COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iOS Backups: iTunes/Finder and iCloud

The Copy of the Phone That Survives When the Phone Does Not, and Why Encryption Helps You

When the iPhone itself is locked, difficult or gone, the backup is frequently the way in. An iPhone can be backed up in two places: to a computer, through iTunes on older systems or Finder on newer Macs, and to iCloud. Either backup is a substantial copy of the phone's data, messages, photos, app data and more, that exists independently of the device and can be examined when the device cannot. There is a striking twist for the lawyer: an encrypted local backup actually contains more than an unencrypted one, because Apple only includes certain sensitive categories (health data, saved passwords, and more) when the backup is encrypted. So encryption, usually an obstacle, here works in the investigator's favour, provided the backup password is available. This guide sets out for UK lawyers where iOS backups live, what each contains, why an encrypted backup holds more, how backups are located and examined, and how backup evidence is authenticated and dated.

⏱ 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. iOS backup analysis is one of the most productive parts of its mobile work: locating and examining iTunes, Finder and iCloud backups that hold a substantial copy of the phone independently of the device, and using the fact that an encrypted local backup contains more than an unencrypted one. The analysis authenticates and dates each backup, reaches it lawfully, and is reported under CPR Part 35 and CrimPR Part 19, so a locked or lost phone rarely means the evidence is gone.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ITUNES, FINDER & ICLOUD BACKUPS | ENCRYPTED-BACKUP ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 1 · ORIENTATION

Executive summary

The headline point: an iPhone can be backed up to a computer (iTunes or Finder) or to iCloud, and either backup is a substantial copy of the phone that exists independently of the device and can be examined when the device cannot, and, strikingly, an encrypted local backup holds more than an unencrypted one.

Where they live (§3): local backups on a computer via iTunes or Finder, and iCloud backups in the user's Apple account. **What they contain (§4):** a substantial copy of the phone, messages, photos, app data, settings and more, though not always everything on the device. **Why encryption helps (§5):** Apple includes certain sensitive categories (health, saved passwords and more) only in an encrypted local backup, so an encrypted backup contains more than an unencrypted one, encryption working for the investigator where the password is available. **Locating and dating (§6):** backups located on computers and in the account, reached lawfully, and each dated and authenticated. **Deployment (§7):** using a backup when the phone is locked, lost or wiped, and to recover deleted data and prior states.

- **The phone's shadow copy:** a backup holds much of the phone independently of the device.
- **Two homes:** local backups on a computer (iTunes/Finder) and iCloud backups.
- **Encryption helps here:** an encrypted local backup contains more, including sensitive categories.
- **The way in when the phone is not:** a backup is examinable when the device is locked or gone.
- **Date and authenticate:** each backup is a dated record of the phone at a past moment.

The backup: a copy of the phone that outlives the phone, and encryption adds more

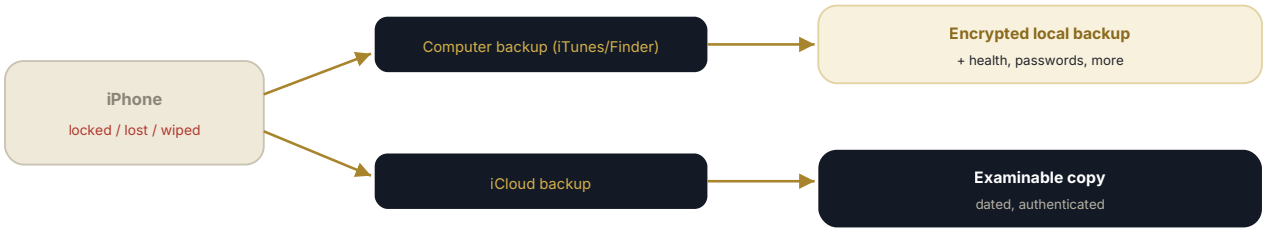

Figure 1 - a phone backs up to a computer and to iCloud, and either backup is an examinable copy that outlives the device, with the encrypted local backup holding the most.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the phone's shadow copy

The previous guides in this block explained why the iPhone is so hard to acquire directly. The good news is that the phone is rarely the only copy of its own data. Most iPhones are backed up, and a backup is a substantial copy of the phone's contents, its messages, photos, app data, settings and much more, that exists somewhere other than the device. There are two places this shadow copy lives. A local backup is made to a computer: through the iTunes application on older systems, or through Finder on newer Macs, and stored on that computer's disk. An iCloud backup is made to the user's Apple account and stored in the cloud. Either kind is, in effect, a copy of the phone that can be examined when the phone itself cannot, when it is locked, lost, damaged or wiped.

