



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Android Usage, Activity and System Artefacts

Usage Stats, Digital Wellbeing, Notifications and Logs: The Phone's Own Record of What Was Done, and When

Just as an iPhone keeps a diary of its own use in the KnowledgeC and Biome databases, an Android phone keeps its own record of what was done with it. Android's usage statistics track which apps were used and for how long; Digital Wellbeing and its manufacturer equivalents keep a finer-grained history of screen time and app sessions; the notification history records what arrived and when; and a family of system databases and logs records screen and lock events, battery and charging, connections, and installations. Together these reconstruct whether the phone was in use at a given moment, which app was open, and how the user's activity flowed through the day, a powerful complement to the content the phone holds. As on iOS, these artefacts are technical, vary by manufacturer and version, and age out, so they demand expert interpretation and honesty about their reach. This guide sets out for UK lawyers what Android's usage and system artefacts record, how they reconstruct a device-activity timeline, how they vary and rotate, and how their evidence is corroborated and read honestly.

© 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 usage and system-artefact analysis is a specialist strand of its mobile work: reconstructing from usage statistics, Digital Wellbeing, notification history and system logs a fine-grained record of app use, screen and lock state and device events, interpreting these manufacturer-dependent stores by expertise, and stating honestly how far back they reach. The analysis shows what a device was doing and when, corroborated across the estate, and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

USAGE STATS & DIGITAL WELLBEING

DEVICE-ACTIVITY RECONSTRUCTION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the phone keeps a diary here too
- 03 What Android's usage and system artefacts record
- 04 Reconstructing the device-activity timeline
- 05 Manufacturer variation and expert interpretation
- 06 Rotation, corroboration and honest limits
- 07 Deployment: proving what the device was doing
- 08 Source architecture: where else the evidence lives
- 09 Worked examples
- 10 Common mistakes and technical limitations
- 11 Questions to ask · Suggested wording
- 12 Checklist and red flags · When to involve a digital forensic expert
- 13 Frequently asked questions
- 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

The headline point: an Android phone keeps its own record of what was done with it, usage statistics of app use, Digital Wellbeing's finer history of screen time and sessions, the notification history, and system databases and logs of screen, lock, battery, connection and installation events, which together reconstruct whether the phone was in use, which app was open and how activity flowed, but vary by manufacturer, demand expert interpretation, and age out.

What they record (§3): app usage and duration, screen and lock events, notifications, battery and charging, connections and installations, at fine time resolution. **The timeline (§4):** combined, these reconstruct a detailed record of what the device was doing and when. **Variation and interpretation (§5):** the artefacts differ by manufacturer and version and are cryptic, so they demand specialist interpretation. **Rotation and limits (§6):** older entries age out, so a gap is not proof of inactivity, and findings are corroborated. **Deployment (§7):** proving whether a device was in use and what was being done at a time, at honest confidence.

- **The phone keeps a diary here too:** Android's counterpart to KnowledgeC and Biome.
- **Usage, wellbeing, notifications, logs:** a layered record of activity.
- **Varies by manufacturer:** the artefacts differ by maker and version.
- **Expert-read and rotating:** cryptic stores that age out; gaps are not inactivity.
- **Corroborate honestly:** the activity record is cross-checked and read at honest confidence.

