COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Android Backups: Local, Google and Manufacturer Cloud

Several Backups, Several Makers, Selective Contents: What a Backup Holds, What It Leaves Out, and Why It Is a First-Class Source

An Android phone can be backed up in several ways at once, and none of them is complete. Google's own backup, into the Google account, saves settings, app data for apps that opt in, and, for many devices, messages, call logs and photos. The manufacturer's cloud, Samsung Cloud and its equivalents, saves its own set, often including the maker's apps and, on Samsung, a Secure Folder backup under its own credential. A local backup, made through the maker's desktop tool or a backup app, may hold more still. Each is selective, each depends on the user's settings, and each holds the phone's contents at the moment it was made, so it preserves what the phone has since deleted, and it survives the phone. For the lawyer, this makes backups first-class sources on Android as on iOS, but sources that must be found, whose contents must be established rather than assumed, and which are reached lawfully. This guide sets out for UK lawyers what Android backups exist, what each holds and leaves out, how they are found and reached, and how they are read and deployed, especially when the device itself is gone or sealed.

⏱ 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. Android backup analysis is a central strand of its mobile work: finding the Google, manufacturer and local backups a device has made, establishing what each holds and leaves out, reaching them lawfully, comparing them with the live device to recover deleted data and date deletions, and treating them as first-class sources when the device itself is gone or sealed. The analysis is honest about each backup's selectivity and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | GOOGLE, MANUFACTURER & LOCAL BACKUPS | BACKUP-AS-SOURCE ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: an Android phone can be backed up several ways at once, to the Google account, to the manufacturer's cloud and to local backups, none of them complete and each selective according to the user's settings and each app's choices, yet each preserving the phone's contents at the moment it was made and surviving the phone, so backups are first-class sources that must be found, whose contents must be established rather than assumed, and which are reached lawfully.

The backups (§3): Google's backup into the account, the manufacturer's cloud (Samsung Cloud and equivalents), and local backups from desktop tools or backup apps. **What each holds (§4):** settings, opted-in app data, and for many devices messages, call logs and photos, with each backup's coverage differing and none complete. **Finding and reaching (§5):** backups located from the account, the maker's cloud and any computer, and reached lawfully by consent, process or production. **Reading (§6):** a backup is a prior state, so it recovers deleted data and, compared with the live device, dates deletions, with its selectivity stated. **Deployment (§7):** the backup as a source in its own right and as the route when the device is gone or sealed.

- **Several backups, none complete:** Google, manufacturer and local, each selective.
- **Settings decide contents:** what a backup holds depends on the user's and each app's choices.
- **A prior state that survives the phone:** preserving what the device has since deleted.
- **Find them and establish them:** never assume what a backup holds.
- **Reached lawfully:** consent, process to the provider, or production.

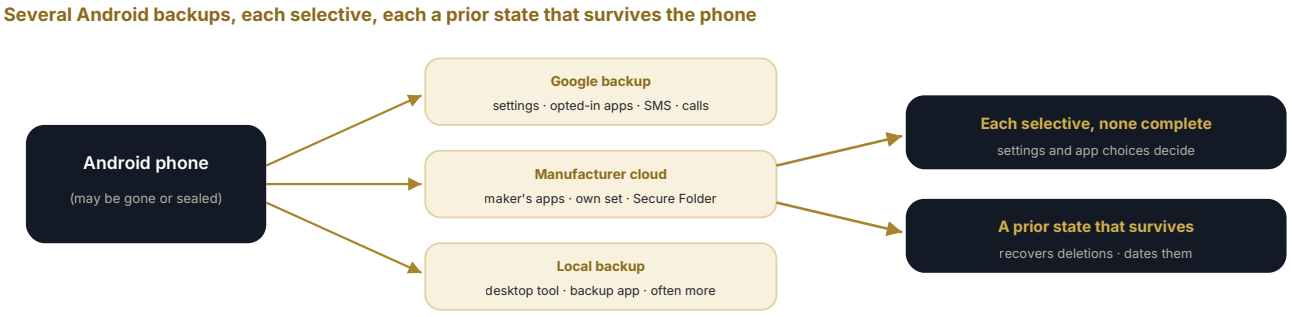

Figure 1 - an Android phone backs up to the Google account, the manufacturer's cloud and local backups, each selective and none complete, and each a prior state that survives the phone and recovers and dates deletions.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: several backups, none complete