This is transformative for the lawyer, because it means a difficult phone often does not mean lost evidence. And there is a counter-intuitive twist that is genuinely useful. Normally encryption is the obstacle in mobile forensics. But with local backups, encryption works the other way. Apple only includes certain sensitive categories of data, such as health data and saved passwords, when a local backup is encrypted; an unencrypted backup leaves those categories out. So an encrypted local backup actually contains more than an unencrypted one, and where the backup password is available (by cooperation or lawful means), the encrypted backup is the richer source. This is one of the few situations in iOS forensics where encryption helps rather than hinders. The tasks, then, are to find the backups, on computers and in the account, to establish which are encrypted, to reach them lawfully, and to authenticate and date each one, since a backup is a copy of the phone as it was at a particular moment. This guide sets out where iOS backups live, what each contains, why an encrypted backup holds more, how they are located and examined, and how backup evidence is authenticated.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 3 · WHERE BACKUPS LIVE

Where iOS backups live

- **Local computer backups:** backups made to a computer through iTunes (older systems) or Finder (newer Macs) and stored on that computer's disk, so a computer the phone was synced to may hold a substantial copy of it (§2): the on-computer copy.
- **iCloud backups:** backups made to the user's Apple account and stored in iCloud, reachable through the account by lawful means, independent of any computer (§6): the cloud copy.
- **Multiple and historic backups:** a computer or account often holding more than one backup, including older ones, so several dated copies of the phone may exist (§6): the multiple states.
- **Backups of several devices:** a computer or account holding backups of more than one device (an old phone, an iPad), so the relevant device's backup is identified among them (§6): the right-device backup.
- **Located and examined soundly:** the backups located, and the local ones acquired forensically and the iCloud ones obtained lawfully, with integrity preserved (guides 2, 3), so each is examined without alteration: the sound basis.

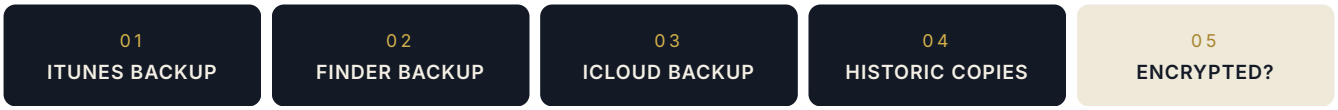

Figure 2 - the homes of an iOS backup: local iTunes and Finder backups on a computer, iCloud backups in the account, often several and historic, and the key question of whether a local backup is encrypted.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 4 · WHAT EACH CONTAINS

What each backup contains

- **A substantial copy:** a backup containing a large part of the phone's data, messages, photos, app data, contacts, settings and more, so it answers many of the same questions the device would (guides 146, 148): the broad copy.
- **Not always everything:** a backup not necessarily including every category on the device (some data is not backed up, and unencrypted backups omit sensitive categories, §5), so its scope is understood, not assumed complete (§6): the bounded copy.
- **Local versus iCloud differences:** local and iCloud backups differing in what they include and how they are reached, so both are considered and the fuller source used (§5): the two sources compared.
- **App data within limits:** app data included to the extent apps allow it to be backed up, so the completeness of a given app's history in a backup is checked against a device extraction (guide 148): the app-data scope.
- **A dated snapshot:** each backup a copy of the phone at the time it was made, so it evidences the phone's state at that moment, a dated record (§6, guide 137): the point-in-time copy.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 5 · WHY ENCRYPTION HOLDS MORE

