COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Android Location: Fused Location, Wi-Fi and Cell Data

How an Android Phone Works Out Where It Is, What It Keeps, and Why the Source of a Fix Governs Its Weight

An Android phone works out where it is by fusing several signals: satellite positioning when it can see the sky, the Wi-Fi networks around it, the cell towers it can hear, and motion sensors that fill the gaps. The result, a "fused" location, is what apps see and what the phone records, and its accuracy depends entirely on which signals fed it. Android keeps this location in several places: in Google's own Location History and the phone's location caches, in the databases of apps that asked for location, in the metadata of photographs, and in the cell and Wi-Fi records the phone retains. Every discipline from the iPhone location guide applies, location is a phone's not a person's, accuracy varies from a precise point to a broad area, and convergence carries weight, but Android's fused model and its Google-centred storage give the analysis its own shape. This guide sets out for UK lawyers how Android derives location, where it keeps it, how the source of a fix governs its accuracy and weight, and how Android location evidence is corroborated and read honestly.

⏱ Estimated reading time: 25 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 location analysis is a high-value, sensitive strand of its mobile work: recovering location from Google's Location History, the phone's caches, app databases, photo metadata and cell and Wi-Fi records, establishing the source and accuracy of each fix, converging the sources on a place and time, and attributing a phone's location to a person with care. The analysis handles sensitive location data proportionately and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | FUSED, WI-FI & CELL LOCATION | SOURCE, ACCURACY & CONVERGENCE | 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 fuses satellite, Wi-Fi, cell and sensor signals into a single location whose accuracy depends entirely on which signals fed it, and keeps that location in Google's Location History, the phone's caches, app databases, photo metadata and cell and Wi-Fi records, so the source of every fix must be established because it governs the fix's accuracy and weight, and a placement rests on sources converging.

The fused model (§3): the phone combining satellite, Wi-Fi, cell and sensor inputs into a fused location, so a fix's quality is inherited from its inputs. **Where it lives (§4):** Google's Location History and the phone's location caches, app databases, photo geotags, and retained cell and Wi-Fi records. **Accuracy by source (§5):** satellite gives a point, Wi-Fi a locality, cell only an area, and each fix carries an accuracy value that must be read. **Attribution and convergence (§6):** location is a phone's not a person's, and a placement rests on several sources agreeing. **Deployment (§7):** placing a phone at a place and time, or contradicting an account, honestly and proportionately.

- **A fix is as good as its source:** fused location inherits the accuracy of its inputs.
- **Several places it lives:** Location History, caches, apps, photos, cell and Wi-Fi records.
- **Point, locality, area:** satellite, Wi-Fi and cell give very different precision.
- **A phone, not a person:** attribution needs care and corroboration.
- **Convergence carries weight:** a place rests on sources agreeing, never on one coarse fix.