The iPhone backups guide (guide 147) explained why a backup is a first-class source: it holds the phone's contents at the moment it was made, so it preserves what the phone has since deleted, it survives the loss or wiping of the phone, and, compared with the live device, it can date a deletion. Every one of those points applies to Android. What differs is that an Android phone rarely has one backup. It may have several at once, made by different systems to different places, and none of them is complete. Google's own backup saves into the Google account (guide 164): device settings, the data of apps that have opted in to backup, and, on many devices, SMS and call logs, with photos handled separately by Google Photos. The manufacturer's cloud, Samsung Cloud and the equivalents from other makers, saves its own set, typically the maker's apps and settings, sometimes messages and call logs, and, on Samsung, a backup of the Secure Folder under its own credential (guide 171). A local backup, made through the manufacturer's desktop tool or a third-party backup app, may hold more than either cloud, including app data the clouds do not take.

Two consequences follow for the lawyer. The first is that a backup's contents can never be assumed. Whether messages are in it, whether a given app's data is in it, whether photos are in it, all depend on the user's settings and on each app's own decision to opt in, so what a backup holds must be established for that backup rather than presumed from the fact that a backup exists. The second is that backups must be found. A Google backup is discoverable from the account; a manufacturer backup from the maker's cloud, under the user's manufacturer account; a local backup from whichever computer or app made it. Each is reached lawfully, by the account holder's consent, by lawful process to Google or the manufacturer, or by production in disclosure, and never by improper access. Once found and reached, a backup is read as what it is: a prior state of the phone, selective in its coverage, dated to the moment it was made, from which deleted data is recovered and deletions are dated, and which stands in for the device when the device is gone, wiped or sealed (guide 163). This guide sets out what Android backups exist, what each holds and leaves out, how they are found and reached, and how they are read and deployed.

§ 0 3 · THE BACKUPS

The backups: Google, manufacturer and local

- **Google backup:** Android's backup into the Google account, saving device settings, opted-in app data and, on many devices, SMS, call logs and contacts, made automatically when enabled (guide 164): the account backup.
- **Google Photos:** the photo and video library backed up separately to the account, so images are held even when the device backup does not include them (guide 166): the separate photo backup.
- **Manufacturer cloud:** Samsung Cloud and other makers' clouds saving the maker's apps, settings and often messages and call logs, under the user's manufacturer account, and on Samsung a Secure Folder backup under its own credential (guide 171): the maker's backup.
- **Local backups:** backups made through the manufacturer's desktop tool (Smart Switch and equivalents) or a backup app to a computer or SD card, often holding more than the clouds, including app data they omit (guide 166): the fuller local copy.
- **Several at once:** a phone commonly having Google, manufacturer and local backups simultaneously, each with different coverage and dates, so all are sought (§5): the multiple backups.

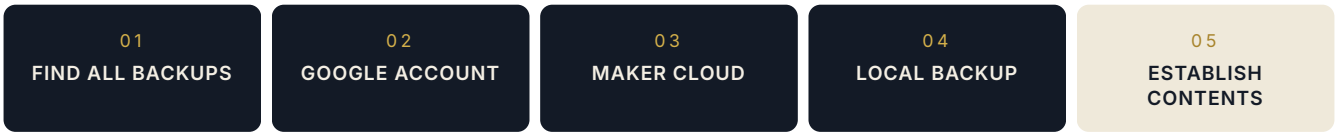

Figure 2 - find every backup, Google, manufacturer and local, and establish what each actually holds rather than assuming it.

§ 0 4 · WHAT EACH HOLDS

What each holds, and what it leaves out

- **Settings and configuration:** device settings, Wi-Fi networks, and system configuration in most backups, evidencing the phone's setup and the networks it knew (guide 168): the configuration record.
- **App data, selectively:** app data included only for apps that opt in to backup (guide 167), so some apps' data is present and others' absent, and a missing app is not proof it was unused: the selective app coverage.
- **Messages and calls, depending:** SMS, RCS and call logs included in many Google and manufacturer backups but not all, depending on device and settings (guide 165): the conditional communications.
- **Photos, separately:** photos usually handled by Google Photos or the maker's gallery sync rather than the device backup, so the photo backup is a separate source (guide 166): the separate media backup.
- **What is left out:** secure-messenger data, many apps' data, some system artefacts and, unless separately backed up, the Secure Folder, so a backup's silence about an app or item is read against its coverage, never as absence (§6): the honest gaps.