Why an encrypted backup holds more

- **Encryption adds categories:** Apple including certain sensitive categories, such as health data and saved passwords, only when a local backup is encrypted, so an encrypted backup contains more than an unencrypted one, the useful twist (§2): the encryption bonus.
- **The counter-intuitive help:** encryption, normally the obstacle, here working for the investigator, since the richer backup is the encrypted one, provided the password is available (§6): the reversal.
- **The password is the key:** the encrypted backup accessible with its password, obtained by cooperation or lawful means, so reaching it is a matter of the password, not of breaking encryption (guide 117): the access point.
- **Prefer the encrypted backup:** the encrypted local backup preferred as the fuller source where it exists and the password is available, over an unencrypted backup or, sometimes, a limited device extraction (§7): the richer choice.
- **State what is and is not included:** the categories a given backup does and does not contain stated, so its completeness is understood and absence is not misread (guide 100): the honest scope.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 6 · LOCATING AND DATING

Locating, accessing and dating backups

- **Find the local backups:** the computers the phone was synced to located and examined for iTunes and Finder backups, since a backup a party has forgotten may hold the evidence (§3): the local search.
- **Reach the iCloud backups lawfully:** the iCloud backups obtained through the account by consent or lawful process (guides 111 to 114), so the cloud copy is reached with proper authority: the lawful cloud access.
- **Establish encryption and password:** whether a local backup is encrypted established, and the password obtained where possible, so the fuller encrypted backup can be examined (§5, guide 117): the access resolved.
- **Date each backup:** each backup dated to when it was made, so it is understood as the phone's state at that moment and used as a dated checkpoint (guides 96, 137): the backup placed in time.
- **Authenticate the backup:** the backup's integrity and provenance established, whose phone, from which source, how obtained, so the recovered data is a genuine, unaltered copy (guides 2, 3): the backup proved sound.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 7 · DEPLOYMENT

Deployment: the locked phone and the deleted data

- **When the phone is locked or gone:** a backup examined when the device is locked, lost, damaged or wiped, so the evidence is reached independently of the difficult device (guide 145): the way in.
- **Recovering deleted data:** data deleted from the phone recovered from a backup made before the deletion, and deleted content within a backup recovered from its databases (guides 4, 148): the deleted data restored.
- **The richer encrypted backup:** the encrypted local backup used as the fuller source, reaching health, password and other categories an unencrypted backup omits (§5): the fullest copy deployed.
- **Prior states and dating:** older backups used to evidence the phone's state at past moments, dating changes and deletions (guides 96, 137): the phone's history from its backups.
- **Honest, corroborated presentation:** the backup evidence authenticated, dated, its scope stated, and corroborated with the device and estate, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the backup evidence deployed defensibly.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: iOS backups are themselves a central "where else the evidence lives" answer for a difficult phone, and they sit among the device and the wider Apple estate. The device holds the live data reachable at logical or full-file-system depth (guide 146). But a computer backup (iTunes/Finder) holds a substantial copy independently of the device, and an encrypted local backup holds more than an unencrypted one; iCloud holds iCloud backups and synced messages, photos and app data; the paired Mac and iPad (guides 131, 135) hold the same synced data; and the app providers hold their own records. The discipline is to treat the backups as first-class sources alongside the device, so that a locked, lost or wiped phone is approached through its backups, and the richer encrypted local backup is preferred where its password is available. When the device cannot be acquired, a computer or iCloud backup holds much of the same data; when a backup omits a category (an unencrypted local backup), the encrypted backup, iCloud or the device may hold it; and several dated backups together give the phone's history, not just its present.

EVIDENCE	THE DEVICE	ENCRYPTED LOCAL BACKUP	UNENCRYPTED LOCAL BACKUP	ICLOUD BACKUP / SYNC	PAIRED MAC / IPAD	APP PROVIDER
Messages	Y: if accessible	Y	Y	Y: synced	Y: same threads	Some records
Photos	Y: if accessible	Y	Y	Y: iCloud Photos	Y: same library	n/a
Health data	Y: if accessible	Y: included	Not included	Often synced	Paired data	n/a
Saved passwords	Keychain	Y: included	Not included	iCloud Keychain	Paired trust	n/a
Deleted data	Full-file-system	In backup databases	In backup databases	Recently deleted	Device remnants	Retention varies

