COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Android Acquisition: Logical, File System and Physical

Three Depths of Extraction, and Why the Method Chosen Decides What the Court Will Ever See

On Android, more than any other platform, the method of acquisition decides the evidence. A logical extraction takes what the device is willing to hand over through its ordinary interfaces: a useful but partial view. A file-system extraction reaches the device's storage itself, including app databases and, often, deleted data. A physical extraction captures the raw storage bit for bit, the most complete view, reaching everything the file system holds and more, but available on fewer and fewer modern devices. Which of these is possible depends on the particular phone, and the gap between them is not a matter of degree but of kind: material that a logical extraction simply cannot see may be plentiful in a physical one. For the lawyer, this makes acquisition depth a question to ask about every Android device, because a report built on a shallow extraction is silent about far more than it says. This guide sets out for UK lawyers the three depths of Android acquisition, what each reaches, how the device decides which is possible, and how to read a report in the light of the method that produced it.

⏱ 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 acquisition is at the core of its mobile work: assessing which of the logical, file-system and physical depths a given device permits, obtaining the deepest lawful extraction available, and reporting precisely what that depth reached and what it could not, so that no one mistakes a shallow extraction's silence for absence. The analysis preserves integrity throughout and is reported under CPR Part 35 and CrimPR Part 19, with the acquisition method and its limits stated plainly.

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

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: on Android the acquisition method decides the evidence, a logical extraction takes only what the device hands over, a file-system extraction reaches the storage and app databases including deleted data, and a physical extraction captures the raw storage bit for bit, and the gap between them is one of kind, not degree, so the depth must be asked about for every device and every report.

The three depths (§3): logical (what the device offers through its interfaces), file system (the storage and databases, often with deleted data), and physical (the raw storage, most complete). **What the device decides (§4):** which depth is possible depends on the specific phone, its version, security state and lock, with physical increasingly rare on modern devices. **Integrity (§5):** whatever the depth, the extraction is hashed, verified and its method recorded, so it is accountable. **Reading a report (§6):** every finding, and every silence, is read in the light of the method's reach. **Deployment (§7):** choosing the deepest lawful depth the device permits, obtaining it soundly, and defending it with its limits stated.

- **The method decides the evidence:** depth governs what the court will ever see.
- **Three depths:** logical, file system, physical, each reaching more than the last.
- **A gap of kind, not degree:** a shallow extraction cannot see what a deep one holds.
- **The device decides:** model, version and security state set the ceiling.
- **Read the report by its method:** silence in a shallow extraction is not absence.

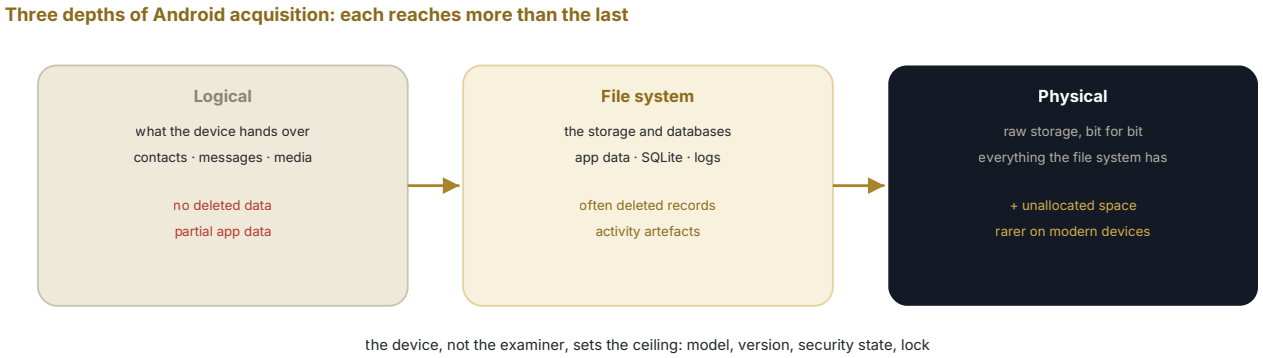

Figure 1 - logical, file-system and physical acquisition each reach more than the last, from what the device hands over to the raw storage itself, and the device's model, version and security state set the ceiling.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the method decides the evidence