§ 0 5 · FINDING AND REACHING

Finding and reaching backups lawfully

- **From the Google account:** Google backups and their dates listed in the account, so their existence and currency are established there, reachable by consent, process to Google or production (guide 164): the account route.
- **From the manufacturer account:** manufacturer backups held in the maker's cloud under the user's manufacturer account, reachable by consent, process to the maker or production (guide 161): the maker route.
- **From computers and cards:** local backups found on the user's computers and SD cards, identified by the tool that made them, and imaged and analysed as files (guides 166, 141): the local route.
- **Lawfully, never improperly:** every backup reached by the account holder's consent, by lawful process, or by production, and never by guessing credentials or unauthorised access (guide 117): the lawful boundary.
- **Credentials for encrypted backups:** some backups (local, Secure Folder) encrypted with their own credential, sought lawfully as the key, as for the device itself (guides 163, 171): the backup's own key.

§ 0 6 · READING A BACKUP

Reading a backup: prior states, deletions and honest limits

- **A dated prior state:** a backup holding the phone's contents at the moment it was made, so it is read as a snapshot of that moment, dated and bounded (guide 147): the snapshot.
- **Recovering deleted data:** data deleted from the phone after the backup surviving in it intact, so the backup recovers what the device has lost (guide 170): the pre-deletion copy.
- **Dating deletions:** comparing a backup with the live device, or two backups with each other, bounding when a deletion occurred, so the removal itself becomes evidence (guide 109): the deletion dated.
- **Selectivity stated:** a backup's coverage established and its gaps stated, so an app or item absent from it is read against what the backup was set to include, never as proof of absence (§4): the honest coverage.
- **Reconciled with the device:** the backup reconciled with the live device and other backups, so the same item is not double-counted and differences are understood (guide 130): the reconciled sources.

§ 0 7 · DEPLOYMENT

Deployment: the backup as first-class source and fallback

- **The backup as a source in its own right:** a backup's contents, messages, app data, settings, used as evidence directly, with its date and coverage stated (§6): the backup as evidence.
- **The route when the device is gone:** backups reconstructing a lost, wiped or destroyed phone's contents, so the evidence survives the device (guide 147): the backup as fallback.
- **The route when the device is sealed:** Google and manufacturer backups reached lawfully regardless of the phone's lock, so a sealed device does not seal its backed-up contents (guide 163): the route around the vault.
- **Recovering what depth could not:** a backup supplying deleted data that the device's extraction depth, encryption or TRIM prevented recovering (guide 170): the depth workaround.
- **Lawful, honest presentation:** the backups found, reached lawfully, their coverage established, reconciled with the device, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the backup evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: backups are the preserved prior states of the estate, and on Android they are several and scattered, so mapping them is part of mapping the estate. The device holds its live contents at the acquired depth. But the Google account (guide 164) holds the Google backup and Google Photos; the manufacturer's cloud holds the maker's backup and, on Samsung, the Secure Folder backup; the user's computers and SD cards hold local backups from desktop tools and backup apps; the app providers hold their own cloud copies for apps that sync (guide 167); and the counterparts hold their side of communications regardless of any backup. The discipline is to find every backup, establish what each holds, reach it lawfully, and read it as a dated, selective prior state reconciled with the device and the other backups, so that deleted data is recovered from whichever backup predates the deletion and a deletion is dated by comparison. When the device is gone, the backups reconstruct it; when the device is sealed, the cloud backups are reached regardless; when one backup omits an app, another or the app's own cloud may include it; and the backups together give the estate its memory.