Android's own diary of what was done, layered and expert-read

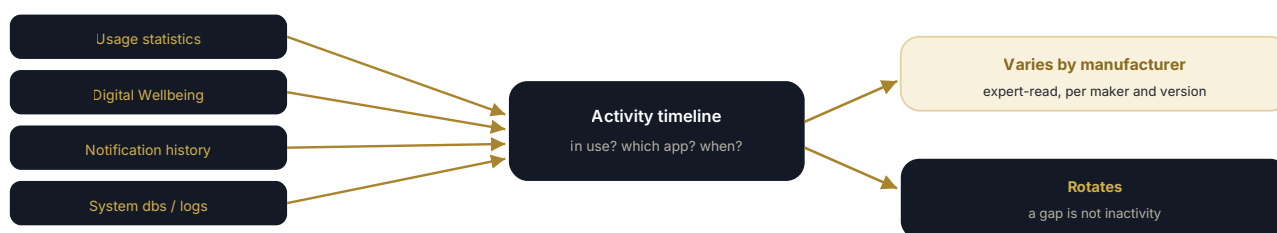


Figure 1 - usage statistics, Digital Wellbeing, notification history and system logs reconstruct an Android activity timeline that varies by manufacturer, demands expert reading and rotates, so a gap is never inactivity.

The problem in plain English: the phone keeps a diary here too

The iPhone block explained that an iPhone keeps a fine-grained diary of its own use in the KnowledgeC and Biome databases, recording which apps were used and when, when the screen was on and the phone locked or unlocked, and much more (guide 154). Android keeps a diary too, and in some respects a more visible one, because parts of it are shown to the user. Android's usage statistics service tracks which apps were used, when and for how long, so the system can rank and manage them. Digital Wellbeing, Google's screen-time feature, and the manufacturers' equivalents keep a finer history of screen time, app sessions and unlocks, kept precisely so the user can see how they use their phone. The notification history records what notifications arrived and when. And beneath these, a family of system databases and logs records screen-on and screen-off events, locks and unlocks, battery and charging, Wi-Fi and Bluetooth connections, app installations and removals, and a great deal else.

Assembled, these reconstruct what the device was doing moment to moment: whether it was actively in use at a given time or sitting idle, which app was open and for how long, when it was locked and unlocked, what reached it and what it connected to, and how its user's activity flowed through the day. That is a powerful complement to the content the phone holds, because it can corroborate or contradict an account of what someone was doing, and when, with a precision that content alone rarely offers. But the same cautions that governed the iPhone's activity databases apply here, and one applies more strongly. These artefacts are technical and often cryptic, so they demand expert interpretation rather than face-value reading. They age out, keeping only a window of history, so a gap is not proof that nothing happened. And, because Android is a fragmented landscape (guide 161), they vary by manufacturer and version far more than their iOS counterparts: the same information may be kept in different stores, formats and retention windows on a Samsung, a Pixel and a Xiaomi, so the specific device's artefacts must be understood, not assumed from Android in general. The task, then, is to recover and correctly interpret these usage and system artefacts for the device in hand, to reconstruct the activity timeline they support, to state their variation, rotation and limits honestly, and to corroborate the picture. This guide sets out how.

§ 0 3 · WHAT THEY RECORD

What Android's usage and system artefacts record

- **Usage statistics:** Android's record of which apps were used, when, and for how long, kept by the system to rank and manage apps, so app engagement across the day is traced (guide 167): the app-use record.
- **Digital Wellbeing and equivalents:** Google's and the manufacturers' screen-time features keeping a finer history of app sessions, screen time and unlocks, kept for the user to see, so a detailed usage picture exists (§5): the wellbeing record.
- **Notification history:** the record of notifications received, from which app and when, so what reached the user is evidenced, sometimes including content previews (guide 165): the notification record.
- **Screen, lock and power events:** system logs and databases recording screen on and off, lock and unlock, battery level and charging, so periods of active use, idleness and charging are distinguished (guide 154): the device-state record.
- **Connections and installations:** records of Wi-Fi and Bluetooth connections, network changes, and app installations and removals, adding context and provenance to the activity (guides 168, 167): the contextual layer.

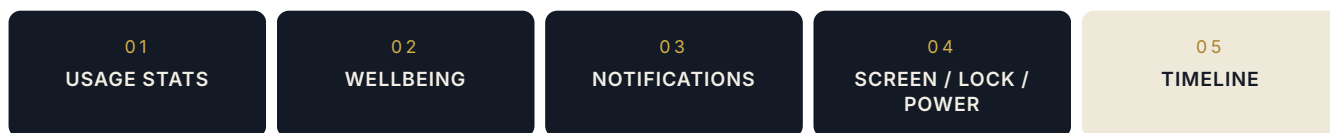


Figure 2 - the Android activity artefacts: usage statistics, Digital Wellbeing, notification history and screen, lock and power events, feeding a device-activity timeline.