The iPhone block explained that the depth of an extraction governs what is seen (guide 146). On Android, the point is sharper still, because the range of depths is wider and which one is possible varies more from phone to phone (guide 161). There are three broad depths. A logical extraction asks the device, through its ordinary interfaces, to hand over its data, and takes what the device is willing to give: contacts, messages, call logs, media and some app data. It is quick and available on most devices, and it is also partial, because the device hands over only what those interfaces expose, and never the deleted material or the internal databases behind them. A file-system extraction goes deeper, reaching the device's storage itself: the app databases, the logs, the internal files, and, because these are SQLite databases, very often the deleted records still lingering within them (guide 155). A physical extraction goes deeper again, capturing the raw storage bit for bit, so that it reaches everything the file system holds and, in addition, the unallocated space where deleted files and fragments survive.

The crucial thing to grasp is that the differences between these are not differences of degree, as though a logical extraction were a slightly smaller version of a physical one. They are differences of kind. A deleted message that a physical or file-system extraction recovers in full does not appear faintly in a logical extraction; it does not appear at all. The internal database that reveals an app's real history is simply not there in the logical view. So a report built on a logical extraction is silent about far more than it says, and its silence must never be mistaken for absence. Which depth is possible is not the examiner's choice but the device's: its manufacturer, model, Android version, security patch level, security hardware and lock state together set a ceiling, and on modern, fully patched devices that ceiling is often lower than on older ones, with physical extraction in particular becoming rare. For the lawyer, all this makes acquisition depth a question to ask about every Android device and every Android report: what method produced this, what could it reach, and what could it not? This guide sets out the three depths, what each reaches, how the device decides which is possible, and how to read a report in the light of the method that produced it.

§ 0 3 · THE THREE DEPTHS

The three depths and what each reaches

- **Logical: what the device hands over:** data obtained through the device's ordinary interfaces, contacts, messages, call logs, media and some app data, quick and widely available but partial, never reaching deleted data or the internal databases (guide 146): the surface view.
- **File system: the storage itself:** the device's file system reached, app databases, logs and internal files, and with them, very often, deleted records lingering in SQLite (guide 155), and the activity artefacts (guide 154): the internal view.
- **Physical: the raw storage:** the storage captured bit for bit, reaching everything the file system holds plus unallocated space with deleted files and fragments (guide 4), the most complete view, but rare on modern devices: the complete view.
- **Deleted data is the great divide:** deleted material absent from a logical extraction, often present in a file-system one, and most fully present in a physical one, so the depth decides whether deletion is defeated (guide 155): the deletion divide.
- **Each includes the last:** a deeper extraction containing what a shallower one would, so the deepest lawful depth is always preferred where the device permits it (§7): the inclusive hierarchy.

Figure 2 - the three depths in order, each including the last, with deleted data the great divide between them, and every extraction hashed and verified.

§ 0 4 · WHAT THE DEVICE DECIDES

How the device decides which is possible

- **Model and manufacturer:** the specific model and maker governing which methods exist for it at all, since methods are developed device by device (guide 161): the model ceiling.
- **Version and patch level:** the Android version and security patch closing or opening routes, so an update can lower the ceiling overnight (guide 161): the version ceiling.
- **Security hardware and encryption:** the security chip and file-based encryption governing whether storage can be read and decrypted, so modern hardware often limits depth (guide 133): the hardware ceiling.
- **Lock state and credentials:** whether the device is locked and whether the passcode is available often deciding between a full file system and a shallow or no extraction (guide 145): the lock ceiling.
- **Assessed, not assumed:** the achievable depth assessed for this device rather than assumed, and expectations set from that assessment (guide 161): the per-device answer.

