COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

iOS Photos, Media and Location Metadata

What a Photograph Records Beyond the Picture, and How to Read It Honestly

A photograph on an iPhone is far more than an image. Each one carries metadata, when it was taken, on what device, and very often exactly where, and the Photos library adds its own rich record: albums, edits, favourites, the analysis the phone runs on faces and scenes, and a database that tracks every asset over time. For the lawyer, this makes photos and videos among the most powerful evidence a phone holds, placing a person or an object at a time and a place, or contradicting an account of where someone was. But it also demands care. Metadata can be absent, altered or misread; a photo's dates mean specific things that are easily confused; an edited image differs from its original, which often survives; and location must be interpreted, not assumed. This guide sets out for UK lawyers what iOS photo and media metadata records, how the Photos library tracks assets, how location and dates are read honestly, and how deleted and edited media are recovered.

⏱ 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. Photo and media analysis is a core strand of its mobile work: reading the metadata a photograph carries, mining the Photos library database for the record of every asset, edit and album, interpreting location and dates honestly, and recovering deleted and edited media. The analysis places people and objects in time and place at honest confidence, distinguishing genuine from altered media, and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | PHOTO & MEDIA METADATA ANALYSIS | LOCATION & TIMELINE EVIDENCE | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: a photograph on an iPhone records far more than the image, when, on what device and often exactly where it was taken, and the Photos library tracks every asset, edit and album, making photos powerful for placing people and objects in time and place, provided the metadata and location are read honestly.

Photo metadata (§3): each image carries when it was taken, the device, camera settings and, very often, precise location, information beyond the picture itself. **The Photos library (§4):** a rich database tracking every asset over time, with albums, edits, favourites, faces and scenes, and a record of additions and deletions. **Location and dates (§5):** location must be interpreted, not assumed, and a photo's several dates mean specific things easily confused, so both are read with care. **Edited and deleted (§6):** an edited image differs from its original, which often survives, and deleted photos persist in the recently-deleted area, backups and remnants. **Deployment (§7):** placing a person or object at a time and place, or contradicting an account, at honest confidence.

- **The picture is only the surface:** a photo records when, on what device and often exactly where.
- **The library tracks everything:** assets, edits, albums, faces and deletions over time.
- **Location needs interpretation:** it is read, not assumed, and can be absent or altered.
- **Dates mean specific things:** a photo's several timestamps are easily confused.
- **Originals often survive edits and deletion:** edited and deleted media are frequently recoverable.

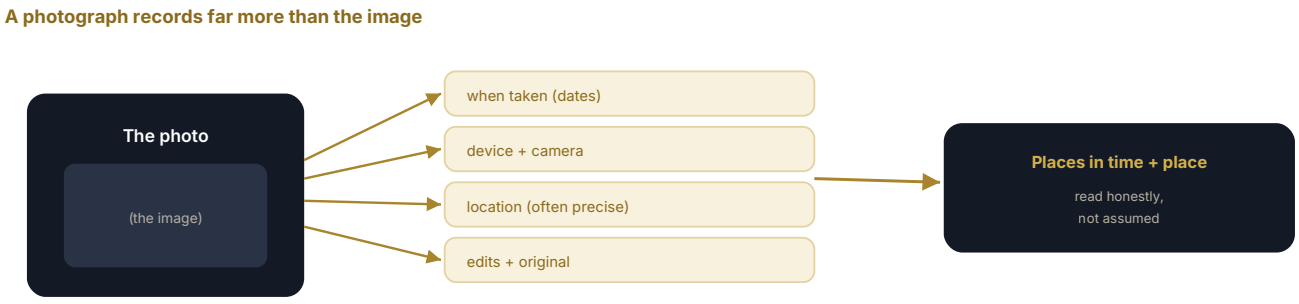

Figure 1 - beyond the image, a photograph carries its dates, device, location and edit history, which, read honestly, place a person or object in time and place.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the picture is only the surface