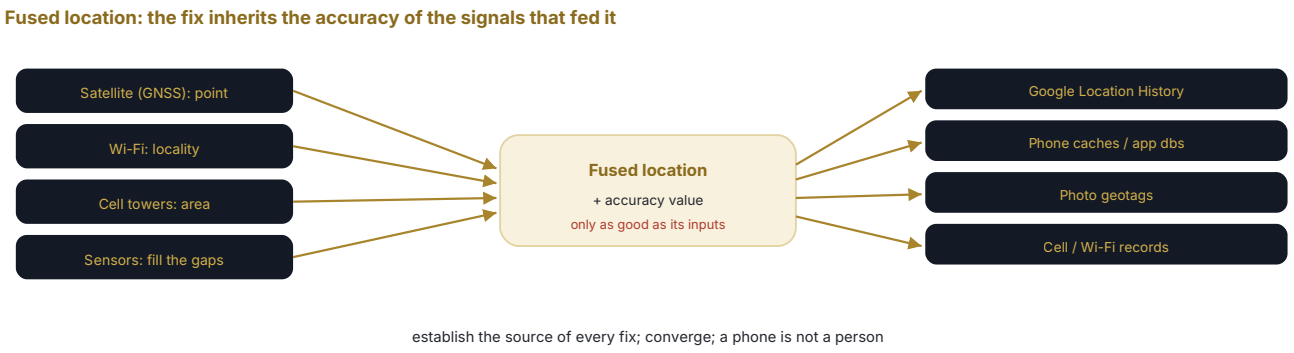

Figure 1 - satellite, Wi-Fi, cell and sensor signals fuse into a location whose accuracy depends on its inputs, kept in Location History, caches, apps, photos and network records, so the source of every fix is established and the sources converged.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: a fix is only as good as its source

The iPhone location guide (guide 152) set out the disciplines that govern all location evidence: it tells you where a phone was, not automatically where a person was; its accuracy varies enormously, from a satellite fix good to a few metres to a cell-tower position that only places the phone somewhere in a wide area; and a placement is safest when several independent sources converge on it. Every one of those disciplines applies to Android without change. What Android adds is a particular way of working out where it is, and a particular set of places where it keeps the answer, and both shape how the evidence is read.

The way is fusion. An Android phone does not rely on a single positioning method. It draws on satellite positioning (GNSS) when it can see the sky, on the Wi-Fi networks it can detect, whose positions Google has mapped, on the cell towers it can hear, and on its motion sensors to fill the gaps between fixes, and it fuses these into a single best estimate of its location, together with an accuracy value expressing how confident it is. That fused location is what apps receive and what the phone records. The crucial consequence for the evidence is that a fused fix is only as good as the signals that fed it: a fix built on satellite positioning may be precise to metres, while one built on cell towers alone may be an area a kilometre across, and both are recorded as "a location" with the difference visible only in the accuracy value and the source. So the source of every fix must be established, because it governs the fix's accuracy and therefore its weight. The places are several. Google's Location History, now Timeline, holds the running record of where the phone went, in the Google account or, increasingly, on the device (guide 164). The phone keeps location caches of its own. Apps that asked for location keep it in their databases. Photographs carry geotags. And the phone retains records of the cell towers and Wi-Fi networks it connected to, which are themselves coarse location evidence. The task, then, is to recover location from all these places, establish the source and accuracy of each fix, converge the sources on a place and time, attribute the phone's location to a person with care, and handle the sensitive result proportionately. This guide sets out how.

§ 0 3 · THE FUSED MODEL

How Android derives location: the fused model

- **Satellite positioning (GNSS):** the phone's satellite receiver giving a precise point fix, to a few metres in the open, but degraded or unavailable indoors and in dense cities (guide 124): the precise input.
- **Wi-Fi positioning:** the phone detecting nearby Wi-Fi networks and, using Google's database of their positions, deriving a locality-level fix, useful indoors where satellite fails (§5): the locality input.
- **Cell positioning:** the cell towers the phone can hear giving a coarse fix, an area rather than a point, always available where there is signal (guide 153): the coarse input.
- **Sensor fusion:** motion sensors (accelerometer, gyroscope) carrying the estimate between fixes and refining it, so location is continuous but partly inferred (guide 150): the gap-filling input.
- **The fused output and its accuracy value:** the inputs combined into one location with an accuracy radius, so the fix's quality is expressed in that value and inherited from its inputs (§5): the fix and its confidence.

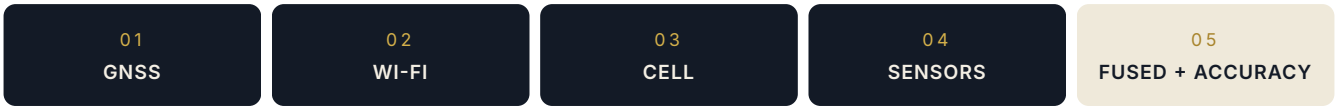

Figure 2 - the fused location model: satellite, Wi-Fi, cell and sensor inputs combined into one fix with an accuracy value that reflects which inputs fed it.