EVIDENCE	GOOGLE BACKUP	GOOGLE PHOTOS	MANUFACTURER CLOUD	LOCAL BACKUP	APP PROVIDER CLOUD	LIVE DEVICE
Settings / config	Y	n/a	Y	Y	n/a	Y: current
Messages / calls	Y: many devices	n/a	Y: often	Y: usually	Provider metadata	Y: at depth
App data	Opted-in apps only	n/a	Maker's apps, some others	Often more	Y: syncing apps	Y: at depth
Photos / media	Usually no	Y: library	Y: gallery sync	Y: often	n/a	Y
Secure Folder	No	No	Y: Samsung, own credential	Sometimes	Second accounts' clouds	Y: if opened

Fallback strategy in one line: find every backup, Google, Photos, manufacturer and local, establish each one's coverage, reach it lawfully, and reconcile it with the device; when the device is gone or sealed, or one backup omits an item, another usually holds it.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE THREE BACKUPS THAT TOGETHER HELD THE ANSWER

A party's phone had been wiped, and it seemed the evidence was lost. The §3 search found three backups: a §3 Google backup in the account holding settings, SMS and call logs (guide 164), a §3 Samsung Cloud backup holding the maker's apps and a Secure Folder backup under its own credential (guide 171), and a §3 local Smart Switch backup on the party's computer holding app data neither cloud had taken. §4 None was complete, but §6 reconciled together they reconstructed most of the wiped phone, and the local backup, made before a deletion, §6 recovered messages the later cloud backups lacked. The device was gone; its memory was in three places. The lesson is §2's and §8's: an Android phone often has several backups at once, each selective, so all are found and their coverage established, because together they reconstruct a lost device that no single backup could, and the oldest may hold what the later ones do not.

EXAMPLE 2 · THE BACKUP THAT WAS SILENT, READ CORRECTLY

A party argued that a messaging app's absence from the Google backup proved the party had never used it. The §4 selectivity discipline corrected this: the app had not opted in to Google backup, so its data would never appear there whether or not it was used, and the §6 backup's silence was read against its coverage, not as proof of absence (guide 167). The §8 app's own cloud and the §8 local backup, which did include it, showed extensive use. The backup had been silent because of a setting, not a fact. The lesson is §4's and §6's: a backup's contents depend on the user's settings and each app's choice to opt in, so an item's absence from a backup is read against what that backup was set to include, never as evidence that the item did not exist, and the other backups and clouds are checked.

EXAMPLE 3 · THE TWO BACKUPS THAT DATED THE DELETION

A matter turned on when a party had deleted certain messages. The §6 comparison answered it: a §3 Google backup from one date held the messages, a later §3 manufacturer backup did not, and the §6 live device held only remnants (guide 170), so the deletion was bounded between the two backup dates, well after the duty to preserve had arisen (guide 110). The backups, §5 reached lawfully by production, were §6 reconciled with each other and the device. The deletion itself became the evidence. The lesson is §6's: because each backup is a dated prior state, comparing two backups, or a backup with the live device, bounds when a deletion occurred, so the timing of a party's deletion, and its relationship to their preservation duties, is established from the backups' dates.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Assuming one backup:** the cardinal Android error, finding the Google backup and stopping, missing the manufacturer and local ones (Example 1, §3).
- **Assuming a backup's contents:** presuming messages, photos or an app's data are in a backup without establishing its coverage (Example 2, §4).
- **Reading a backup's silence as absence:** treating an item's absence from a selective backup as proof it did not exist (Example 2, §6).
- **Forgetting Google Photos is separate:** expecting photos in the device backup (§4).
- **Improper access:** reaching a backup by guessing credentials rather than lawfully (§5).
- **Not comparing backups:** failing to use two backups, or a backup and the device, to date a deletion (Example 3, §6).
- **Missing the Secure Folder backup:** not recognising that a manufacturer backup may hold the container under its own credential (§4, guide 171).
- **Double-counting:** counting the same item in the device and several backups as several (§6).

Technical limitations

- **No backup is complete:** each is selective by settings and app opt-in: the core limit (§2).
- **Coverage varies by maker and version:** what a backup includes differs by device (§4).
- **Encrypted backups need their key:** local and Secure Folder backups may require their own credential (§5).
- **A backup is only as recent as its date:** it holds nothing after it was made (§6).
- **Backups depend on the user having enabled them:** a phone may have none (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Was the phone backed up, and to where, Google, the manufacturer's cloud, a computer or SD card, and when?
- Were messages, photos and the relevant apps set to back up, so we know what each backup holds?
- Are the Google and manufacturer accounts, and any computer holding a local backup, available?

