what it misses

- **Logical reaches the available:** the readily available content, messages, photos, contacts, exposed app data, enough for many matters but bounded by the phone's interfaces (§3): the surface record.
- **Full-file-system reaches the hidden:** everything logical reaches plus the system-level, deep app and deleted data, so it finds material a logical extraction cannot, the decisive difference (§4): the complete reach.
- **Deleted data is the key gap:** deleted messages, photos and records typically beyond a logical extraction but often within a full-file-system one, so a matter turning on deleted data needs the deeper method (guide 4): the deletion divide.
- **App completeness differs:** some apps' full history reachable only at file-system depth, so a logical extraction may show only part of a conversation or none (guide 148): the app-depth difference.
- **Absence is not proof:** the central consequence, that not finding something in a logical extraction does not prove it is not on the phone, since the method may not have reached it (§2, guide 100): the honest reading of a shallow result.

§ 0 6 · AVAILABILITY AND HONEST LIMITS

Availability, method choice and honest limits

- **Availability depends on the device:** which method is possible determined by the model, iOS version and state (guide 145), so full-file-system is available on some devices and not others, and the choice is constrained, not free: the feasibility check.
- **Choose the deepest the matter needs:** the deepest extraction the device allows obtained where the matter requires reach, deleted data, full app history, rather than settling for logical by default (§7): the method matched to need.
- **State the depth achieved:** the method used and the depth reached stated plainly, so a conclusion is understood in light of how deep the extraction went (guide 100): the depth disclosed.
- **Do not overclaim from logical:** a logical extraction's silence not presented as proof of absence, since the method may not have reached the data (§5): the shallow result read honestly.
- **Integrity and validation throughout:** whichever method is used, the extraction hashed, documented and validated (guides 2, 3, 71), so it is accountable and reproducible regardless of depth: the sound extraction.

§ 0 7 · DEPLOYMENT

Deployment: matching the method to the matter

- **Logical where it suffices:** a logical acquisition used where the readily available content answers the matter proportionately, quick and low-risk (guide 20): the sufficient extraction.
- **Full-file-system where depth is needed:** the deeper method used where deleted data, full app history or system records matter, so the evidence that a logical extraction would miss is reached (guides 4, 148): the deeper extraction deployed.
- **Testing a shallow result:** a matter resting on a logical extraction's silence tested by a deeper extraction where feasible, so a claim that evidence is absent is properly examined (§5): the silence challenged.
- **Disclosure of method and depth:** the method and depth disclosed in evidence, so the court and the parties understand the reach of the examination and can weigh its conclusions (guide 100): the transparent extraction.
- **The estate alongside:** the backups and iCloud estate used to complement the device extraction, since they may hold data at a different depth or that the device method could not reach (§8): the estate as complement.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the depth of a device extraction is one dimension of where the evidence lives, and the backups and estate provide others, so a difficult or shallow device extraction is complemented across the estate. The device holds the data reachable at logical or full-file-system depth. But a computer backup (iTunes/Finder, guide 147) holds a copy of much of the phone's data, sometimes including material at a useful depth, and an encrypted backup can hold more than an unencrypted one; iCloud holds synced messages, photos, location and app data and iCloud backups; the paired Mac and iPad hold the same synced data; and the app providers and carriers hold their own records. The discipline is to see the device extraction and the estate as complementary: where a logical extraction on the device reaches only the surface, a computer backup or the iCloud estate may add depth, and where the deeper file-system method is not available on the device, the backups and estate may still hold the relevant data. When the device yields only a shallow extraction, the backups and iCloud complement it; when full-file-system is not feasible, the estate carries part of the record; and the sources together give a fuller picture than any single extraction depth.