§ 0 4 · WHERE IT LIVES

Where Android keeps location

- **Google Location History (Timeline):** Google's running record of where the phone went, in the Google account or, under current settings, on the device, subject to the user's pause, auto-delete and storage choices (guide 164): the running diary.
- **The phone's location caches:** the phone caching recent fixes and the Wi-Fi and cell environments it has seen, so recent location survives on the device even where History is off (guide 154): the device cache.
- **App location databases:** apps that requested location keeping it in their own databases, maps, rideshare, social, fitness and many more, so location is spread across the apps (guide 167): the per-app location.
- **Photo geotags:** geotagged photographs carrying precise location at the moment of capture (guide 166): the photo point.
- **Cell and Wi-Fi connection records:** the phone's records of the towers and networks it connected to, and the carrier's cell-site records, each coarse location evidence in its own right (guide 153): the network trail.

§ 0 5 · ACCURACY BY SOURCE

Accuracy by source: point, locality, area

- **Satellite: a point:** a GNSS fix accurate to a few metres in good conditions, a genuine point, though worse indoors, in cities and at the start of a session (guide 124): the point source.
- **Wi-Fi: a locality:** a Wi-Fi fix accurate to tens of metres, placing the phone near a known network, so it locates a building or block rather than a spot (§3): the locality source.
- **Cell: an area:** a cell fix placing the phone within a tower's coverage, hundreds of metres to kilometres across, never a point, so it must never be presented as precise (guide 152): the area source.
- **Read the accuracy value:** each fused fix carrying an accuracy radius, so the uncertainty is read from the record rather than assumed, and a large radius is treated as the area it describes (guide 100): the recorded uncertainty.
- **Establish the source per fix:** the source and accuracy established for each fix relied on, so a coarse cell-derived fix is never mistaken for a satellite point merely because both are recorded as "locations" (§2): the source check.

§ 0 6 · ATTRIBUTION AND CONVERGENCE

Attribution, convergence and honest limits

- **A phone, not a person:** location evidencing where the device was, so the inference to a person is made with care and corroboration, since a phone may be left, lent or carried by another (guides 105, 152): the device-not-person limit.
- **Convergence carries weight:** a placement resting on several location sources agreeing, Location History, an app, a geotag, a Wi-Fi or cell record, so it does not depend on a single, possibly coarse, fix (guide 130): the converging conclusion.
- **Corroborate with motion and activity:** location corroborated with the phone's motion, activity and usage records (guides 150, 169), so presence and movement are cross-checked (§7): the corroborated place.
- **Gaps, settings and coverage:** location absent where services were off, History paused or auto-deleted, or coverage poor, so a gap is read as a gap and the settings are established (guide 164): the gaps read honestly.
- **State accuracy and confidence:** the place, its source and accuracy, and the strength of the inference to a person expressed at honest confidence, distinguishing a precise, converged placement from a coarse, single-source one (guide 100): the honest location account.