§ 0 5 · INTEGRITY AND METHOD

Integrity, verification and the record of method

- **Hash the extraction:** the extracted data hashed at acquisition and verified thereafter, so any alteration is detectable and the evidence's integrity is demonstrable (guides 2, 3): the integrity anchor.
- **Record the method:** the method, tool, version, depth and any credentials or settings used documented, so the extraction is reproducible and its reach understood (guide 100): the method record.
- **Record what was not reached:** the limits of the method, what it could not access, recorded as carefully as what it obtained, so silence is explained (§6): the honest scope.
- **Preserve the device state:** the device's state before and after, and any changes the method necessarily made, documented, so the process is transparent (guide 145): the state record.
- **Validated tools and methods:** tools and methods validated for the device and version, as the Forensic Science Regulator's Code expects, so results are reliable (guide 100): the validated process.

§ 0 6 · READING A REPORT

Reading a report in the light of its method

- **Ask what method produced it:** the first question of any Android report, since its reach bounds every finding and every silence (§2): the method question.
- **Silence is not absence:** the absence of a message, record or app in a logical extraction meaning only that the method did not reach it, never that it does not exist (guide 146): the cardinal reading rule.
- **Deleted data needs depth:** a report claiming no deleted data, or no evidence of deletion, read against whether its method could have found any (guide 155): the deletion check.
- **Compare depths across parties:** reports from different parties, or different times, compared for method, since a deeper extraction may reveal what a shallower one missed (§7): the cross-report comparison.
- **Challenge the shallow report:** a report built on a shallow extraction, where a deeper one was feasible, challenged and the deeper extraction sought (§7): the depth challenge.

§ 0 7 · DEPLOYMENT

Deployment: choosing, obtaining and defending the depth

- **Choose the deepest lawful depth:** the deepest extraction the device permits and the matter warrants chosen, since it includes all shallower ones (§3): the maximised depth.
- **Obtain it soundly:** the extraction obtained by validated methods with integrity preserved and the method recorded (§5): the sound extraction.
- **Seek a deeper extraction where it matters:** where a party's report rests on a shallow extraction and deleted or app data is in issue, a deeper extraction sought, by agreement or order (guide 6): the depth pursued.
- **Defend the depth obtained:** the method and its reach explained, and its limits stated, so the extraction is defensible and its silences understood (§6): the defended method.
- **Fill from the estate:** where the device's ceiling is low, the Google account, backups and estate supplying what the extraction could not reach (§8): the estate deployed.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the depth of extraction bounds what the device yields, so the estate is the way to reach past a device whose ceiling is low. The device holds what the achievable depth can reach. But the Google account (guide 161) syncs messages, photos, backups and app data that a shallow extraction may not reach on the device; local and cloud backups hold earlier states, including deleted material from before deletion; the manufacturer's cloud holds backups and synced data; a paired wearable holds shared data; the counterparts hold their side of communications; and the app providers and carriers hold records. The discipline is to treat the extraction depth as one dimension of the enquiry and the estate as the other, so that where the device permits only a logical extraction, the account, backups and counterparts supply the deleted messages, app data and history that the device's ceiling withheld. When the depth is shallow, the estate is deep; when the device is sealed, the cloud and counterparts are the route; and a low ceiling on the device is not a low ceiling on the evidence.

EVIDENCE	LOGICAL EXTRACTION	FILE-SYSTEM EXTRACTION	PHYSICAL EXTRACTION	GOOGLE ACCOUNT / BACKUPS	COUNTERPART / PROVIDER
Current messages	Y	Y	Y	Y: if synced / backed up	Y: their side
Deleted messages	No	Often (SQLite)	Y: incl. unallocated	Y: pre-deletion backup	Y: their copy
App internal data	Partial	Y: databases	Y	Y: app backups	App provider
Activity artefacts	Limited	Y	Y	Some	n/a
Deleted files / fragments	No	Some	Y: unallocated	Earlier backups	n/a

Fallback strategy in one line: treat extraction depth and the estate as two dimensions; where the device's ceiling is low, the Google account, backups and counterparts supply the deleted and internal data the shallow extraction could not reach.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE REPORT THAT WAS SILENT ABOUT WHAT IT COULD NOT SEE

A party's expert report, built on a §3 logical extraction, stated that no relevant messages existed on the device. The §6 method question exposed the flaw: a logical extraction cannot reach deleted messages or the internal databases, so its silence meant only that the method had not reached them, not that they did not exist (guide 146). A §7 deeper extraction was sought and obtained, and the §3 file-system extraction recovered the deleted messages from SQLite remnants (guide 155). The §6 shallow report had mistaken silence for absence. The lesson is §6's: every Android report is read in the light of the method that produced it, and a logical extraction's silence is never absence, so a report that declares nothing exists is challenged on its depth, and a deeper extraction sought where the device permits it.