Ask your opponent

- Please preserve and disclose all backups of the device at Schedule 1, including Google backups, Google Photos, manufacturer cloud backups (including any Secure Folder backup) and local backups on any computer or card, with their dates and settings.
- Please confirm the backup settings in force, including which apps were set to back up.
- Please provide the credentials for any encrypted local or Secure Folder backup for lawful access.

Ask your eDiscovery / forensic provider

- What backups exist for this device, where, and from when?
- What does each backup actually hold and leave out, and how is it reached lawfully?
- What deleted data does a backup recover, and can the backups date the deletion?

SUGGESTED WORDING · INSTRUCTION FOR AN ANDROID BACKUP ANALYSIS

> "We instruct you to identify and analyse the backups of the Android device at Schedule 1 relevant to Schedule 2. Please, obtaining access lawfully (by consent, lawful process to Google or the manufacturer, or production) and never improperly: (1) find every backup, Google backups and Google Photos in the Google account, manufacturer cloud backups including any Secure Folder backup, and local backups on any computer or SD card, and record each one's date; (2) establish what each backup actually holds and leaves out, given the device, the user's settings and each app's opt-in, and never assume its contents or read an item's absence as proof it did not exist; (3) obtain lawfully the credential for any encrypted local or Secure Folder backup; (4) read each backup as a dated prior state, recover from it data since deleted from the device, and compare backups with each other and with the live device to bound when any deletion occurred; (5) reconcile the backups with the device and each other without double-counting; and (6) where the device is lost, wiped or sealed, reconstruct its contents from the backups, and present findings, with each backup's date and coverage stated, at honest confidence."

§ 12 · QUICK CONTROL

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

The Android backup checklist

- ☐ All backups sought: Google, Google Photos, manufacturer, local
- ☐ Each backup's date recorded
- ☐ Each backup's coverage established, not assumed
- ☐ Backups reached lawfully; encrypted backups' credentials obtained lawfully
- ☐ Secure Folder backup identified where present
- ☐ Deleted data recovered from pre-deletion backups
- ☐ Deletions dated by comparing backups and device
- ☐ An item's absence read against coverage, never as absence
- ☐ Backups reconciled with device and each other
- ☐ Device reconstructed from backups where lost or sealed

Red flags

- Only the Google backup found: Example 1.
- A backup's contents assumed: Example 2.
- An app's absence from a backup read as proof of non-use: Example 2.
- Photos expected in the device backup.
- A backup accessed improperly.
- Backups not compared to date a deletion: Example 3.
- The Secure Folder backup missed.

When to involve a digital forensic expert

Whenever an Android device has been lost, wiped or sealed, whenever deletion is in issue, and in truth whenever an Android device is examined at all, because its backups are several, scattered and selective, and only an expert can find and read them properly: the expert finds every backup, Google backups and Google Photos in the account, manufacturer cloud backups including any Secure Folder backup, and local backups on computers and cards, and records their dates (Example 1, §3, §5), and establishes what each actually holds and leaves out so that an item's absence from a selective backup is never read as proof it did not exist (Example 2, §4, §6). Each backup is reached lawfully, read as a dated prior state from which deleted data is recovered, and compared with the others and the device to bound when a deletion occurred (Example 3, §6); the backups are reconciled without double-counting; and where the device is gone or sealed they reconstruct its contents (§7). Findings are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Through **cflab.uk** and **e-discovery.uk**, backup work gives the Android estate its memory, finding the several

selective snapshots a phone leaves behind and reading them, honestly and lawfully, for what the device has since lost.

§ 13 · COMMON QUESTIONS

Frequently asked questions

How is an Android phone backed up?

Usually in several ways at once, none complete (§2, §3). Google's backup saves settings, opted-in app data and often messages and call logs into the Google account, with photos handled separately by Google Photos; the manufacturer's cloud, Samsung Cloud and its equivalents, saves the maker's apps and settings, often messages, and on Samsung a Secure Folder backup; and local backups made by the maker's desktop tool or a backup app may hold more than either. A phone commonly has all three, with different coverage and dates, so all are sought.

Does a backup contain everything on the phone?

No, every Android backup is selective (§4, Example 2). What it holds depends on the user's settings and on each app's own decision to opt in, so some apps' data is present and others' absent, messages are included on some devices and not others, photos usually sit in a separate Google Photos or gallery backup, and secure-messenger data and the Secure Folder are typically left out unless separately backed up. So a backup's contents are established for that backup, and an item's absence is read against its coverage, never as proof the item did not exist.

