Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/mobile-location-evidence-limits/

MOBILE EVIDENCE ANALYSIS

One Location Timeline From GPS, Cell Tower and App Data

A phone's location history mixes satellite fixes, WiFi lookups and cell tower estimates whose accuracy ranges from meters to kilometers, and a map that carries those radii holds up under an informed challenge. Put the device in airplane mode and preserve it, then call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Veronica Perez, Mobile and vehicle evidence examiner, Global Digital Forensics

Why Validated Coordinates Make a Stronger Map Exhibit

Mobile location records from iPhones, Android handsets, Google Timeline and third party applications frequently serve as decisive evidence in commercial disputes, employment matters, accident reconstruction and criminal defense. Validating the underlying sensor telemetry before latitude and longitude coordinates go onto a map exhibit is what prepares a timeline for scrutiny at trial. A smartphone blends satellite fixes, nearby WiFi router MAC address lookups, Bluetooth beacons and cellular tower triangulation, each carrying vastly different horizontal accuracy radii and caching behaviors.

Reconciling Accuracy Radii, Cached Beacons and Timezone Shifts

Working directly for retained legal counsel, Global Digital Forensics performs rigorous mobile device examination and location timeline validation engagements. When our examiners extract location databases from iOS cache_encryptedB.db records, Apple KnowledgeC artifacts or Android Fused Location Provider logs, we evaluate every coordinate alongside its recorded horizontal uncertainty meter value, confidence score and timestamp origin. A location entry with a twenty five hundred meter uncertainty radius or a stale WiFi lookup table is presented with that radius and age attached, as an area the device was estimated to be within. We also reconcile device activity logs, such as screen unlocks, step counter pedometer data and CarPlay or Bluetooth connections, to test whether the handset was actively carried by the user at the relevant moment.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Which Location Sources Live on the Phone and Which Live With the Provider

Location evidence comes from at least four places, and each answers a different question. On the handset, iOS and Android keep caches of recent location fixes, significant locations or visits, and application specific records such as a fitness app's route or a ride share app's pickup point, with retention measured in days or weeks for the caches and longer for application data. On the account side, Google Timeline and similar services store a user's history on the provider's servers, subject to the user's settings and the provider's processing, which smooths raw fixes into visits and routes. Those two sources can disagree, and the disagreement is informative.

Carrier records sit in a third category. Call detail records with cell site information show which tower and sector a phone used for a call or data session, which places the phone within a sector's coverage area, often a wedge extending a kilometer or more. Timing advance and per call measurement data, where carriers retain them, narrow the estimate within that sector. Counsel obtains these records by subpoena, and the examiner interprets them with the sector geometry and the carrier's own documentation, presenting the phone's position as the coverage area of the sector it used.

The fourth category is the vehicle. Infotainment and telematics systems record GPS tracks, door events, paired phones and sometimes call logs, and a car's record can corroborate or contradict the handset's. Our vehicle forensics and mobile device forensics pages describe how both are collected, and Veronica Perez, whose background includes location artifacts and vehicle systems, leads much of this work. Knowing which of the four sources a proposed exhibit came from is the first question we ask about any map. When the answer is a screenshot of an app, the conversation about what the exhibit can support starts there.

NIST SP 800-101 and the Method Behind a Mobile Examination

Mobile examinations follow a structure that the NIST NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics describe: preservation, acquisition, examination and analysis, and reporting, with attention at each stage to the volatility of mobile data and the variety of acquisition methods available for different devices. Preservation begins with isolating the device from networks so that the record stays as it was, beyond the reach of remote wipe commands, new synchronizations and cache rotation. Airplane mode, a shielded container or both accomplish this, and the time of isolation is recorded because every location artifact afterward is frozen at that moment.

Acquisition depends on the device, its operating system version and its lock state. A full file system extraction captures the databases where location caches live, while a logical extraction captures a narrower set, and the method chosen is documented with the tool, the version and the scope of what it reached. Where the device is with a cooperating custodian, our supported remote collection works through a link and a computer connection, normally with continued phone use, and usually runs from a few minutes to overnight depending on setup. Either way the extraction is hashed and the method is described in a form that can be repeated.