§ 0 4 · THE ACTIVITY TIMELINE

Reconstructing the device-activity timeline

- **Combine the artefacts:** usage statistics, Wellbeing, notifications and system events read together as one activity stream, so app use, device state and events align rather than sit in isolation (guides 130, 154): the reconstruction.
- **Normalise the timing:** timestamps reconciled to a common time base for time zone and any offset, since Android artefacts use various epochs and formats (guides 108, 130): the aligned timeline.
- **Was the device in use?:** screen, lock and usage records establishing whether the phone was actively used at a moment or idle, so presence at and use of the device is evidenced (§7): the in-use answer.
- **What was being done?:** usage statistics and Wellbeing showing which app was in the foreground and for how long, so the nature of the activity is evidenced (guide 167): the what-was-done answer.
- **Corroborate across sources:** the activity timeline corroborated with messaging, location, app and media data (guides 165, 168, 166), so the picture rests on convergence (guide 130): the cross-checked timeline.

Manufacturer variation and expert interpretation

- **Different makers, different stores:** the same information kept in different databases, formats and locations by Samsung, Google, Xiaomi and others, so the specific device's artefacts are identified rather than assumed (guide 161): the per-maker layout.
- **Different retention windows:** makers and versions keeping usage and event history for different periods, so how far back each artefact reaches is established per device (§6): the per-device reach.
- **Cryptic and undocumented:** the artefacts largely undocumented, with cryptic event types, flags and timestamps, so they are interpreted by expertise and not at face value (guide 154): the specialist nature.
- **Meanings established, not assumed:** the meaning of each relevant event and field established through analysis and validation for this device and version (guide 151): the disciplined interpretation.
- **Conclusions to the evidence:** conclusions drawn only to the extent the correctly-understood data supports, with interpretive uncertainty stated (guide 100): the honest, expert conclusion.

Rotation, corroboration and honest limits

- **Older entries age out:** usage statistics, Wellbeing history and logs retaining only a window before pruning, so the record's reach in time is bounded and varies by artefact (guide 134): the retention limit.
- **A gap is not inactivity:** an absence of entries reflecting rotation, a setting or the artefact's scope, not proof nothing happened, so gaps are read honestly (guide 154): the crucial distinction.
- **Preserve promptly:** the record eroding with continued use, so prompt preservation and acquisition maximise reach, as throughout the block (guide 163): the preservation consequence.
- **Backups extend the reach:** earlier states in local, manufacturer and Google backups preserving activity since aged out, where the artefacts are included (guides 164, 147): the recovered history.
- **Attribution and honesty:** the activity attributed to the device and, with care, to a person, and findings stated at honest confidence, distinguishing what the record shows from what it does not (guides 105, 100): the honest activity account.

