



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

iOS Location Services, Significant Locations and Frequent Locations

The Places a Phone Remembers, and Why It Matters Where the Location Came From

Among the most powerful, and most sensitive, evidence a phone holds is its record of where it has been. iOS keeps location in several distinct places: the encrypted Significant Locations record of the places a person regularly visits and when, the location data stored by individual apps, cached network and system location, and the geotags on photos. Together these can place a phone, and by inference a person, at a place and time with real force. But two disciplines are essential. First, location must be attributed and interpreted honestly: it is a phone's location, not necessarily a person's, and its accuracy varies enormously by source. Second, and specific to iOS, Significant Locations is protected: it is encrypted and access-controlled, so reaching it lawfully depends on the passcode and proper authority, not on defeating the protection. This guide sets out for UK lawyers where iOS keeps location, what each source shows and how accurate it is, how location evidence is corroborated and attributed, and the lawful and honest limits on reaching and reading it.

🕒 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. iOS location analysis is a high-value, sensitive strand of its mobile work: recovering the Significant Locations record and the location data held by apps, network and photos, interpreting each source's accuracy honestly, attributing a phone's location to a person with care, and reaching protected location data lawfully. The analysis places devices in time and place through convergence, handles sensitive location data proportionately, and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

SIGNIFICANT & APP LOCATION

ACCURACY & CONVERGENCE ANALYSIS

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 remembers where it has been
- 03 Where iOS keeps location
- 04 Significant Locations and its protection
- 05 Accuracy: not all location is equal
- 06 Attribution, convergence and honest limits
- 07 Deployment: placing a phone in time and place
- 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: iOS keeps location in several places, the encrypted Significant Locations record, app location, cached network and system location, and photo geotags, which together can place a phone in time and place with force, provided location is attributed and its accuracy read honestly, and Significant Locations is reached lawfully.

Where it lives (§3): Significant Locations (regularly visited places and times), location stored by individual apps, cached network and system location, and photo geotags. **Significant Locations and protection (§4):** a rich record of where a person regularly goes, encrypted and access-controlled, so it is reached lawfully via the passcode and proper authority, not by defeating protection. **Accuracy (§5):** not all location is equal, a GPS fix is precise, a cell or coarse fix is only an area, so each source's accuracy is stated. **Attribution and convergence (§6):** it is a phone's location, not necessarily a person's, so it is attributed with care and rests on convergence. **Deployment (§7):** placing a phone at a place and time, or contradicting an account, honestly.

- **The phone remembers where it has been:** several location sources, each different.
- **Significant Locations is rich but protected:** encrypted; reached lawfully, not by force.
- **Not all location is equal:** accuracy varies from a precise point to a broad area.
- **A phone, not a person:** location is attributed to a person with care and corroboration.
- **Convergence carries weight:** a place rests on several sources agreeing.

Several location sources, differing accuracy, converging on a place



Figure 1 - iOS keeps location in several sources of differing accuracy that converge on a place and time; it is a phone's location, attributed with care, and Significant Locations is encrypted and reached lawfully.

The problem in plain English: the phone remembers where it has been

A phone goes everywhere its owner goes, and it remembers. iOS keeps a record of where the device has been, and it does so in several distinct places, each with a different character. There is Significant Locations, a feature that quietly logs the places a person regularly visits, home, work, the addresses they frequent, and when they were there, building a detailed picture of a life's movements. There is the location data stored by individual apps, a map app's history, a rideshare app's journeys, a photo's geotag, each app holding its own slice. There is cached network and system location, the coarser positioning the phone works out from cell towers and Wi-Fi. And there are the geotags embedded in photographs (guide 149). Assembled together, these can place a phone, and by reasonable inference the person carrying it, at a particular place at a particular time, which is often exactly what a case needs.