Fallback strategy in one line: treat the backups as first-class sources; when the phone is locked or gone, a computer or iCloud backup holds much of it, and the encrypted local backup, with its password, holds the most.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE LOCKED PHONE AND THE COMPUTER BACKUP THAT ANSWERED

An iPhone central to a matter was locked and, without the passcode, yielded little by direct means (guide 145). The §3 and §7 backup route resolved it: a computer the phone had been synced to held an iTunes backup, a substantial copy of the phone made independently of the device, and it was located, acquired forensically and examined (guide 2). The §6 backup was dated and authenticated, and it held the messages, photos and app data the matter needed. The locked phone had not, after all, meant lost evidence. The lesson is §2's: a phone is rarely the only copy of its own data, and when the device is locked, lost or wiped, a computer or iCloud backup frequently holds a substantial, examinable copy, so the first response to a difficult phone is to find its backups, which routinely supply the evidence the device will not.

EXAMPLE 2 · THE ENCRYPTED BACKUP THAT HELD MORE

Two backups of the same phone existed: an unencrypted one and an encrypted one whose password the user provided. The §5 encryption twist was decisive: the encrypted backup contained categories the unencrypted one omitted, including health data that placed the user's activity at a relevant time, and saved passwords that mapped the user's accounts (guide 140). The §6 password made the richer backup accessible, and it was preferred as the fuller source. Encryption, usually the obstacle, had here worked in the investigator's favour. The lesson is §5's: with local backups, an encrypted backup contains more than an unencrypted one, because Apple includes sensitive categories only when the backup is encrypted, so where the password is available the encrypted backup is the richer source, one of the few situations in iOS forensics where encryption helps rather than hinders.

EXAMPLE 3 · THE DELETED MESSAGES A PRIOR BACKUP PRESERVED

A party had deleted messages from their phone, and even a device extraction could not recover all of them. The §7 backup route did: an older backup, made before the deletion, held the messages intact (guides 4, 137), and within the backup's own databases further deleted content was recovered. The §6 backup was dated, so the messages were shown to have existed at that earlier time, and a later backup showed them gone, bracketing the deletion (guide 109). The §8 backup, a copy of the phone from before the deletion, had preserved what the current device no longer held. The lesson is §7's: a backup is a dated copy of the phone, so one made before a deletion frequently holds the deleted data intact, and comparing backups over time can date a deletion, making backups a powerful route to deleted messages and prior states that the current device cannot supply.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Not looking for backups:** the biggest miss, treating a locked or lost phone as the end without finding its backups (Example 1, §7).
- **Ignoring the encrypted backup:** overlooking that an encrypted local backup holds more than an unencrypted one (Example 2, §5).
- **Not obtaining the backup password:** failing to seek the password that unlocks the richer encrypted backup (§5, guide 117).
- **Assuming a backup is complete:** treating a backup as everything on the phone, when it may omit categories (§4).
- **Not dating the backup:** reading a backup as the phone's current state rather than its state when made (§6).
- **Missing historic backups:** overlooking older backups that preserve deleted data and prior states (Example 3, §7).
- **Altering a local backup:** examining a computer backup without preserving its integrity first (§3).
- **Overlooking iCloud backups:** searching computers but not reaching the iCloud backups lawfully (§6).

Technical limitations

- **Backups are not always complete:** some data is not backed up, and unencrypted backups omit sensitive categories: the scope limit (§4, §5).
- **Encrypted backups need the password:** without it, the richer backup is inaccessible (§5, guide 117).
- **A backup is a past state:** it reflects the phone when made, not later (§6).
- **iCloud access requires authority:** reaching iCloud backups needs lawful process (§6).
- **iOS evolves:** what backups include and how they are made changes with iOS, checked per version (§3).

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Was the phone backed up to a computer or to iCloud, and is the backup, and any backup password, available?
- Is there an encrypted local backup, which holds more, and can its password be obtained?
- Are there older backups that might hold deleted data or prior states?

Ask your opponent

- Please preserve and disclose all iTunes, Finder and iCloud backups of the device at Schedule 1, including encrypted local backups and any backup passwords, and older backups.
- Please confirm which backups are encrypted and provide the passwords for lawful access.
- Please confirm the dates of the backups and whether any have been deleted.