§ 0 7 · DEPLOYMENT

Deployment: placing a phone in time and place

- **Placing a phone at a place and time:** the converged location placing the device, and by careful inference the person, at a place at a time, corroborating or contradicting an account (guides 152, 98): the placement proved.
- **Reconstructing movements:** Location History, app journeys and the network trail reconstructing movements over a period on a timeline (guides 96, 164): the movements traced.
- **Testing an alibi:** location contradicting a claimed whereabouts, read with the source, accuracy and attribution stated (guide 149): the account tested.
- **Reaching location when the phone is sealed:** Google Location History in the account, and the carrier's cell-site records, supplying location when the device gives up little (guides 163, 164): the estate's location.
- **Honest, proportionate presentation:** the location evidence converged, its sources and accuracy stated, attributed with care, handled proportionately as sensitive data, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 20): the location evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: Android location comes from several on-device sources and is corroborated by others across the estate and beyond, and because the fused model makes every fix's quality depend on its source, convergence across sources of known accuracy is what carries a placement. The phone holds its location caches, app location databases, photo geotags and cell and Wi-Fi connection records. But Google Location History in the Google account (guide 164) holds the running diary, reachable regardless of the phone's lock where it is stored in the cloud, or on the device where the user keeps it there; a paired wearable holds its own location and motion; the carrier holds cell-site records, an area not a point, independently of the device; the app providers hold journey and check-in records by disclosure; and independent sources, CCTV, ANPR, transactions, corroborate a place from outside the estate. The discipline is to recover every on-device source, establish each fix's source and accuracy, and converge them with the account, the carrier, providers and independent evidence, so that a placement rests on agreement among sources of known quality. When History is paused or on-device, the caches, apps and network trail supply location; when the phone is sealed, the account and carrier are the route; and the sources together, honestly weighed, make the placement.

EVIDENCE	GOOGLE LOCATION HISTORY	PHONE CACHES / APPS / PHOTOS	CELL / WI-FI RECORDS (DEVICE)	CARRIER CELL-SITE	WEARABLE / COUNTERPART	INDEPENDENT (CCTV / ANPR)
Precise point	Y: where GNSS fed it	Y: geotags, GNSS fixes	Wi-Fi: locality	n/a (area)	Wearable GNSS	Y: at a location
Area only	Cell-fed entries	Cell-fed fixes	Y: cell area	Y: cell area	n/a	n/a
Movement over time	Y: Timeline	App journeys	Connection sequence	Historic cell	Wearable motion	Repeated sightings
Accuracy value	Per entry	Per fix	Implicit (coarse)	Implicit (coarse)	Per fix	n/a
When phone sealed	Y: if in cloud	Inaccessible	Inaccessible	Y: from carrier	Y: wearable	Y

Fallback strategy in one line: recover every on-device source, establish each fix's source and accuracy, and converge with Location History, the carrier, providers and independent evidence; when History is off or the phone sealed, the caches, network trail, account and carrier supply the placement.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE FUSED FIX THAT WAS REALLY A CELL FIX

A party relied on a location record from an Android phone as placing it at a precise address. The §5 source check told a different story: the fix had been §3 fused from cell towers alone, indoors with no satellite view, and carried an §5 accuracy radius of several hundred metres; it was an area, not a point, and the address lay merely within that area alongside many others (guide 152). Read for its source and accuracy, the fix supported only a broad placement, stated at §6 modest confidence pending §8 corroboration from a Wi-Fi fix and a geotag that did narrow it. The apparent precision dissolved. The lesson is §2's and §5's: a fused fix is only as good as the signals that fed it, and both a satellite point and a cell area are recorded as "a location", so the source and accuracy value of every fix are established, and a coarse fix is never presented as precise merely because it appears as a coordinate.

EXAMPLE 2 · THE CONVERGENCE THAT PLACED THE PHONE

A matter required establishing that a phone had been at a place at a time. No single source was decisive, but they converged: §4 Google Location History recorded the visit, an §4 app journey ended there, a §4 photo geotag placed the phone precisely, and the §4 Wi-Fi connection records showed the phone joining a network at that address (guides 164, 166). The §5 source and accuracy of each were stated, the satellite-fed geotag distinguished from the coarser entries, and the §6 placement rested on convergence and was corroborated with §6 motion data and a §8 wearable. The §6 inference to the person was made with care. The lesson is §6's: a placement is strongest when several location sources of known accuracy converge, Location History, an app, a geotag, a network record, so that the conclusion rests on agreement rather than one fix, and the inference from phone to person is made with corroboration.