But location evidence, for all its power, is where careless analysis does the most damage, and two disciplines are non-negotiable. The first is honest attribution and accuracy. Location tells you where a phone was, not, by itself, where a person was, a phone can be left, lent or carried by another, so the inference from device to person must be made with care and corroboration. And not all location is equal: a GPS fix may be accurate to a few metres, while a cell-derived position may only place the phone somewhere in a wide area, so treating a coarse fix as a precise one is a serious error. Each source's accuracy must be stated, and a place is safest when several sources converge on it (guide 124). The second discipline is specific to iOS: Significant Locations is protected. Because it is so revealing, Apple encrypts it and controls access to it, so reaching it depends on the passcode and proper legal authority, not on defeating the protection. The task, then, is to recover location from all its sources, to read each source's accuracy honestly, to attribute the phone's location to a person with care and convergence, and to reach the protected Significant Locations lawfully. This guide sets out where iOS keeps location, what each source shows and how accurate it is, and how location evidence is attributed, corroborated and reached.

§ 0 3 · WHERE IOS KEEPS LOCATION

Where iOS keeps location

- **Significant Locations:** iOS's record of the places a person regularly visits and when, built from the device's movements, a rich picture of a life's patterns, encrypted and access-controlled (§4): the frequently-visited-places record.
- **App location data:** individual apps storing their own location, a map's history, a rideshare's journeys, a social app's check-ins, so location is spread across many apps (guide 151): the per-app location.
- **Network and system location:** cached location the phone derived from cell towers and Wi-Fi, coarser than GPS but broad in coverage, so an area can often be established even without a precise fix (§5): the network positioning.
- **Photo geotags:** the precise locations embedded in geotagged photographs (guide 149), a highly accurate point source tied to a specific moment: the photo location.
- **Recovered on the decrypted device:** these sources recovered from the acquired, decrypted device (guides 145, 133), at the depth needed (guide 146), and, given sensitivity, proportionately (§6, guide 20): the sound, proportionate recovery.

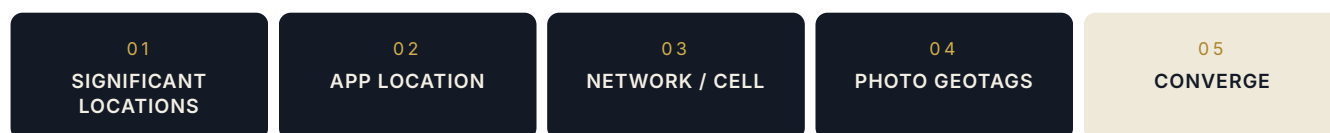


Figure 2 - the iOS location sources, from the protected Significant Locations record to app, network and photo location, converged on a place and time.

Significant Locations and its protection

- **A record of patterns:** Significant Locations logging the places a person regularly visits and the times, so a detailed pattern of home, work and frequented addresses emerges, powerful for establishing routine and presence (§7): the pattern-of-life record.
- **Encrypted and access-controlled:** because it is so revealing, the record encrypted and protected, so it is not simply readable and requires proper access, an iOS-specific protection (guide 133): the guarded record.
- **Reached lawfully via the passcode:** access depending on the passcode and proper authority (cooperation or lawful compulsion), so it is reached by authentication, not by defeating the encryption (guide 117): the lawful access.
- **Rich but sensitive:** the record intimate, revealing where a person lives, works and goes, so it is handled with particular care and proportionality as sensitive data (§6, guide 20): the sensitive handling.
- **Interpreted, not assumed:** the entries interpreted, a visit is the device's presence, not proof of the person's, and the record read for what it shows (§6): the honest reading.

Accuracy: not all location is equal

- **GPS: precise:** a satellite (GPS) fix accurate to a few metres in good conditions, a point location, so where available it places the phone precisely, though it degrades indoors and in cities (guide 124): the precise source.
- **Wi-Fi: local:** Wi-Fi-based location accurate to a locality, useful indoors where GPS fails, placing the phone near a known network (§3): the local source.
- **Cell: an area, not a point:** cell-tower positioning placing the phone within a wide area served by a tower, not at a point, so a cell fix is an area and must never be read as precise (guide 124): the coarse source.
- **Each fix carries its uncertainty:** a location reading often carrying an accuracy or radius value, so the uncertainty of each fix is stated rather than ignored (guide 100): the honesty about precision.
- **State accuracy plainly:** the accuracy of each source and fix stated, so a coarse area is never presented as a precise point and the weight of each fix is clear (§6): the calibrated accuracy.