People think of a photograph as its image, but for evidence the image is often the least of it. When an iPhone takes a photo, it records a body of metadata alongside the picture: the date and time it was captured, the device that took it, the camera settings, and, if location services were on, the precise place, latitude and longitude, where the shutter was pressed. The Photos app then adds a further, rich layer: a database that tracks every photo and video as an asset over time, recording which albums it belongs to, whether it has been edited or favourited, the phone's own analysis of the faces and scenes in it, and when it was added, changed or deleted. So a single photograph can carry, invisibly, an answer to when, where and on what device, and the library around it can show how that photo was handled across the life of the phone.

This makes photos and videos among the most powerful evidence on a device. A geotagged, timestamped photograph can place a person or an object at a particular place at a particular moment, corroborate or contradict an account of where someone was, or establish that a thing existed at a time. But the same power demands discipline, because the metadata is easy to misread and easy to misuse. Location may be absent, if services were off, or, in rare cases, altered, so it must be interpreted rather than assumed. A photo carries several different dates, capture, modification, when it was added to the library, and confusing one for another produces wrong conclusions. An edited image differs from the original the user first captured, and that original very often survives and must be distinguished from the edit. And deleted photos are rarely truly gone: they persist in the recently-deleted area, in backups and in remnants, and can usually be recovered. The task, then, is to read the metadata for exactly what it records, to mine the library for the full history of each asset, to interpret location and dates honestly, and to recover edited and deleted media, so that photographs become reliable evidence of time and place rather than a source of confident error. This guide sets out how.

§ 0 3 · PHOTO METADATA

What a photo's metadata records

- **When it was taken:** the capture date and time recorded with the image, so a photo can be placed in time, read carefully because a photo carries several dates that mean different things (§5): the when.
- **The device and camera:** the make and model of the device and the camera settings recorded, so the photo can be tied to a particular device and its authenticity assessed (guide 126): the on-what.
- **Where it was taken:** for geotagged photos, the precise location, latitude and longitude, where the photo was captured, often the single most valuable datum, interpreted honestly (§5, guide 124): the where.
- **The embedded EXIF and more:** the standard embedded metadata (EXIF) plus Apple's additional data, so a rich technical record travels with the image, subject to being stripped or altered in some copies (guide 138): the technical layer.
- **Read from the original:** the metadata read from the original asset on the device, since sharing, exporting or messaging a photo can strip or change its metadata, so the device's own copy is preferred (§6): the authoritative source.

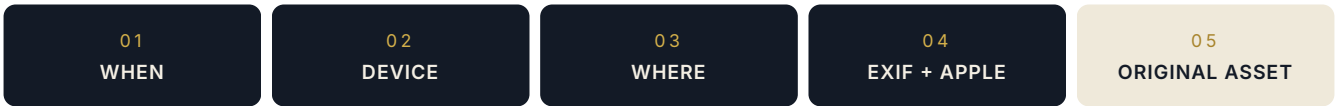

Figure 2 - a photo's metadata records when, on what device and where it was taken, in EXIF and Apple's own data, read from the original asset on the device.

§ 0 4 · THE PHOTOS LIBRARY

The Photos library: the record of every asset

- **A database of assets:** the Photos library keeping a database that tracks every photo and video as an asset, with its metadata, over the life of the phone, so the history of each asset is recorded, not just the current file (guide 134's activity theme): the asset ledger.
- **Albums, favourites and edits:** the library recording which albums an asset belongs to, whether it is favourited, and whether and how it has been edited, so how the user treated a photo is evidenced (§6): the handling record.
- **Faces, scenes and analysis:** the phone's own analysis of faces and scenes stored in the library, which can help locate and characterise relevant images, used with care as the phone's inference, not proof (guide 100): the analysis layer.
- **Additions and deletions:** the library recording when assets were added, imported or deleted, so the appearance and disappearance of a photo can be dated (guides 96, 138): the timeline of assets.
- **Read on the decrypted device:** the library database and the assets recovered from the acquired, decrypted phone (guides 145, 133), including deleted assets and earlier states (guides 4, 132), integrity preserved (guides 2, 3): the sound recovery basis.