EXAMPLE 3 · THE PAUSED HISTORY AND THE CACHES THAT REMAINED

A party had §6 paused Location History, and their Google account held no location record for the relevant period, which they urged as proof they had not travelled. The §4 on-device sources answered: the phone's §4 location caches held recent fixes, the §4 app databases of a maps and a rideshare app held journeys, the §4 Wi-Fi and cell connection records traced the phone's network trail, and the §8 carrier's cell-site records placed the phone in the relevant area (guides 167, 153). The §6 absence in the account was a setting, not a fact, and the §6 gap read honestly. The pause had silenced one source and left several others. The lesson is §4's and §6's: Android keeps location in several places beyond Google's History, so a paused, deleted or on-device History is not proof of no movement, and the caches, app databases, network trail and carrier records are pursued, with the account's settings established, before any conclusion is drawn from its silence.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Treating every fix as precise:** the cardinal error, presenting a cell-fed fused fix as a point (Example 1, §5).
- **Ignoring the accuracy value:** not reading the uncertainty each fix carries (§5).
- **Confusing phone with person:** inferring a person's location from a phone's without care or corroboration (§6, guide 105).
- **Resting on a single source:** a placement built on one fix rather than convergence (Example 2, §6).
- **Reading a paused History as no movement:** treating the account's silence as proof, ignoring caches, apps and the network trail (Example 3, §4, §6).
- **Not establishing the settings:** assuming History is in the cloud when it is paused, deleted or on-device (§6, guide 164).
- **Ignoring the network trail:** overlooking Wi-Fi and cell connection records as location evidence (§4).
- **Over-collecting sensitive location:** gathering an intimate movement record without proportionality (§7, guide 20).

Technical limitations

- **A fix inherits its inputs' accuracy:** fused location can be precise or coarse, and looks the same: the core limit (§3).
- **Location is a phone's, not a person's:** the inference to a person is never automatic (§6).
- **User controls govern History:** pause, auto-delete and on-device storage decide what the account holds (§4, §6).
- **Coverage and settings create gaps:** location is absent where services were off or signal poor (§6).
- **Google and Android evolve:** where location is kept, and how, changes over time (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Does the matter turn on where a phone, and by inference a person, was at a time, and how precisely?
- What are the Google Location History settings, and is the account, the carrier's records and any wearable available?
- What period and places matter, so the sensitive location data is collected proportionately?

Ask your opponent

- Please preserve and disclose, proportionately, the location data on the device at Schedule 1, including caches, app location databases, photo geotags and Wi-Fi and cell connection records, with source and accuracy values, and the Google Location History for the account, with its settings.
- Please confirm the Location History settings, any pause, auto-delete period and on-device storage.
- Please confirm who was carrying the device during the relevant period.

Ask your eDiscovery / forensic provider

- What is the source and accuracy of each fix relied on, and does it describe a point, a locality or an area?
- Do the sources converge, and how is the inference to a person made and corroborated?
- Where History is paused or on-device, what do the caches, apps, network trail and carrier supply?

SUGGESTED WORDING · INSTRUCTION FOR AN ANDROID LOCATION ANALYSIS

> "We instruct you to examine the location data for the Android device at Schedule 1 relevant to Schedule 2, scoped to the places and period the matter requires. Please, on the acquired device at sufficient depth and preserving integrity, and handling location as sensitive data: (1) recover every location source, Google Location History (establishing its settings, any pause, auto-delete and on-device storage), the phone's location caches, app location databases, photo geotags, and Wi-Fi and cell connection records, and obtain the carrier's cell-site records and any wearable's data where available; (2) establish for each fix relied on its source (satellite, Wi-Fi, cell, sensor-fused) and its accuracy value, and describe it as a point, a locality or an area accordingly, never presenting a coarse fix as precise; (3) converge the sources on a place and time, corroborating with motion, activity and independent evidence; (4) make the inference from the phone's location to a person's presence with care and corroboration, treating gaps and a silent History as settings or coverage rather than proof of absence; and (5) state the place, its source and accuracy, and the strength of the inference at honest confidence, collecting and handling the intimate data proportionately."