Attribution, convergence and honest limits

- **A phone, not a person:** location evidencing where the device was, not automatically where its owner was, so the inference to a person is made with care, since a phone may be left, lent or carried by another (guides 105, 124): the device-not-person limit.
- **Convergence carries weight:** a place resting on several location sources agreeing, Significant Locations, an app, a geotag, a network fix, so it does not depend on a single, possibly coarse, source (guide 124): the converging conclusion.
- **Corroborate with movement and activity:** location corroborated with motion and activity data (guides 150, 134), so presence and movement are cross-checked, not asserted from location alone (guide 130): the corroborated place.
- **Gaps and coverage:** location absent where services were off or coverage poor, so a gap is not proof of absence and coverage is understood (guide 100): the gaps read honestly.
- **State confidence and accuracy:** the place, its accuracy, and the strength of the inference to a person expressed at honest confidence, distinguishing a precise, corroborated placement from a coarse, single-source one (guide 100): the honest location account.

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 124, 98): the placement proved.
- **Establishing a pattern of life:** Significant Locations establishing where a person routinely was, home, work, frequented places, relevant to residence, association and routine (§4): the routine established.
- **Contradicting an alibi or account:** location contradicting a claimed whereabouts, a phone shown elsewhere than the person claimed to be, read with proper attribution (guide 149): the account tested.
- **Reconstructing movements:** the location sources and app journeys reconstructing a person's movements over a period on a timeline (guides 96, 151): the movements traced.
- **Corroborated, honest, lawful presentation:** the location evidence converged, accuracy stated, attributed with care, protected sources reached lawfully, and handled proportionately, presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 20): the location evidence deployed defensibly.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: location on an iPhone comes from several on-device sources and is corroborated by others across the estate and beyond, which is exactly why convergence, not a single source, carries a placement. The phone holds Significant Locations, app location, network and system location, and photo geotags. But the paired Apple Watch and other devices (guide 123) hold their own location and motion; iCloud and backups (guide 147) hold synced and backed-up location data; the app providers hold journey and check-in records obtainable by disclosure; the carriers hold cell-site records (an area, not a point); and independent sources, CCTV, ANPR, transactions, corroborate a place at a time. The discipline is to converge the on-device sources with each other and with these external ones, so a placement rests on agreement rather than a single, possibly coarse, fix, and to reach the protected Significant Locations lawfully. When one source is coarse or absent, another sharpens or fills it; when device location is doubted, an independent source corroborates it; and the strength of a placement comes from the convergence of many sources of differing accuracy, honestly weighed.

EVIDENCE	SIGNIFICANT LOCATIONS	APP / PHOTO LOCATION	NETWORK / CELL (DEVICE)	ICLOUD / BACKUP / PAIRED	CARRIER CELL-SITE	INDEPENDENT (CCTV/ANPR)
Precise point	Visited places	Y: GPS / geotag	Wi-Fi local	Synced fixes	n/a (area)	Y: at a location
Area only	n/a	Some app coarse	Y: cell area	Coarse fixes	Y: cell area	n/a
Pattern of life	Y: routine	App history	n/a	Backup history	Historic cell	Repeated sightings
Timing	Y: with times	Y: timestamps	Cache times	Sync times	Call/data times	Timestamped
Attribution	Device presence	Device / account	Device	Account	Device (SIM)	Y: person visible

Fallback strategy in one line: converge the on-device location sources with the paired devices, providers, carrier records and independent sources; reach Significant Locations lawfully, and never rest a placement on a single coarse fix.