EXAMPLE 2 · THE DEVICE WHOSE CEILING WAS LOW, AND THE ESTATE THAT WAS NOT

A modern, fully patched flagship §4 permitted only a logical extraction; its security hardware and patch level set a low ceiling. The §7 estate reached past it: the §8 Google account held synced messages and app backups, a cloud backup from before a deletion held the deleted material, and the counterpart's device held the other side of the conversations (guide 161). The §7 limits of the device's extraction were stated honestly, and the evidence the device's ceiling withheld was obtained from the estate. A low ceiling on the device was not a low ceiling on the evidence. The lesson is §8's: extraction depth and the estate are two dimensions of the enquiry, so where the device permits only a shallow extraction, the Google account, backups and counterparts frequently supply the deleted and internal data the device could not, and the estate is mapped early precisely for this.

EXAMPLE 3 · THE METHOD THAT WAS RECORDED, AND THE CHALLENGE THAT FAILED

An extraction was challenged on the ground that its integrity and reach were unknown. The §5 record of method answered the challenge: the extraction had been hashed at acquisition and verified since, the method, tool, version and depth were documented, the device's state before and after was recorded, and what the method could not reach had been stated as carefully as what it obtained. Because the §5 method was validated for the device and version and its scope honestly bounded, the §7 extraction was defensible and the challenge failed. The lesson is §5's: whatever the depth, an extraction is defended by its record, hashed and verified for integrity, documented in method and reach, transparent about the device's state and honest about its limits, so that a challenge to integrity or scope meets a complete answer.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Reading silence as absence:** the cardinal error, treating a logical extraction's gaps as proof nothing exists (Example 1, §6).
- **Not asking the method:** accepting a report without establishing what depth produced it (§6).
- **Settling for a shallow extraction:** not seeking the deeper depth the device permits when deleted or app data matters (§7).
- **Assuming the depth:** promising a physical extraction the device cannot give (§4).
- **Ignoring the estate when the ceiling is low:** stopping at the device's limit instead of reaching past it (Example 2, §8).
- **Not recording the method and limits:** leaving the extraction open to challenge on integrity or scope (Example 3, §5).
- **Using unvalidated tools:** relying on methods not validated for the device and version (§5).
- **Letting the device change:** allowing an update or lock to lower the ceiling before acquisition (§4, guide 161).

Technical limitations

- **The device sets the ceiling:** the achievable depth is the device's decision, not the examiner's: the core limit (§4).
- **Physical is increasingly rare:** modern devices seldom permit raw storage capture (§3).
- **Encryption bounds depth:** file-based encryption and security hardware limit what can be read (§4).
- **Lock state can seal the device:** without credentials, depth may collapse to little or nothing (§4).
- **Methods evolve:** what is possible changes with tools, devices and versions (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Does the matter turn on deleted messages, app history or internal data that only a deeper extraction can reach?
- Is the device preserved and unlocked, or the passcode available, so the deepest depth remains possible?
- Is the Google account and are backups available, to reach past a low device ceiling?

Ask your opponent

- Please disclose the acquisition method, tool, version and depth (logical, file system or physical) used for the device at Schedule 1, and what the method could not reach.
- Please disclose the hash values and verification of the extraction and the record of the device's state.
- Where your extraction is logical and deleted or app data is in issue, please agree to a deeper extraction or explain why the device does not permit one.

Ask your eDiscovery / forensic provider

- What depth does this device permit, and what would each depth reach and miss?
- Has the deepest lawful depth been obtained, and is its method, integrity and scope fully recorded?
- Where the ceiling is low, what does the estate supply?