Examination and analysis evaluate every location record with its horizontal accuracy value, its source type, its timestamp and the timestamp's clock reference, and correlate it against device activity such as unlocks, application use, step counts and Bluetooth or CarPlay connections that indicate whether the phone was being

© 2026 Global Digital Forensics, Inc. All rights reserved.

carried. The report presents the chronology with the uncertainty attached to each point so the litigators and the court see a range rather than a pin. This is the practice that prepares the record for the challenge the first section of this guide describes, and it is the reason a validated chronology takes longer than a plotted one.

Practices That Keep a Location Chronology Sound

The first practice is labeling every source. A timeline that places a GPS fix with a five meter radius beside a WiFi lookup with a hundred meter radius and a cell sector estimate with a kilometer radius draws each at its own scale, so the exhibit is as accurate as the points it carries. The second is the time zone. Mobile databases store most timestamps in UTC or in seconds since a platform specific epoch, so the examiner applies the correct offset and every daylight saving change, keeping each event at its true hour. We record the clock reference for each source and convert once, in writing.

A third is reading account side history as the provider's inference. Google Timeline and similar services infer visits and routes from the underlying fixes and may snap a location to a nearby business or smooth a route along a road other than the one traveled. The inference is useful, and the report identifies it as the provider's processing, distinct from the phone's own sensor record. A fourth is going behind a screenshot of a location sharing app or a Find My display to the underlying record, where the examiner looks for the accuracy value, the source type and the time the position was computed.

The fifth practice comes first in time: isolate and preserve the device. Location caches rotate during normal use, so isolating the phone promptly keeps whatever the caches hold for the relevant dates in place. Our guide to preventing evidence loss at handoffs describes the quarantine steps, and the common evidence mistakes resource covers the broader pattern. A careful examiner refines every other practice during the analysis, and isolation is the one that happens at the start. Whoever learns of a relevant device treats its isolation as the first task of the day.

Presenting a Chronology That Holds Up

A defensible location exhibit shows uncertainty. Each point carries its source type and accuracy radius, drawn to scale, and the chronology states which clock each timestamp came from and how it was converted. Where two sources disagree, the exhibit shows both and the report explains the likely reason. A litigator reading an opposing expert's map looks first for those same features, which is where a rebuttal begins. Our expert witness page describes how the chronology is presented in a declaration or at trial. An exhibit that shows its own uncertainty answers the impeachment questions before they are asked.

The same reading covers how the report moves from device to person and from area to address. Placing the owner with the phone combines the device record with the activity correlation described above, along with interviews and other corroboration. A cell sector places a phone within an area, and the report describes it as that area even when the area helps the client's position. Statements made at their true scope are what make the helpful findings credible, and a court that sees each finding stated that carefully has good reason to credit the rest.

Security teams and internal auditors encounter location evidence in employee matters, fleet disputes and policy violations, and the same standards apply. A corporate mobile device management console records last known locations built for device recovery, and an auditor using them confirms their source and accuracy first.

© 2026 Global Digital Forensics, Inc. All rights reserved.

We help organizations understand what their management tools actually record before a dispute calls on it, and we recommend basing policy enforcement decisions on a validated record rather than a console map.

Preserving Smartphone Location Data Before Rolling Databases Overwrite

Mobile operating systems overwrite high resolution location caches in a matter of days or weeks during normal phone usage. If location history is relevant to your case, place the target device in Airplane Mode immediately, review how our mobile device forensics practice collects phones remotely and on site, and call Global Digital Forensics at (800) 868-8189 to schedule rapid forensic acquisition. The initial consultation is free.

Where Each Location Source Lives and What It Can Support

The guide explains why each coordinate is drawn with its own weight and radius. This table separates the four places location evidence comes from, the typical precision of each, what it can honestly support and the records used with it. Read the precision column as a reason to draw each point to scale with its own radius. The carrier and vehicle rows draw on records obtained by subpoena or acquisition alongside the handset.

Location evidence sources, their typical precision and what each supports.