Why are backups so valuable?

Because each is a prior state that survives the phone (§6, §7). A backup holds the phone's contents at the moment it was made, so data deleted from the device afterwards survives in it intact; it survives the loss, wiping or destruction of the phone; cloud backups are reachable lawfully regardless of the phone's lock; and a backup can supply deleted data that the device's extraction depth, encryption or TRIM prevented recovering. So backups are first-class sources, and often the route to evidence when the device itself is gone or sealed.

Can a backup show when something was deleted?

Often, by comparison (§6, Example 3). Because each backup is dated, comparing a backup that holds an item with a later backup or the live device that lacks it bounds when the deletion occurred, so the timing of a party's deletion, and whether it followed a duty to preserve, is established from the backups' dates. Several backups from different dates give a finer timeline. This is one of the most useful things backups do, turning the deletion itself into evidence.

How are backups obtained lawfully?

By consent, lawful process or production (§5). Google and manufacturer backups are reached through the respective accounts, by the account holder's consent, by lawful process served on Google or the manufacturer, or by production in disclosure; local backups are found on the user's computers and cards and imaged as files; and the credential for an encrypted local or Secure Folder backup is sought lawfully as its key, exactly as for the device. A backup is never reached by guessing credentials or unauthorised access, which would be unlawful and inadmissible.

If the phone is wiped, can the backups rebuild it?

Often substantially (§7, Example 1). Because a phone commonly has Google, manufacturer and local backups with different coverage, reconciling them together frequently reconstructs most of a wiped device's contents, settings, messages, app data and photos, with the oldest backup sometimes holding what the later ones lack. Google Photos and the app providers' own clouds add more. No reconstruction is complete, and what the backups cannot replace is stated honestly, but a wiped phone with backups behind it is rarely a lost case.

§ 14 · REFERENCE

Glossary

Google backup
Android's backup of settings and opted-in data to the Google account.

Google Photos
The separate backup of the photo library.

Manufacturer cloud
A maker's backup service (e.g. Samsung Cloud).

Local backup
A backup to a computer or card via a desktop tool or app.

Smart Switch
Samsung's transfer and backup tool.

Opt-in backup
An app's choice whether its data is backed up.

Selective coverage
What a backup includes, per settings and opt-in.

Prior state
A backup's snapshot of the phone at its date.

Deletion dating
Bounding a deletion by comparing backups.

Secure Folder backup
A container backup under its own credential.

Sources and authoritative references

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

- cflab.uk, digital forensics services (Google, manufacturer and local backup analysis, backup-as-source and deletion dating, 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 identification and lawful 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
- Google, Android backup help and Auto Backup documentation; Samsung, Samsung Cloud and Smart Switch: support.google.com, back up and restore · developer.android.com, Auto Backup · samsung.com, backup and restore
- Forensic Science Regulator, Code of Practice v2 (lawful handling and honest reporting) and ISO/IEC 27037: gov.uk, FSR Code · iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35 · UK GDPR: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Backup work at the laboratory gives the Android estate its memory. Because an Android phone is commonly backed up in several ways at once, every backup is sought: Google backups and Google Photos in the Google account (guide 164), manufacturer cloud backups including, on Samsung, a Secure Folder backup under its own credential (guide 171), and local backups made by desktop tools or backup apps to the user's computers and SD cards (guide 166), each with its date recorded (Example 1). Because every backup is selective, what each actually holds and leaves out is established from the device, the user's settings and each app's opt-in, so that an item's absence from a backup is read against its coverage and never as proof the item did not exist (Example 2, guide 167). Each backup is reached only lawfully, by consent, lawful process to Google or the manufacturer, or production, with the credentials for encrypted backups sought lawfully as their keys (guides 117, 163). Each is read as a dated prior state from which data since deleted from the device is recovered (guide 170), and backups are compared with each other and with the live device to bound when a deletion occurred, turning the deletion into evidence (Example 3, guide 109). The backups are reconciled with the device and each other without double-counting, and where the device is lost, wiped or sealed they reconstruct its contents, with what they cannot replace stated honestly. Findings are reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding rule is the block's own applied to memory: several backups, none complete, so find them all, establish each, and read them together.

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