SUGGESTED WORDING · INSTRUCTION FOR AN ANDROID ACQUISITION

> "We instruct you to acquire the Android device at Schedule 1 relevant to Schedule 2. Please: (1) assess which acquisition depths (logical, file system, physical) this specific device permits, given its model, version, patch level, security hardware and lock state, and advise what each would reach and miss; (2) obtain the deepest lawful extraction the device permits and the matter warrants, by validated methods, preserving the device from locking, the network, remote wipe, updates and use beforehand; (3) hash the extraction at acquisition and verify it, and record the method, tool, version, depth, credentials used, the device's state before and after, and what the method could not reach; (4) state plainly the limits of the depth obtained, so that no absence of data is read as proof that it does not exist; and (5) where the device's ceiling is low, identify and use the Google account, backups, manufacturer cloud and counterparts to supply the deleted and internal data the extraction could not reach, and present findings at honest confidence with the method explained."

§ 12 · QUICK CONTROL

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

The Android acquisition checklist

- ☐ Device preserved from locking, network, wipe, updates and use
- ☐ Achievable depths assessed for this specific device
- ☐ Deepest lawful depth obtained by validated methods
- ☐ Extraction hashed at acquisition and verified
- ☐ Method, tool, version, depth and credentials recorded
- ☐ Device state before and after documented
- ☐ What the method could not reach recorded
- ☐ Every report read in the light of its method
- ☐ Silence in a shallow extraction never read as absence
- ☐ Estate used to reach past a low device ceiling

Red flags

- A logical extraction's silence treated as proof of absence: Example 1.
- A report accepted without knowing its method.
- A shallow extraction settled for when deeper was possible.
- A depth promised that the device cannot give.
- The estate ignored when the ceiling is low: Example 2.
- Method, hashes or limits not recorded: Example 3.
- Unvalidated tools or a device allowed to change state.

When to involve a digital forensic expert

Before any Android acquisition, and whenever an Android report is received, because the method decides the evidence and only an expert can assess, obtain and read it properly: the expert assesses which depths this specific device permits, given its model, version, security hardware and lock state (§4), preserves it so the ceiling does not fall, and obtains the deepest lawful extraction the device permits by validated methods, hashed, verified and fully documented in method, reach and limits (Example 3, §5). Every report is read in the light of its method, so a logical extraction's silence is never taken for absence and a deeper extraction is sought where the device permits and the matter needs it (Example 1, §6, §7); and where the device's ceiling is low, the Google account, backups and counterparts are used to reach past it (Example 2, §8). Findings are reported at honest confidence with the method explained, under CPR Part 35 or CrimPR Part 19. This guide continues the Android block. Through **cflab.uk** and **e-discovery.uk**, Android acquisition work obtains the most the device will give, records precisely what that reached and what it could not, and ensures that no court is left to mistake a shallow extraction's silence for the truth.

§ 13 · COMMON QUESTIONS

Frequently asked questions

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

Depth, and it is a difference of kind (§3). A logical extraction takes what the device hands over through its ordinary interfaces, contacts, messages, media and some app data, but never deleted data or internal databases. A file-system extraction reaches the storage itself, app databases, logs and internal files, and often deleted records within them. A physical extraction captures the raw storage bit for bit, reaching everything plus unallocated space with deleted files and fragments. Each includes the last, so the deepest lawful depth the device permits is always preferred.

Why does the acquisition method matter so much for the evidence?

Because a shallow extraction cannot see what a deep one holds (§2, §6, Example 1). A deleted message recovered in full by a file-system or physical extraction does not appear faintly in a logical one; it does not appear at all, and neither does the internal database that reveals an app's real history. So a report built on a logical extraction is silent about far more than it says, and its silence must never be mistaken for absence. The method bounds every finding and every silence, which is why it is the first question to ask of any Android report.

Can the examiner just choose the deepest method?