Worked examples

EXAMPLE 1 · THE CONVERGENCE THAT PLACED THE PHONE

A matter required establishing that a phone had been at a particular address at a particular time. No single source was decisive, but together they were: §4 Significant Locations recorded the address as a visited place at that time, an §3 app journey ended there, a §3 photo geotag placed the phone precisely at the location, and a §3 network fix was consistent (guide 124). The §5 accuracy of each was stated, the precise geotag distinguished from the coarser network fix, and the §6 placement rested on convergence. The §6 inference to the person was made with care and corroborated with motion data (guide 150). The phone's presence was established with real force. The lesson is §6's: a placement is strongest when several location sources of differing accuracy converge on the same place and time, each read for its true accuracy, so the conclusion rests on agreement rather than a single fix, and the inference from phone to person is made with corroboration.

EXAMPLE 2 · THE CELL FIX THAT WAS ONLY AN AREA

A party's location was asserted precisely on the strength of a single cell-derived position. The §5 accuracy discipline corrected this: a cell fix places a phone within a wide area served by a tower, not at a point, so presenting it as a precise location was wrong (guide 124). Read honestly, the cell data placed the phone in a broad area consistent with several possibilities, not at the specific spot claimed, and the §6 conclusion was stated at appropriately modest confidence, pending §8 corroboration from a more precise source. The apparent precision dissolved on proper reading. The lesson is §5's: not all location is equal, and a coarse cell fix is an area, not a point, so treating it as precise is a serious error, and each source's accuracy must be stated so that a broad area is never presented as a specific location.

EXAMPLE 3 · SIGNIFICANT LOCATIONS REACHED LAWFULLY

A rich Significant Locations record on a locked phone promised to establish a party's pattern of movements, but it was §4 encrypted and access-controlled. Rather than attempt to defeat the protection, the §4 lawful route was taken: with the passcode obtained by cooperation, and consistent with proper authority (guide 117), the device was unlocked and the record read lawfully. Given its §6 sensitivity, revealing home, work and frequented places, the collection was scoped and the data handled proportionately (guide 20). The pattern of movements was established without any attempt to break the protection. The lesson is §4's: Significant Locations is encrypted and access-controlled precisely because it is so revealing, so it is reached lawfully through the passcode and proper authority, not by defeating the protection, and, being intimate, it is handled with proportionality and care.

Common mistakes and technical limitations

Common mistakes

- **Treating a coarse fix as precise:** the cardinal error, presenting a cell area as a specific point (Example 2, §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 1, §6).
- **Trying to defeat Significant Locations' protection:** attempting to break the encryption rather than reaching it lawfully (Example 3, §4).
- **Ignoring accuracy values:** not stating the uncertainty each fix carries (§5).
- **Reading gaps as absence:** treating missing location as proof the phone was not somewhere (§6).
- **Over-collecting sensitive location:** gathering an intimate location record without proportionality (§6, guide 20).
- **Ignoring corroborating sources:** not converging with carrier, provider and independent evidence (§8).

Technical limitations

- **Location is a phone's, not a person's:** the inference to a person is never automatic: the core limit (§6).
- **Accuracy varies widely:** from a few metres (GPS) to a broad area (cell), so each fix is weighed on its accuracy (§5).
- **Significant Locations is protected:** it requires lawful access via the passcode (§4).
- **Coverage gaps exist:** location is absent where services were off or coverage poor (§6).
- **iOS evolves:** location sources and their storage change across versions, checked per version (§3).

§ 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?
- Is the passcode available to reach the protected Significant Locations lawfully, and what period and places matter so collection is proportionate?
- Are there corroborating sources, other devices, providers, carrier records, CCTV?

Ask your opponent

- Please preserve and disclose, proportionately, the location data on the device at Schedule 1, including Significant Locations (with lawful access), app and photo location, and network location, with accuracy values.
- Please provide the passcode necessary for lawful access to protected location data.
- Please confirm who was carrying the device during the relevant period.

Ask your eDiscovery / forensic provider

- What location sources place the phone, and how accurate is each?
- Do the sources converge, and how is the inference to a person made and corroborated?
- How is Significant Locations reached lawfully and the sensitive data handled proportionately?