Deployment: proving what the device was doing

- **Proving the device was in use:** the screen, lock and usage records establishing that the phone was actively used at a moment, or idle, relevant to presence, alibi and responsibility (guide 154): the use proved.
- **Proving what was being done:** usage statistics and Wellbeing showing which app the person was in and for how long, so the activity is characterised (guide 167): the activity characterised.
- **Evidencing what reached the user:** the notification history showing what arrived and when, corroborating communications and their timing (guide 165): the arrival evidenced.
- **Corroborating or contradicting an account:** the activity timeline tested against a person's account of what they were doing, so a claim is supported or undermined by the phone's own diary (guide 98): the account checked.
- **Corroborated, honest, expert presentation:** the findings interpreted by expertise for the specific device, corroborated, their variation and rotation stated, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the activity evidence deployed defensibly.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: Android's usage and system artefacts are a rich but time-limited and maker-dependent node, corroborated with the phone's other evidence and preserved through the estate. The phone holds the usage statistics, Wellbeing history, notification history and system logs, in the layout its manufacturer chose. But the Google account (guide 164) holds activity records of its own, app, search and browsing activity, that corroborate what the device's artefacts indicate, and Google or manufacturer backups may hold earlier states of some artefacts; a paired wearable holds its own usage and wear record; and the phone's other data, messaging, location, apps, media (guides 165 to 168), corroborates the activity record, which corroborates them in turn. The discipline is to reconstruct the device-activity timeline from the artefacts, interpreted by expertise for this device, and to corroborate it across the phone's other sources, the Google account's activity records and the wearable, so that a gap from rotation is filled or explained and an activity finding rests on convergence rather than a single cryptic store. When the live artefacts have rotated, a backup or the Google account's activity may preserve the earlier record; when an event is doubtful, the phone's other data corroborates or qualifies it; and the activity record anchors the wider account of the person's use of the device.

EVIDENCE	LIVE DEVICE ARTEFACTS	GOOGLE ACCOUNT ACTIVITY	BACKUPS (GOOGLE / MAKER)	PAIRED WEARABLE	OTHER PHONE DATA	AGED-OUT / RECOVERABLE
App usage	Y: usage stats, Wellbeing	Y: app activity	Some artefacts	Own usage	App data (guide 167)	Backup / account
Device in use	Y: screen / lock events	Indirect (activity times)	Some	Wear / interaction	Messaging / location	Backup
Notifications	Y: history	n/a	Some	Mirrored	App records	Limited
Connections / installs	Y: logs	Install history (Play)	Some	Some	Location (guide 168)	Play records
Reach in time	Limited (varies by maker)	Longer (settings)	At backup time	Own window	Varies	Extends reach

Fallback strategy in one line: reconstruct the activity timeline from the device's artefacts, interpreted for this maker and version, and corroborate with the Google account's activity, backups, the wearable and the phone's other data; where the live record has rotated, the account or a backup may preserve it.

Worked examples

EXAMPLE 1 · THE DIARY THAT SHOWED THE PHONE UNLOCKED AND IN USE

A party claimed not to have been using their phone at a critical time. The §3 artefacts said otherwise: the §3 screen and lock events showed the device unlocked and its screen on at that moment, the §3 usage statistics and §3 Digital Wellbeing history showed which app was in the foreground and for how long (guide 167), and the §3 notification history showed a message arriving and being acted on. The §5 artefacts were interpreted by expertise for this manufacturer's layout, the §4 timeline normalised, and the picture §4 corroborated with messaging and location data (guides 165, 168). The phone's own diary contradicted the account. The lesson is §7's: Android's usage and system artefacts can show whether a device was actively in use at a given moment and what was being done with it, so they can corroborate or contradict an account of activity, provided they are interpreted by expertise for the specific device and corroborated.

EXAMPLE 2 · THE SAME ARTEFACT IN A DIFFERENT PLACE

An examiner familiar with one manufacturer's devices looked for the usage history where that maker kept it and, on a different maker's phone, found nothing, and was minded to report that no usage record existed. The §5 variation discipline corrected this: on this device the equivalent history sat in a different store, in a different format, with a different retention window, and once identified for this maker and version it was recovered in full and §4 reconstructed. The record had not been absent; it had been elsewhere. The lesson is §5's and the block's: Android artefacts vary by manufacturer and version, so the specific device's stores are identified rather than assumed from another maker's layout, and an apparent absence is checked against where this device actually keeps the record before any conclusion that it does not exist.