§ 12 · QUICK CONTROL

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

The Android location checklist

- ☐ Relevant places and period identified; collection proportionate
- ☐ Location History settings, pause, auto-delete and storage established
- ☐ Caches, app databases, geotags and network records recovered
- ☐ Carrier cell-site records and wearable data obtained where available
- ☐ Source of each fix established (satellite, Wi-Fi, cell, fused)
- ☐ Accuracy value read; point, locality or area stated
- ☐ Sources converged on place and time
- ☐ Corroborated with motion, activity and independent evidence
- ☐ Inference from phone to person made with care
- ☐ Gaps and silent History read as settings, not absence

Red flags

- A cell-fed fused fix presented as a precise point: Example 1.
- Accuracy values ignored.
- A placement rested on a single source: Example 2.
- A paused or on-device History read as proof of no movement: Example 3.
- The network trail overlooked.
- A person's location inferred from a phone's without care.
- Intimate location data over-collected.

When to involve a digital forensic expert

Whenever a case turns on where an Android phone, and by inference a person, was, because the fused model makes every fix look alike while their accuracy differs enormously: the expert recovers every location source, Google Location History with its settings established, the phone's caches, app location databases, photo geotags and Wi-Fi and cell connection records, and obtains carrier cell-site records and wearable data (§4, §8), then establishes the source and accuracy of each fix so that a cell-fed area is never presented as a satellite point (Example 1, §5). The sources are converged on a place and time and corroborated with motion, activity and independent evidence so a placement rests on agreement (Example 2, §6), a paused or on-device History is read as a setting rather than as proof of no movement while the caches, apps and network trail supply the location it withheld (Example 3), and the inference from phone to person is made with care. The intimate data is handled proportionately and findings 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**, Android location work reads each fix for the

source that made it, converges the many places Android keeps location, and places a phone in time and place through honest, corroborated evidence rather than a coordinate's false precision.

§ 13 · COMMON QUESTIONS

Frequently asked questions

How does an Android phone know where it is?

By fusing several signals (§3). It uses satellite positioning when it can see the sky, the Wi-Fi networks around it (whose positions Google has mapped), the cell towers it can hear, and its motion sensors to fill the gaps, combining them into one "fused" location with an accuracy value expressing its confidence. The crucial point for evidence is that the fused fix inherits the accuracy of whatever fed it: satellite gives a point, Wi-Fi a locality, cell only an area, and all are recorded as a location, so the source of each fix must be established.

Where does an Android phone keep its location?

In several places (§4). Google's Location History, now Timeline, keeps a running diary in the Google account or, under current settings, on the device; the phone caches recent fixes and the Wi-Fi and cell environments it has seen; apps that asked for location keep it in their own databases; photographs carry geotags; and the phone retains records of the towers and networks it connected to, which are coarse location evidence in themselves. Because location is spread across all of these, a silence in one, such as a paused History, does not mean the phone kept no record.

A location record shows an exact coordinate. Isn't that precise?

Not necessarily, and this is the commonest error (§5, Example 1). Every fused fix is recorded as a coordinate whether it came from satellite positioning good to a few metres or from cell towers good only to an area hundreds of metres or kilometres across. The difference is in the fix's source and its accuracy value, which must be read. A cell-fed fix is an area, not a point, and presenting it as a precise placement is a serious error. Each fix is described honestly as a point, a locality or an area according to what made it.

Google Location History is empty. Does that prove the person didn't travel?

No, it usually reflects the user's settings (§6, Example 3, guide 164). Location History can be paused, auto-deleted, deleted manually or kept only on the device, so an empty cloud record is read as the product of settings, not as proof of no movement. And Android keeps location in several other places: the phone's caches, app databases, photo geotags and the Wi-Fi and cell connection trail, and the carrier holds cell-site records independently. These are pursued, and the account's settings established, before any conclusion is drawn from History's silence.