EVIDENCE	LOGICAL (DEVICE)	FULL-FILE-SYSTEM (DEVICE)	COMPUTER BACKUP	ICLOUD	PAIRED MAC / IPAD	APP PROVIDER / CARRIER
Messages	Y: available	Y: full + deleted	Y: in backup	Y: synced	Y: same threads	Some records
Deleted data	Rarely	Y: often	Sometimes	Recently deleted	Device remnants	Retention varies
App history (full)	Partial	Y: full	Varies	Varies	Some synced	Provider records
System / location	Limited	Y: detailed	Some	Often synced	Paired data	Carrier location (coarse)
Photos / media	Y: available	Y: full + deleted	Y: in backup	Y: iCloud Photos	Y: same library	n/a

Fallback strategy in one line: treat extraction depth and the estate as complementary; where a logical device extraction reaches only the surface or the deeper method is not feasible, the backups, iCloud and paired devices add the depth.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DELETED MESSAGES A LOGICAL EXTRACTION MISSED

A party's phone had been examined by a logical acquisition, which found no trace of certain deleted messages, and it was argued that the messages had never existed. The §5 depth discipline tested that claim: a §4 full-file-system acquisition, feasible on this device, reached the deeper app databases and unallocated space and recovered the deleted messages the logical extraction had never touched (guide 4). The §2 point was proved in practice, the logical extraction's silence had not meant absence, only limited reach. The §6 depth of each method was stated plainly. The messages, thought gone, were there all along at greater depth. The lesson is §5's: a logical extraction's failure to find something is not proof it is not on the phone, deleted and deep app data typically lie beyond a logical acquisition, so a matter turning on such data needs a full-file-system extraction, and a conclusion of absence from a shallow method must never be overstated.

EXAMPLE 2 · THE LOGICAL EXTRACTION THAT WAS ENOUGH

In a straightforward matter, the question was simply what a set of readily available messages and photos showed, with no issue of deletion or hidden app data. The §7 proportionate choice was a logical acquisition (guide 20): quick, safe and widely available, it captured the messages, photos and contacts that answered the matter, and a deeper, more demanding extraction was unnecessary. The §6 method and depth were stated, and the conclusion rested squarely on what the logical extraction reached. Depth was matched to need, no more. The lesson is §7's: full-file-system is not always required, where the readily available content answers the matter and there is no issue of deleted or deep data, a logical acquisition is the proportionate and sufficient method, and the discipline is to match the depth to the matter, using the deeper method where it is needed and the shallower where it suffices, always stating which was used.

EXAMPLE 3 · THE DEPTH THAT WAS NOT AVAILABLE, AND THE ESTATE THAT HELPED

A matter needed deleted app history from an iPhone whose model, iOS version and state did not permit a full-file-system acquisition (guide 145), so the deep device extraction simply was not available. Rather than overstate a logical extraction, the §6 honest limit was stated, and the §8 estate was turned to: an encrypted computer backup (guide 147) held more app data than an unencrypted one would, and the iCloud estate held further synced records, together supplying part of the depth the device method could not. The §6 limits of each source were stated plainly. The lesson is §6's and §8's: the deeper extraction is not always feasible, its availability depends on the device, and when it is not, the honest course is to say so and to complement the device with the backups and iCloud estate, which may hold at a different depth what the device extraction could not reach, rather than pretending a shallow extraction is complete.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Reading logical silence as absence:** the cardinal error, treating a logical extraction's failure to find something as proof it is not there (Example 1, §5).
- **Not seeking the deeper method:** settling for logical when the matter needs deleted or deep app data and full-file-system is feasible (§7).
- **Not stating the depth:** presenting a conclusion without making clear which method and depth were used (§6).
- **Assuming full-file-system is always possible:** promising the deeper extraction when the device does not permit it (Example 3, §6).
- **Over-extracting disproportionately:** using the deeper, more demanding method where logical would suffice (Example 2, §7).
- **Ignoring the estate's depth:** overlooking that an encrypted backup or iCloud may add depth the device method missed (§8).
- **Confusing the two in disclosure:** not distinguishing what a logical and a full-file-system extraction each reached (§6).
- **Skipping validation:** not documenting and validating the extraction whatever its depth (§6).

Technical limitations

- **Depth is device-dependent:** which method is possible depends on model, iOS and state, so the deeper method is not always available (§6, guide 145).
- **Logical misses the deep and deleted:** a logical extraction cannot reach system-level and deleted data: the core limit (§5).
- **Full-file-system is more demanding:** it requires more of the device and is more constrained (§4).
- **Neither is infinite:** even full-file-system has limits, and some data may be beyond any method (§4).
- **iOS evolves:** what each method reaches changes with iOS, so capability is current-aware (§6).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Does the matter turn on deleted data or full app history, so a full-file-system extraction is needed, or is readily available content enough?
- What extraction method was used on any phone already examined, and what depth did it reach?
- Is the deeper method feasible on this device, and if not, what does the estate hold?