EXAMPLE 3 · THE GAP THAT WAS ROTATION, AND THE ACCOUNT THAT FILLED IT

A party argued that the absence of usage records for an earlier period proved the phone had not been used then. The §6 rotation discipline corrected the inference: this device's usage statistics retained only a short window, and the period predated the surviving records, so the silence was rotation, not proof of inactivity (guide 154). The §8 estate filled the gap: the §8 Google account's activity records, with a longer retention under the user's settings, showed app and search activity during the earlier period (guide 164), and a manufacturer backup preserved some earlier artefacts. The honest reading of the gap and the recovery from the estate together defeated the false inference. The lesson is §6's: Android's usage artefacts age out over windows that vary by maker, so a gap is not proof of inactivity, and the analysis says so, preserves promptly, and looks to the Google account and backups, which frequently preserve activity the device has rotated away.

Common mistakes and technical limitations

Common mistakes

- **Assuming one maker's layout:** the cardinal Android error, looking where another manufacturer keeps the record and concluding it is absent (Example 2, §5).
- **Reading the artefacts naively:** drawing confident conclusions from cryptic records without expertise (§5).
- **Reading a gap as inactivity:** treating rotation, a setting or an artefact's scope as proof nothing happened (Example 3, §6).
- **Not normalising timestamps:** mixing the various epochs and formats Android artefacts use (§4).
- **Not preserving promptly:** letting rotation age out the relevant period (§6).
- **Ignoring the Google account and backups:** not using them to recover aged-out activity (Example 3, §8).
- **Not corroborating:** resting an activity finding on the artefacts alone (§4).
- **Shallow extraction:** a logical extraction that never reaches the system databases and logs (§3, guide 162).

Technical limitations

- **Manufacturer variation:** the artefacts differ by maker and version, so nothing is assumed: the core Android limit (§5).
- **Rotation bounds the reach:** windows vary and gaps are not absences (§6).
- **Cryptic and undocumented:** interpretation carries uncertainty that is stated (§5).
- **Attribution needs care:** the record shows device activity; tying it to a person requires care (§6).
- **Depth-dependent:** the artefacts are reached only by a fuller extraction (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Does the matter turn on whether the phone was in use at a time, or what was being done with it?
- What is the device's manufacturer and version, and has it been preserved promptly before rotation ages out the period?
- Is the Google account available, whose activity records may reach further back than the device?

Ask your opponent

- Please preserve the device at Schedule 1 without continued use that may cause rotation, and disclose its usage statistics, Digital Wellbeing history, notification history and system logs for the relevant period, together with any backups.
- Please disclose the Google account's activity records for the period.
- Please confirm the device's manufacturer, model and version.

Ask your eDiscovery / forensic provider

- Where does this manufacturer's device keep its usage and system artefacts, and what do they show about use at the relevant time?
- How far back does each artefact reach, and what fills any gap?
- How is the cryptic data interpreted for this device, and the activity corroborated and attributed?

SUGGESTED WORDING · INSTRUCTION FOR AN ANDROID ACTIVITY ANALYSIS

"We instruct you to examine the usage, activity and system artefacts on the Android device at Schedule 1 relevant to Schedule 2. Please, on the acquired device at sufficient depth and preserving integrity: (1) identify, for this manufacturer, model and version, where the device keeps its usage statistics, Digital Wellbeing or equivalent history, notification history, and screen, lock, power, connection and installation records, rather than assuming another maker's layout; (2) recover and analyse these artefacts, reconstructing a device-activity timeline on a normalised clock, and establish whether the device was actively in use at the relevant time and what was being done with it; (3) interpret the cryptic, undocumented artefacts by expertise, establishing and validating the meaning of each relevant event for this device rather than assuming it; (4) address rotation honestly, stating how far back each artefact reaches and treating gaps as rotation, settings or scope rather than proof of inactivity, and draw on the Google account's activity records and any backups to recover aged-out activity; and (5) corroborate the activity with the phone's messaging, location, app and media data and any wearable, attribute it to the device and, with care, to a person, and state conclusions and interpretive limits at honest confidence."