Source	Typical precision	What it can support	What it needs
GPS fix on the handset	Meters, with a recorded accuracy value	The phone estimated this position at this time	Isolation before caches rotate
WiFi and Bluetooth lookups	Tens to hundreds of meters	The phone saw known access points nearby	The stored accuracy value read with each point
Google Timeline and account history	Inferred visits and routes	The provider inferred a visit from underlying fixes	Reading it as provider processing, distinct from raw sensor data
Cell site in carrier records	A sector wedge of a kilometer or more	The phone used this tower and sector	A subpoena and the carrier sector geometry
Vehicle infotainment and telematics	Device dependent GPS tracks and events	Paired phones, routes, door and call events	Acquisition of the module, often before salvage
Find My or sharing app screenshot	A rendered position only	That the app displayed a position	The underlying record with its accuracy and clock

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Our Mobile Preservation Checklist: Airplane Mode First, Questions Later sets out the items to secure in the order they expire. Have the device make and model, its current state and location, whether it is still in use, the date range at issue, the account and carrier associated with it, any account exports or carrier records already obtained and the proposition the location evidence is meant to test. The examiner asks what the matter concerns, whether the device can be isolated now, who holds it, whether the custodian cooperates and whether a declaration or testimony will be needed. The conversation produces a written proposal naming the device and account sources, the acquisition method including whether remote collection fits, the analyses to be performed, the deliverable and the timing drivers. The initial consultation is free. Call (800) 868-8189 at any hour.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST SP 800-101 Revision 1.

Authorities cited in this guide: NIST SP 800-101 Revision 1, Guidelines on Mobile Device Forensics. Establishes the preservation, acquisition, examination and reporting structure for mobile examinations described in the guide, Revision 1 published May 2014. Federal Rule of Evidence 702. Sets the reliability standard a location chronology and the expert presenting it must meet, current text at Cornell LII. Federal Rule of Evidence 901. Sets the authentication standard for location records and extracted databases offered as exhibits, current text at Cornell LII.

FREQUENTLY ASKED

Location Evidence: Proof, Recovery and Timing

Can a phone's location data prove someone was at a specific place?

It can establish that the device recorded a position within a stated radius at a stated time, and the reliability of that depends on the source type and accuracy value attached to the fix. Placing the owner there combines that record with device activity such as unlocks, messages or step counts that indicate the phone was being carried, along with other corroboration. We present both the position and its uncertainty and state plainly whether each finding speaks to the device, the person holding it or both.

Can you obtain location history without access to the phone?

Yes, for several sources. Account side history such as Google Timeline can be exported by the account holder or obtained through legal process directed to the provider, and carrier cell site records are available by subpoena. Each source is read on its own terms: account history is processed and inferred from the raw fixes, and cell site data places the phone within a sector. The handset's caches, which hold the most precise recent fixes, are collected from the device itself.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How long does a phone collection take?

With the device in hand, the time depends on the model, the storage size, the lock state and the extraction method the device supports. Our supported remote collection, used when the phone is with a cooperating custodian, works through a link and a computer connection, normally with continued phone use, and usually runs from a few minutes to overnight depending on setup. The analysis that follows is scoped separately and depends on the date range and the questions the matter raises.

Can deleted location history be recovered from a phone?

The examiner looks for it. Location caches and application databases are SQLite files whose deleted records can persist in free pages or write ahead logs until the database is vacuumed or overwritten, and a full file system extraction captures those remnants where they survive. How much remains turns on how long the device kept running after the deletion and how the specific application manages its database, which is why prompt isolation matters. We report recovered records with the qualifications that apply to carved data, marking any entry that is partial or whose attribution is open.

Are vehicle systems also a source of location evidence?

Yes. Infotainment and telematics modules commonly store GPS tracks, trip logs, door and gear events, paired phone identifiers and sometimes contact lists and call logs synchronized from a phone. Those records can corroborate a handset chronology or contradict it, and they carry their own clock and accuracy characteristics. Collection requires specialized hardware and methods, and the vehicle must be preserved in the same way as a phone. Our vehicle forensics page describes the process.

Web Addresses for the Sources Cited

1. NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics: https://csrc.nist.gov/pubs/sp/800/101/r1/final
2. Federal Rule of Evidence 702: https://www.law.cornell.edu/rules/fre/rule_702
3. Federal Rule of Evidence 901: https://www.law.cornell.edu/rules/fre/rule_901

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.