Ask your eDiscovery / forensic provider

- What backups exist, where, and which is the fullest source (is there an encrypted local backup)?
- What does each backup contain and omit, and how is it dated and authenticated?
- Can a backup supply what the locked device cannot, including deleted data?

SUGGESTED WORDING · INSTRUCTION FOR AN IOS BACKUP ANALYSIS

> "We instruct you to locate, preserve and analyse the backups of the Apple mobile device at Schedule 1, relevant to Schedule 2. Please: (1) locate all local backups (iTunes and Finder) on any computers the phone was synced to, and all iCloud backups in the account, including older and historic backups, and identify which are encrypted; (2) acquire the local backups forensically without alteration and obtain the iCloud backups lawfully, and establish and obtain any backup password, preferring an encrypted local backup as the fuller source since it includes sensitive categories (such as health data and saved passwords) that an unencrypted backup omits; (3) examine each backup for the relevant data, including deleted content within its databases, and recover data deleted from the phone from backups made before the deletion; (4) date each backup to when it was made, use older backups to evidence prior states and date deletions, and authenticate each backup's integrity and provenance; and (5) state plainly what each backup does and does not contain, and corroborate with the device and estate, so no absence is misread from a backup that did not include a category."

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 12 · QUICK CONTROL

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

The iOS backup checklist

- ☐ Local backups located on all synced computers
- ☐ iCloud backups reached lawfully through the account
- ☐ Older and historic backups identified
- ☐ Encryption status of each local backup established
- ☐ Backup password obtained; encrypted backup preferred
- ☐ Local backups acquired without alteration; integrity preserved
- ☐ Deleted data recovered from pre-deletion backups and databases
- ☐ Each backup dated and authenticated
- ☐ Scope stated: what each backup does and does not contain
- ☐ Findings corroborated with device and estate

Red flags

- A locked or lost phone treated as the end without finding backups: Example 1.
- An encrypted backup overlooked or its password not sought: Example 2.
- A backup assumed to be everything on the phone.
- A backup read as the current state, not dated.
- Historic backups holding deleted data ignored: Example 3.
- A local backup examined without preserving integrity.
- iCloud backups not reached lawfully.

When to involve a digital forensic expert

Whenever an iPhone is locked, lost, damaged or wiped, and as a matter of course alongside any device acquisition, because the backup so often holds what the device will not: the expert locates the local iTunes and Finder backups on synced computers and reaches the iCloud backups lawfully, identifying the historic ones (Example 1, §3), and, crucially, establishes which local backups are encrypted and obtains the password, preferring the encrypted backup as the fuller source since it includes health, password and other categories an unencrypted backup omits (Example 2, §5). Deleted data is recovered from backups made before the deletion and from the backups' own databases, prior states date changes, and each backup is dated and authenticated (Example 3, §7). The scope of each backup, what it does and does not contain, is stated plainly, and the findings are corroborated with the device and estate and reported under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, backup analysis turns the phone's shadow copies into evidence, so that a locked or lost iPhone rarely means the data is gone, and, in the one place iOS encryption helps rather than hinders, the encrypted backup gives the fullest picture of all.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 13 · COMMON QUESTIONS

Frequently asked questions

The phone is locked. Can a backup still help?

Very often yes (§2, §7, Example 1). Most iPhones are backed up, either to a computer (iTunes or Finder) or to iCloud, and a backup is a substantial copy of the phone that exists independently of the device. So when the phone is locked, lost, damaged or wiped, a backup can frequently be examined instead, supplying the messages, photos and app data the device will not give up. The first response to a difficult phone is therefore to find its backups, which routinely hold much of the same evidence.

Why would an encrypted backup contain more?

Because of how Apple designs local backups (§5, Example 2). Apple includes certain sensitive categories, such as health data and saved passwords, only when a local backup is encrypted; an unencrypted backup leaves those categories out. So an encrypted local backup actually holds more than an unencrypted one. Where the backup password is available, by cooperation or lawful means, the encrypted backup is the richer source. It is one of the few situations in iOS forensics where encryption works in the investigator's favour rather than against.