No, the device sets the ceiling (§4). Which depths are possible depends on the specific phone's manufacturer, model, Android version, security patch level, security hardware and lock state, and these are the device's decision, not the examiner's. Modern, fully patched devices with strong security hardware often permit only a logical extraction, and physical extraction has become rare. So the achievable depth is assessed for the device, the deepest lawful option it permits is chosen, and where the ceiling is low the estate is used to reach past it.

The other side's report says nothing was found. Should we accept that?

Not without knowing the method (§6, Example 1). If the report rests on a logical extraction, its finding that nothing exists means only that the shallow method did not reach anything, and deleted messages, app history and internal data may all be present and recoverable at a deeper depth. So the method, tool, depth and limits are demanded, and where the device permits a deeper extraction and deleted or app data is in issue, that deeper extraction is sought by agreement or order. A shallow report's silence is a reason to dig, not to stop.

How is an extraction made defensible?

By its record (§5, Example 3). The extraction is hashed at acquisition and verified thereafter, so its integrity is demonstrable; the method, tool, version, depth and credentials are documented, so it is reproducible; the device's state before and after is recorded, so the process is transparent; the tools and methods are validated for the device and version; and what the method could not reach is stated as carefully as what it obtained. An extraction so recorded meets a challenge to integrity or scope with a complete answer.

What if the device only permits a shallow extraction?

Then the estate reaches past it (§8, Example 2). A low ceiling on the device is not a low ceiling on the evidence: the Google account syncs messages, photos, backups and app data; local, cloud and manufacturer backups hold earlier states including material from before a deletion; a paired wearable holds shared data; and counterparts and providers hold their records. Mapped early, these frequently supply the deleted and internal data the shallow extraction could not reach, with the device's own limits stated honestly alongside what the estate provided.

§ 14 · REFERENCE

Glossary

Logical extraction
Data the device hands over via its interfaces.

File-system extraction
Acquisition of the device's storage and databases.

Physical extraction
A bit-for-bit capture of the raw storage.

Unallocated space
Storage holding deleted files and fragments.

Depth
How much of the device an extraction reaches.

Ceiling
The deepest extraction a device permits.

Hash
A fingerprint proving an extraction is unaltered.

Validated method
A method tested as reliable for the device.

Record of method
Documentation of tool, depth and limits.

Silence is not absence
A shallow method's gap proves nothing.

Sources and authoritative references

The acquisition 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, file-system and physical Android acquisition, depth-aware reporting, 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 03 · Preservation (forensically sound acquisition as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/preservation
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (method validation, integrity and honest reporting) and ISO/IEC 27037 (acquisition and preservation): gov.uk, FSR Code · iso.org, 27037
- NIST, Guidelines on Mobile Device Forensics (SP 800-101) and Android security documentation: csrc.nist.gov, SP 800-101 · source.android.com, security
- NPCC digital evidence guidance · CPR Part 35 · PD 57AD: npcc.police.uk · justice.gov.uk, Part 35 · justice.gov.uk, PD 57AD

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Android acquisition work at the laboratory obtains the most the device will give and records precisely what that reached and what it could not. Each device is first preserved from locking, the network, remote wipe, updates and use, so its ceiling does not fall before acquisition, and the depths it permits, logical, file system or physical, are assessed for this specific device given its model, version, patch level, security hardware and lock state (guide 161). The deepest lawful extraction the device permits and the matter warrants is obtained by validated methods, hashed at acquisition and verified thereafter, with the method, tool, version, depth, credentials, the device's state before and after, and what the method could not reach all documented, so the extraction meets any challenge to its integrity or scope with a complete answer (Example 3). Every report, the laboratory's own or another party's, is read in the light of the method that produced it, so a logical extraction's silence is never taken for absence and a deeper extraction is sought where the device permits and the matter needs it (Example 1, guide 146). Where the device's ceiling is low, the Google account, backups, manufacturer cloud and counterparts are used to supply the deleted and internal data the extraction could not reach (Example 2), and findings are reported at honest confidence with the method explained, 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 simple: on Android the method decides the evidence, so the deepest depth is obtained, its reach is recorded, and its silence is never mistaken for the truth.

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