§ 0 5 · LOCATION AND DATES

Reading location and dates honestly

- **Location is interpreted, not assumed:** a geotag evidencing where a photo was captured, read in context and corroborated, since it may be absent, imprecise or, rarely, altered, so it is interpreted honestly (guide 124): the where read with care.
- **Convergence with other location:** photo location corroborated with the phone's other location sources, app data, cell, Wi-Fi (guide 124), so a place rests on convergence rather than a single geotag (guide 130): the corroborated location.
- **Dates mean specific things:** the capture date, the file modification date and the library-added date each recording a different event, so they are read for what they specifically mean, not conflated (guides 108, 138): the dates read precisely.
- **Time zones and clocks:** photo timestamps reconciled for time zone and any clock offset, so a photo's true time is established against a claimed one (guide 108): the time normalised.
- **State confidence plainly:** what the location and dates reliably show, and their limits, expressed at honest confidence, distinguishing a precise geotag from an absent or uncertain one (guide 100): the honest reading.

§ 0 6 · EDITED, DELETED AND ALTERED

Edited, deleted and altered media

- **Edits and the surviving original:** an edited photo differing from the original the user captured, with the original very often retained by the Photos library, so the edit and the original are both recovered and distinguished (guide 4): the original beneath the edit.
- **Deleted photos survive:** deleted photos persisting in the recently-deleted area for a period, and in backups, snapshots and remnants, so a deleted image is very often recoverable (guides 132, 147): the deleted photo recovered.
- **Authenticity and manipulation:** a photo tested for authenticity where it matters, distinguishing a genuine capture from a manipulated or synthetic image, using metadata and provenance (guides 126, 127): the genuine image confirmed.
- **Stripped metadata in shared copies:** a photo shared, exported or messaged often losing metadata, so the device's original asset, not a stripped copy, is examined for the full record (§3): the authoritative copy examined.
- **Deletion and edits in context:** a deletion or edit established and dated, and its significance assessed against any account or duty to preserve (guides 109, 110): the handling read in context.

§ 0 7 · DEPLOYMENT

Deployment: placing people, objects and times

- **Placing a person or object:** a geotagged, timestamped photo placing a person or object at a place at a time, corroborating or contradicting an account of where someone was (guides 124, 98): the placement proved.
- **Contradicting an account:** a party's own photos, with their metadata, tested against their evidence, a claimed location against a geotag, a claimed date against a capture time, so a false account is exposed (guide 129's plain-sight theme): the account checked.
- **Establishing a thing existed:** a dated photograph establishing that an object, a document, a condition existed at a time, so the image evidences a fact, not just a scene (§3): the existence proved.
- **Recovering the deleted or edited image:** a photo a party deleted or altered recovered, with its original and metadata, so the material they tried to remove or change is restored (guide 4): the hidden image recovered.
- **Corroborated, honest presentation:** the photo findings corroborated with other location and the estate and presented at honest confidence, with dates and location read precisely, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the media evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a photograph on an iPhone exists in more than one place, and its metadata is corroborated across sources, which matters because a photo can be deleted, shared with metadata stripped, or its location doubted. The phone holds the Photos library, the original assets and their full metadata. But iCloud Photos holds synced copies and a recently-deleted area; backups (guide 147) hold copies and prior states; the paired Mac and iPad (guides 131, 135) hold the same library through sync; APFS snapshots (guide 132) hold earlier states; the phone's other location sources, app, cell, Wi-Fi (guide 124), corroborate a photo's geotag; and the counterparts a photo was shared with, and the platforms it was posted to (guide 129), hold their own copies, often with metadata stripped. The discipline is to read the metadata from the device's own original asset, to corroborate its location and dates across the estate and the phone's other location data, and to recover a deleted or edited photo from wherever a copy or earlier state survives. When a photo is deleted, the recently-deleted area, a backup or a snapshot holds it; when a shared copy has lost its metadata, the device's original retains it; and the phone's other location sources confirm or qualify a geotag.