Ask your opponent

- Please confirm the acquisition method used on the device at Schedule 1 (logical or full-file-system) and the depth reached, and disclose the extraction.
- Where a logical extraction is relied on to show absence, please confirm whether a full-file-system extraction was feasible and, if so, undertake it.
- Please disclose any computer or iCloud backups that may hold data at a different depth.

Ask your eDiscovery / forensic provider

- Which method is feasible on this device, and what will each reach and miss?
- Does the matter need the deeper method, and is it available?
- How will the depth achieved be stated, and can the estate complement it?

SUGGESTED WORDING · INSTRUCTION FOR AN IOS EXTRACTION

> "We instruct you to acquire the Apple mobile device at Schedule 1 to the depth the matter at Schedule 2 requires. Please: (1) assess, given the device's model, iOS version and state, which acquisition methods are feasible (logical and, where possible, full-file-system); (2) where the matter turns on deleted data, full app history or system and location records, obtain a full-file-system acquisition if the device permits it, since a logical extraction typically will not reach that data; (3) where the readily available content suffices and there is no issue of deleted or deep data, a logical acquisition may be proportionate; (4) whatever the method, hash, document and validate the extraction, and state plainly the method used and the depth reached, so no conclusion of absence is drawn from a shallow extraction that did not reach the relevant data; and (5) where the deeper method is not feasible, say so and complement the device with the computer and iCloud backups, which may hold at a different depth what the device extraction could not reach. Report the method, depth and honest limits."

§ 12 · QUICK CONTROL

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

The extraction-depth checklist

- ☐ Feasible methods assessed for the device, iOS and state
- ☐ Depth needed by the matter identified (deleted, deep app, system)
- ☐ Deepest feasible method obtained where the matter needs reach
- ☐ Logical used where proportionate and sufficient
- ☐ Deleted and deep app data sought where relevant
- ☐ Extraction hashed, documented and validated
- ☐ Method and depth stated plainly
- ☐ No absence concluded from a shallow extraction that did not reach
- ☐ Estate used to complement the device's depth
- ☐ Method, depth and limits disclosed and reported

Red flags

- A logical extraction's silence presented as proof of absence: Example 1.
- The deeper method not sought when the matter needs deleted data.
- The method and depth not stated.
- Full-file-system promised on a device that does not permit it: Example 3.
- The deeper method used where logical would suffice: Example 2.
- The estate's added depth overlooked.
- Logical and full-file-system reaches not distinguished.

When to involve a digital forensic expert

Whenever an iPhone matters and especially where deleted data or full app history is in issue, because the depth of extraction can change the answer and only an expert can obtain and interpret the right one: the expert assesses which methods the specific device permits (guide 145), obtains a full-file-system acquisition where the matter needs its reach into deleted, deep app and system data, and uses a logical acquisition where it is proportionate and sufficient (Examples 1 and 2, §7). Critically, the expert never presents a logical extraction's silence as proof of absence, states plainly the method used and the depth reached, and, where the deeper method is not feasible, says so and complements the device with the computer and iCloud backups that may hold the data at a different depth (Example 3, §8). Every extraction is hashed, validated and documented, and the method, depth and limits are reported under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, iOS extraction work matches the depth to the matter and is scrupulous about what each method reaches, so that evidence is not missed by a shallow acquisition and a conclusion is never mistaken for completeness when the extraction did not go deep enough to support it.

§ 13 · COMMON QUESTIONS

Frequently asked questions

What is the difference between logical and full-file-system extraction?

Depth (§3, §4). A logical acquisition collects the data the phone hands over through its normal interfaces, essentially what a backup holds: messages, photos, contacts, available app data. A full-file-system acquisition captures the underlying file system and reaches far more, the full contents of app databases, system and location records, and deleted and unallocated content. The logical method is quicker, safer and more widely available; the full-file-system method goes much deeper but is more demanding and not always possible.

If a logical extraction found nothing, does that mean it isn't there?