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

The Android activity checklist

- ☐ Device preserved promptly, before rotation ages out the period
- ☐ This manufacturer's artefact stores identified, not assumed
- ☐ Artefacts reached at sufficient extraction depth
- ☐ Usage, Wellbeing, notifications and system events recovered
- ☐ Timeline reconstructed on a normalised clock
- ☐ Whether the device was in use, and what was done, established
- ☐ Cryptic events interpreted by expertise; meanings validated per device
- ☐ Rotation addressed; gaps read honestly; account and backups used
- ☐ Activity corroborated with the phone's other data and wearable
- ☐ Attributed to the device and, with care, to a person; limits stated

Red flags

- Another maker's layout assumed; a record declared absent: Example 2.
- Cryptic artefacts read naively.
- A gap read as proof of inactivity: Example 3.
- Timestamps not normalised across formats.
- Delay allowing rotation to age out the period.
- The Google account's activity records and backups not used.
- An activity finding not corroborated: Example 1.

When to involve a digital forensic expert

Whenever a matter turns on whether an Android phone was in use or what was being done with it, and always for these artefacts, because they vary by manufacturer, are cryptic, and age out: the expert identifies where this specific maker and version keeps its usage statistics, Digital Wellbeing history, notification history and system logs rather than assuming another's layout (Example 2, §5), recovers them at sufficient depth, and reconstructs the activity timeline on a normalised clock, establishing whether the device was actively in use and which app was open (Example 1, §4). The cryptic artefacts are interpreted by expertise with meanings validated for this device, rotation is confronted so that gaps are read as rotation, settings or scope rather than inactivity, and the Google account's activity records and backups are used to recover aged-out activity (Example 3, §6, §8). The picture is corroborated with the phone's other data and any wearable, attributed with care, and reported at honest confidence under CPR Part 35 or CrimPR Part 19. Prompt preservation is essential. This guide continues the Android block. Through **cflab.uk** and **e-discovery.uk**, Android activity work reads the phone's own diary of

what was done, wherever this manufacturer has kept it, with the expertise it demands and the honesty its rotation and variation require.

§ 13 · COMMON QUESTIONS

Frequently asked questions

What activity records does an Android phone keep?

A layered diary of its own use (§2, §3). Usage statistics record which apps were used, when and for how long; Digital Wellbeing and manufacturer equivalents keep a finer history of screen time, app sessions and unlocks; the notification history records what arrived and when; and system databases and logs record screen on and off, lock and unlock, battery and charging, connections, and app installations and removals. Together they reconstruct whether the phone was in use at a given moment, which app was open, and how the user's activity flowed, Android's counterpart to the iPhone's KnowledgeC and Biome.

What can these artefacts show?

Whether the phone was in use and what was being done, at fine resolution (§4, §7, Example 1). They can show that the device was unlocked and actively used at a particular moment, or idle and locked; which app was in the foreground and for how long; what notifications arrived and when; and how activity flowed through the day. This can corroborate or contradict an account of what someone was doing with a precision content alone rarely offers, which is why they are valuable, provided they are interpreted correctly for the specific device and corroborated.

Are these records the same on every Android phone?

No, and that is the key Android caution (§5, Example 2). The same information may be kept in different databases, formats and locations, with different retention windows, on a Samsung, a Pixel and a Xiaomi, and it changes across Android versions. So the specific device's artefact stores are identified for its manufacturer, model and version rather than assumed from another maker's layout, and an apparent absence is checked against where this device actually keeps the record before any conclusion that it does not exist. Fragmentation applies to the diary as much as to everything else.

If there are no usage records for a period, does that prove nothing happened?

No, that is the rotation trap (§6, Example 3). These artefacts retain only a window of activity before older entries are pruned, and the window varies by artefact and manufacturer, so an absence of records for an earlier period may simply mean they have rotated, or that a setting or the artefact's scope excluded them. A gap is not proof of inactivity. The analysis says so, preserves the phone promptly, and looks to the Google account's activity records, which may reach further back, and to backups, which may preserve earlier states.

How reliable is this evidence?