How do you make an Android location finding reliable?

By establishing each fix's source and accuracy, then converging (§5, §6, Example 2). A placement is strongest when several sources of known accuracy agree on the same place and time, Location History, an app journey, a photo geotag, a Wi-Fi connection record, with the precise satellite-fed fixes distinguished from the coarse cell-fed ones, and corroborated with motion data, a wearable, carrier records and independent evidence such as CCTV. A placement built on convergence among sources of stated accuracy is far more reliable than one resting on a single coordinate of unknown origin.

Does location prove where a person was?

It proves where a phone was; the inference to a person needs care (§6, guide 105). A phone can be left at home, lent or carried by someone else, so location evidences the device's presence, and tying that to a particular person requires corroboration, motion data, a wearable worn on the body, activity records, independent sightings, rather than assumption. Where the evidence supports it, the inference can be strong; where it does not, that is acknowledged, and the strength of the inference is stated at honest confidence alongside the place and its accuracy.

§ 14 · REFERENCE

Glossary

Fused location
A single fix combining satellite, Wi-Fi, cell and sensor inputs.

GNSS
Satellite positioning, giving a precise point outdoors.

Wi-Fi positioning
Location from nearby networks, to a locality.

Cell positioning
Location from towers, to an area only.

Accuracy value / radius
The uncertainty a fix carries.

Location History / Timeline
Google's running record of where the phone went.

Location cache
The phone's store of recent fixes and environments.

Network trail
The record of Wi-Fi and cell connections over time.

Cell-site records
The carrier's independent record of tower connections.

Convergence
Several sources agreeing on a place and time.

Sources and authoritative references

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

- cflab.uk, digital forensics services (fused, Wi-Fi and cell location analysis, source and accuracy assessment, convergence, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 04 · Collection and Phase 06 · Analysis (location collection and interpretation as practised): e-discovery.uk/edrm/collection · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Android developer documentation, Fused Location Provider and location accuracy; Google Location History / Timeline help: developer.android.com, location · support.google.com, Timeline
- Forensic Science Regulator, Code of Practice v2 (accuracy, interpretation and honest reporting) and ISO/IEC 27037; ICO, UK GDPR guidance (sensitive location data): gov.uk, FSR Code · iso.org, 27037 · ico.org.uk
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35

DISCLAIMER

This publication provides general information about Android location forensics as at September 2026. How Android derives and stores location, and Google's Location History settings and storage, change over time, and location must be read honestly: a fused fix inherits the accuracy of its inputs and may be a point or a broad area, it is a phone's location rather than automatically a person's, and a silent or paused History is not proof of no movement. Location data is sensitive and must be handled proportionately. 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 location work at the laboratory reads each fix for the source that made it and converges the many places Android keeps location. On the acquired device at sufficient depth (guide 162), every location source is recovered, the phone's location caches, app location databases, photo geotags and Wi-Fi and cell connection records, together with Google Location History from the account (guide 164), whose settings, any pause, auto-delete period and on-device storage, are established first so that its silence is read as a setting rather than as proof of no movement (Example 3). Carrier cell-site records and any wearable's data are obtained where available (guides 153, 157). For each fix relied on, the source, satellite, Wi-Fi, cell or sensor-fused, and the accuracy value are established, and the fix is described honestly as a point, a locality or an area, so that a cell-fed fix is never presented as a precise placement merely because it appears as a coordinate (Example 1). The sources are converged on a place and time and corroborated with motion, activity and independent evidence so that a placement rests on agreement among sources of known quality (Example 2), and the inference from the phone's location to a person's presence is made with care and corroboration. The intimate data is collected and handled proportionately, and findings, with their source, accuracy and confidence, are reported 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 fused model's own lesson: a fix is only as good as its source, so establish the source, converge the sources, and never mistake a coordinate for precision.

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