SUGGESTED WORDING · INSTRUCTION FOR AN IOS LOCATION ANALYSIS

"We instruct you to examine the location data on the device at Schedule 1 relevant to Schedule 2, scoped to the places and period the matter requires. Please, on the acquired, decrypted device and preserving integrity, and handling location as sensitive data: (1) recover the location sources, Significant Locations, app and photo location, and network and system location, reaching the protected Significant Locations lawfully via the passcode and proper authority rather than by defeating the encryption; (2) state the accuracy of each source and fix, distinguishing a precise point (GPS or geotag) from a coarse area (cell), and never presenting an area as a point; (3) converge the sources on a place and time, corroborating with motion and activity data and, where available, carrier, provider and independent sources; (4) make the inference from the phone's location to a person's presence with care and corroboration, treating gaps as gaps rather than proof of absence; and (5) state the place, its accuracy, and the strength of the inference at honest confidence, collecting and handling the intimate location data proportionately and minimised."

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

The iOS location checklist

- ☐ Relevant places and period identified; collection proportionate
- ☐ Location sources recovered: Significant Locations, app, network, photo
- ☐ Significant Locations reached lawfully via the passcode
- ☐ Accuracy of each source and fix stated
- ☐ Coarse (cell) area distinguished from precise (GPS) point
- ☐ Sources converged on place and time
- ☐ Corroborated with motion, activity and external sources
- ☐ Inference from phone to person made with care
- ☐ Gaps read as gaps; sensitive data handled proportionately
- ☐ Place, accuracy and confidence stated honestly

Red flags

- A coarse cell fix presented as a precise point: Example 2.
- A person's location inferred from a phone's without care.
- A placement rested on a single source: Example 1.
- An attempt to defeat Significant Locations' protection: Example 3.
- Accuracy values ignored.
- Gaps read as proof of absence.
- Intimate location data over-collected.

When to involve a digital forensic expert

Whenever a case turns on where a phone, and by inference a person, was, because location is powerful but is where careless analysis does the most damage: the expert recovers all the location sources, Significant Locations, app, network and photo location, reaching the protected Significant Locations lawfully via the passcode rather than by defeating its encryption (Example 3, §4), and states the accuracy of each source so a coarse cell area is never presented as a precise point (Example 2, §5). The sources are converged on a place and time and corroborated with motion, activity and, where available, carrier, provider and independent evidence, so a placement rests on agreement rather than a single fix (Example 1, §6, §8), and the inference from phone to person is made with care and corroboration. The intimate location data is handled proportionately, and findings, with their accuracy and confidence, are reported under CPR Part 35 or CrimPR Part 19. This guide continues the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, location work places a phone in time and place through honest, converging, lawfully-reached evidence, so that where a device has been becomes reliable proof rather than overstated precision.

§ 13 · COMMON QUESTIONS

Frequently asked questions

What is Significant Locations?

An iOS feature that records the places a person regularly visits and when (§4). It builds, from the device's movements, a detailed picture of routine, home, work, frequented addresses, which can be powerful for establishing presence and pattern of life. Because it is so revealing, Apple encrypts it and controls access to it, so it is reached lawfully through the passcode and proper authority rather than by defeating the protection, and, being intimate, it is handled with proportionality and care as sensitive data.

Does location prove where a person was?

It proves where a phone was; the inference to a person needs care (§6). 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, activity, independent sightings, rather than assumption. Where the evidence supports it, the inference from phone to person can be strong; where it does not, that is acknowledged. The distinction between a phone's location and a person's is fundamental and always maintained.

Is all location data equally accurate?

No, and this matters greatly (§5, Example 2). A GPS fix or a photo geotag can be accurate to a few metres, a precise point; a Wi-Fi fix is accurate to a locality; but a cell-tower position places the phone only within a wide area served by the tower, not at a point. Treating a coarse cell fix as precise is a serious error. Each source's accuracy is stated, and a broad area is never presented as a specific location, so the weight of each fix is clear.