No, and this is the crucial point (§2, §5, Example 1). A logical extraction reaches only the readily available data, so its failure to find something, a deleted message, an app's full history, does not prove the data is not on the phone; it may simply mean the method did not reach that far. Deleted and deep app data typically lie beyond a logical acquisition. So a conclusion of absence must never be drawn from a shallow extraction, and where the matter turns on such data, a deeper extraction is needed.

Do we always need the deeper extraction?

No, match the depth to the matter (§7, Example 2). Where the question is answered by readily available content and there is no issue of deleted or deep data, a logical acquisition is proportionate and sufficient. The deeper, more demanding full-file-system method is used where it is needed, for deleted data, full app history, or system and location records, and where the device permits it. The discipline is to obtain the depth the matter requires, no less and no more, and always to state which method was used.

Can you always do a full-file-system extraction?

No, its availability depends on the device (§6, guide 145, Example 3). Whether a full-file-system acquisition is possible turns on the specific model, iOS version and state, so it can be done on some devices and not others. When it is not available, an honest examiner says so rather than overstating a logical extraction, and complements the device with the computer and iCloud backups, which may hold at a different depth what the device method could not reach. Capability is assessed per device and stated plainly.

Why does the method used need to be disclosed?

Because it determines what the examination could reach (§6). A conclusion means something quite different depending on whether it rests on a shallow or a deep extraction: absence found by a logical method is far weaker than absence found by a full-file-system one. So disclosing the method and the depth achieved lets the court and the parties understand and weigh the conclusion properly. An examination that hides its depth invites a false impression of completeness, which is why the method and its reach are always stated.

Can backups make up for a shallow device extraction?

Sometimes, in part (§8, Example 3). A computer backup, especially an encrypted one, can hold more of the phone's data than an unencrypted backup, and the iCloud estate holds synced records, so where a logical device extraction reaches only the surface, or the deeper method is not feasible, the backups and estate may add depth. They are complementary to the device extraction, not a full substitute, but they frequently hold relevant data at a useful depth, which is why the estate is examined alongside the device.

§ 14 · REFERENCE

Glossary

Logical acquisition
Collecting the data the phone exposes normally.

Full-file-system
Capturing the underlying file system, far deeper.

Extraction depth
How far into the device an acquisition reaches.

App database
An app's store of data, fully reached only deep.

Unallocated space
Storage holding deleted, recoverable data.

Deleted data
Removed content, often beyond a logical extraction.

System record
iOS's own activity and location data (cf. guide 134).

Absence-not-proof
Shallow silence does not prove data is absent.

Validation
Confirming an extraction is complete and sound.

Estate
Backups and iCloud that may add depth.

Sources and authoritative references

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

- cflab.uk, digital forensics services (logical and full-file-system extraction, extraction-depth assessment, 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 (mobile extraction and analysis 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 (iOS data protection classes, which shape what each extraction method reaches): support.apple.com, Platform Security
- ISO/IEC 27037 (identification, collection, acquisition and preservation) and Forensic Science Regulator, Code of Practice v2 (method, validation and honest reporting): iso.org, 27037 · gov.uk, FSR Code
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

iOS extraction work at the laboratory matches the depth to the matter and is scrupulous about what each method reaches, because on a phone the depth of the acquisition can change the answer. The feasible methods are assessed for the specific device, given its model, iOS version and state (guide 145), and where the matter turns on deleted data, full app history or system and location records, a full-file-system acquisition is obtained if the device permits it, reaching the deep app databases, system records and unallocated content that a logical extraction never touches (Example 1, §4). Where the readily available content answers the matter and there is no issue of deletion or deep data, a logical acquisition is used as the proportionate, sufficient method (Example 2, §7). Critically, a logical extraction's silence is never presented as proof of absence, the method and depth reached are always stated plainly, and where the deeper method is not feasible on the device, the honest limit is stated and the device is complemented with the computer and iCloud backups, especially encrypted backups, that may hold the data at a different depth (Example 3, §8). Every extraction is hashed, validated and documented, and the method, depth and limits are reported 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 governing discipline is that evidence must not be missed by a shallow extraction, nor a conclusion mistaken for completeness when the acquisition did not go deep enough to support it.

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