Reliable when interpreted by expertise for the specific device and corroborated (§5, §6). Correctly understood, these artefacts are among the most telling sources on the phone, but their value depends on proper interpretation, the meaning of each cryptic event established and validated for this maker and version, on timestamps normalised across Android's various formats, and on honest treatment of rotation and interpretive uncertainty. Findings are corroborated with the phone's messaging, location, app and media data, attributed with care, and stated at honest confidence. Read naively, or by another maker's layout, they can be confidently wrong.

Does the Google account help with activity?

Often, yes (§8, guide 164). The Google account keeps its own activity records, app, search and browsing activity, subject to the user's settings, and these can both corroborate what the device's artefacts indicate and reach further back than the device's rotating stores, filling gaps the phone has aged out. Google and manufacturer backups may also preserve earlier states of some artefacts, and a paired wearable holds its own usage and wear record. So the device's diary is read alongside the account's, not instead of it.

§ 1 4 · REFERENCE

Glossary

Usage statistics

Android's record of app use, timing and duration.

Digital Wellbeing

Google's screen-time and session history feature.

Notification history

The record of notifications received and when.

Screen / lock events

Logs of screen on/off and lock/unlock.

System logs

Records of power, connections and installations.

Device-activity timeline

The reconstructed record of use over time.

Manufacturer variation

Differences in artefact stores by maker.

Retention window

How far back an artefact reaches before rotation.

Normalised clock

Timestamps aligned across formats and zones.

Expert interpretation

Specialist reading of cryptic artefacts per device.

Sources and authoritative references

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

- cflab.uk, digital forensics services (usage statistics and Digital Wellbeing analysis, device-activity reconstruction, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 06 · Analysis and Phase 04 · Collection (device-activity analysis as practised): e-discovery.uk/edrm/analysis · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Android developer documentation, UsageStatsManager and notification history; Digital Wellbeing help: developer.android.com, [UsageStatsManager](https://support.google.com) · support.google.com, [Digital Wellbeing](https://support.google.com)
- Forensic Science Regulator, Code of Practice v2 (interpretation, validation and honest reporting of specialist artefacts) and ISO/IEC 27037: gov.uk, [FSR Code](https://gov.uk) · iso.org, [27037](https://iso.org)
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk) · justice.gov.uk, [Part 35](https://justice.gov.uk)

DISCLAIMER

This publication provides general information about Android usage, activity and system artefacts as at September 2026. These artefacts vary by manufacturer, model and Android version in location, format and retention, are largely undocumented and require specialist interpretation for the specific device, and are subject to rotation, so a gap is not proof of inactivity and their reach in time is limited. Activity must be attributed to a person with care. 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

Android activity work at the laboratory reads the phone's own diary of what was done, wherever this manufacturer has kept it. Because Android's usage and system artefacts vary by maker and version in location, format and retention, the specific device's stores, its usage statistics, Digital Wellbeing or equivalent history, notification history, and screen, lock, power, connection and installation records, are identified for its manufacturer, model and version rather than assumed from another maker's layout, so that a record is never declared absent merely because it is kept elsewhere (Example 2, guide 161). Recovered at sufficient depth (guide 162), the artefacts are reconstructed into a device-activity timeline on a normalised clock, establishing whether the phone was actively in use at a moment and which app was open and for how long (Example 1, guide 167). The cryptic, undocumented artefacts are interpreted by expertise, with the meaning of each relevant event established and validated for this device (guide 154); rotation is confronted honestly, so that gaps are read as rotation, settings or scope rather than inactivity, and the Google account's longer-reaching activity records and any backups are used to recover activity the device has aged out (Example 3, guide 164). The picture is corroborated with the phone's messaging, location, app and media data and any wearable, attributed to the device and, with care, to a person, and reported at honest confidence with interpretive limits stated, under CPR Part 35 or CrimPR Part 19. Because rotation erodes the record with use, prompt preservation is essential. This guide continues the Android block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle joins the block's theme to the iPhone's: the phone keeps a diary, it is read by an expert, and on Android it is read for this device, in this maker's layout, with honesty about how far back it reaches.



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