How do you make a location finding reliable?

By convergence (§6, Example 1). A placement is strongest when several location sources of differing accuracy, Significant Locations, an app journey, a photo geotag, a network fix, agree on the same place and time, each read for its true accuracy, and corroborated with motion and activity data and, where available, carrier, provider and independent sources such as CCTV. A place that rests on convergence is far more reliable than one built on a single, possibly coarse, source, which is why the enquiry assembles and cross-checks all the available location evidence.

Can you get Significant Locations off a locked phone?

Only lawfully, via the passcode (§4, Example 3, guide 117). Significant Locations is encrypted and access-controlled, so it is reached by authentication, obtaining the passcode by cooperation or lawful compulsion, and unlocking the device, not by defeating the protection. Where the passcode is unavailable, the record may be inaccessible by direct means, and other location sources and the estate are relied on. The intimate data, once accessed, is handled proportionately and scoped to what the matter requires.

Is location data sensitive in data-protection terms?

Highly (§6, guide 20). A detailed location history reveals where a person lives, works and goes, and can imply a great deal about their life, so it is treated as sensitive and handled with proportionality and minimisation: collection is scoped to the places and period the matter genuinely requires, and the data is disclosed and presented no more widely than necessary. This is especially so for Significant Locations. The evidential value of location never displaces the duty to handle such intimate data carefully and lawfully.

§ 1 4 · REFERENCE

Glossary

Significant Locations

iOS's encrypted record of regularly visited places.

App location

Location stored by individual apps.

Network location

Coarser position from cell towers and Wi-Fi.

Geotag

The precise location embedded in a photo.

GPS fix

A precise satellite-derived point location.

Cell fix

An area served by a tower, not a point.

Accuracy / radius

The uncertainty carried by a location fix.

Convergence

Several sources agreeing on a place and time.

Pattern of life

A person's routine of places and movements.

Attribution

Inferring a person from a phone's location.

Sources and authoritative references

The 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 (Significant and app location, accuracy and convergence analysis, lawful access to protected location, 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
- Apple Platform Security guide (Location Services, Significant Locations encryption and data protection): [support.apple.com, Platform Security](https://support.apple.com/Platform-Security)
- Forensic Science Regulator, Code of Practice v2 (accuracy, interpretation and honest reporting) and ISO/IEC 27037: [gov.uk, FSR Code](https://gov.uk/FSR-Code) · iso.org, 27037 · ICO, UK GDPR guidance (sensitive location data): 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 iOS location services as at August 2026. Location sources, their accuracy and their storage change across iOS versions, and location must be read honestly: it is a phone's location rather than automatically a person's, its accuracy varies from a precise point to a broad area, and gaps do not prove absence. Significant Locations is encrypted and reached only lawfully via the passcode. 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

Location work at the laboratory places a phone in time and place through honest, converging, lawfully-reached evidence, so that where a device has been becomes reliable proof rather than overstated precision. On the acquired, decrypted device (guides 145, 133), all the location sources are recovered, Significant Locations, app and photo location, and network and system location, with the protected Significant Locations reached lawfully via the passcode and proper authority rather than by defeating its encryption (guide 117). The accuracy of each source and fix is stated, so a precise GPS point or photo geotag is distinguished from a coarse cell area that is only a broad region, never presented as a point (Example 2, §5). The sources are converged on a place and time and corroborated with motion and activity data and, where available, carrier, provider and independent sources such as CCTV, so a placement rests on agreement rather than a single fix (Example 1, §8), and the inference from the phone's location to a person's presence is made with care and corroboration, with gaps read as gaps. The intimate location data, especially Significant Locations, is handled proportionately and minimised, and findings, with their accuracy and confidence, are reported under CPR Part 35 or CrimPR Part 19. This guide continues the iPhone and iPad block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding disciplines are constant: location is a phone's not a person's, accuracy varies and must be stated, convergence carries weight, and the protected record is reached lawfully.



I N S T R U C T T H E L A B

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