Is a backup a complete copy of the phone?

Substantial, but not always complete (§4). A backup holds a large part of the phone's data, messages, photos, app data, settings, but not necessarily every category, and an unencrypted backup omits sensitive categories. Local and iCloud backups can also differ in what they include. So a backup's scope is understood rather than assumed, its contents are stated plainly, and it is corroborated with the device and estate, so that the absence of something from a backup is not misread as its absence from the phone.

Can a backup recover deleted messages?

Often yes (§7, Example 3). A backup is a dated copy of the phone, so one made before a deletion frequently holds the deleted messages intact, and deleted content can also be recovered from the backup's own databases (guide 4). Comparing backups over time can date a deletion by showing when the data was present and when it was gone. So backups are a powerful route to deleted data and prior states, often reaching material the current device no longer holds, provided the backups have been preserved.

Where do we find the backups?

On computers and in the account (§3, §6). Local iTunes and Finder backups sit on the computers the phone was synced to, so those computers are located and examined, and a party may have a backup they have forgotten. iCloud backups sit in the user's Apple account and are reached through it by lawful process. A computer or account often holds several backups, including older ones and backups of other devices, so the relevant device's backups are identified among them and each is dated and authenticated.

Do we need the backup password?

For an encrypted local backup, yes (§5, §6, guide 117). An encrypted backup, which is the fuller source, is accessible with its password, obtained by the user's cooperation or by lawful means, so reaching it is a matter of the password rather than of breaking encryption. Where the password is not available, the unencrypted backup, iCloud and the device are relied on, with the omitted categories noted. Obtaining the password is worthwhile precisely because the encrypted backup holds more than any other backup source.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 14 · REFERENCE

Glossary

iOS backup
A copy of an iPhone's data held off the device.

Local backup
A backup on a computer via iTunes or Finder.

iTunes / Finder
The apps that make local backups.

iCloud backup
A backup stored in the user's Apple account.

Encrypted backup
A password-protected local backup that holds more.

Backup password
The password to an encrypted local backup.

Sensitive categories
Health, passwords and more, only in encrypted backups.

Historic backup
An older backup preserving a prior state.

Dated snapshot
A backup as the phone at the time it was made.

Authentication
Establishing a backup is genuine and unaltered.

Sources and authoritative references

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

- cflab.uk, digital forensics services (iTunes, Finder and iCloud backup analysis, encrypted-backup analysis, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (backup preservation and collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple support and Platform Security guide (iTunes/Finder and iCloud backups, encrypted-backup contents, backup encryption): support.apple.com, Platform Security · support.apple.com, encrypted backups
- Forensic Science Regulator, Code of Practice v2 (integrity, authentication and dating) and ISO/IEC 27037: gov.uk, FSR Code · iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35

DISCLAIMER

This publication provides general information about iOS backups as at August 2026. What backups contain, and how they are made, changes across iOS and macOS versions; a backup is a copy of the phone at the time it was made, is not necessarily complete, and an unencrypted local backup omits sensitive categories that an encrypted one includes. Encrypted backups require the backup password, obtained lawfully. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Backup analysis at the laboratory turns the phone's shadow copies into evidence, so that a locked or lost iPhone rarely means the data is gone. The local iTunes and Finder backups on any synced computers are located and acquired forensically, and the iCloud backups are reached lawfully through the account, including the historic backups a party may have forgotten (Example 1, §3). Crucially, the encryption status of each local backup is established and the password obtained, because an encrypted local backup holds more than an unencrypted one, Apple includes sensitive categories such as health data and saved passwords only when the backup is encrypted, so the encrypted backup is preferred as the fuller source, in the one situation where iOS encryption works in the investigator's favour (Example 2, §5). Data deleted from the phone is recovered from backups made before the deletion and from the backups' own databases, older backups evidence prior states and date deletions, and each backup is dated and authenticated (Example 3, §7). The scope of each backup, what it does and does not contain, is stated plainly, and the findings are corroborated with the device and the wider estate and 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 insight is that the phone is rarely the only copy of itself, and its backups, especially the encrypted one, frequently hold the fullest picture.

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