EVIDENCE	PHONE (ORIGINAL)	ICLOUD PHOTOS	BACKUPS / SNAPSHOTS	PAIRED MAC / IPAD	OTHER LOCATION SOURCES	SHARED COPIES / PLATFORMS
The image	Y: original	Y: synced	Y: in backup	Y: same library	n/a	Y: often stripped
Full metadata	Y: on original	Y: synced	Y: preserved	Y: synced	n/a	Often stripped
Location	Y: geotag	Synced	In backup	Synced	Y: corroborates (guide 124)	Usually stripped
Edits / original	Y: both	Synced	Earlier state	Synced	n/a	Edited copy only
Deleted photos	Recently-deleted / remnants	Recently deleted	Pre-deletion backup	Device remnants	n/a	Their copy

Fallback strategy in one line: read metadata from the device's original asset and corroborate location and dates across the estate and the phone's other location sources; when a photo is deleted or its shared copy stripped, a backup, snapshot or the original holds it.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE GEOTAG THAT CONTRADICTED THE ALIBI

A party claimed to have been in one city at a particular time, but their own phone told a different story. A §3 geotagged, timestamped photograph in the Photos library placed them, and their phone, in a different location at that very time (guide 124). The §5 discipline governed: the geotag was interpreted, not assumed, its dates read precisely and reconciled for time zone, and the location corroborated with the phone's other location sources (§8) so it rested on convergence, not a single tag. The §6 original asset was examined, not a stripped shared copy. The account did not survive. The lesson is §7's: a geotagged, timestamped photograph can place a person and their phone at a time and place, corroborating or contradicting an account, but the geotag and dates must be read honestly and corroborated, so the conclusion rests on properly interpreted, converging evidence rather than an unexamined tag.

EXAMPLE 2 · THE EDITED PHOTO AND THE ORIGINAL BENEATH IT

A photograph produced by a party appeared to show a scene helpful to them, but something seemed off. The §6 edit analysis revealed why: the image had been edited, and the Photos library had retained the original, which showed the scene materially differently (guide 4). The §3 metadata was read from the device's original asset, not a shared, stripped copy, and the §6 authenticity of both versions assessed (guide 126). Distinguishing the edit from the recovered original changed the picture entirely. The lesson is §6's: an edited photo differs from the original the user captured, and the Photos library very often retains that original, so recovering it and distinguishing it from the edit, while reading the metadata from the device's own asset, is essential to an honest account of what the photograph actually showed.

EXAMPLE 3 · THE DELETED PHOTOS THE RECENTLY-DELETED AREA KEPT

A party deleted a set of photographs before their phone was examined, believing them gone. The §6 recovery found them: the images survived in the recently-deleted area and, for those beyond it, in an §8 backup and in remnants (guides 132, 147), and were recovered with their metadata intact. The §5 dates and location were then read to place the images in time and place, and the §7 deletion itself, established and dated, became relevant against the party's account (guide 110). The photos they had tried to erase were restored in full. The lesson is §6's: deleted photos rarely vanish, they persist in the recently-deleted area, in backups and snapshots, and in remnants, so a deleted image is very often recoverable with its metadata, and the deletion, once dated, may itself be evidence, provided the phone and estate are preserved promptly.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Reading only the image:** looking at the picture while ignoring the metadata that records when, where and on what device (§2, §3).
- **Assuming the geotag:** treating a location as certain without interpreting or corroborating it (Example 1, §5).
- **Confusing the dates:** conflating capture, modification and library-added dates, drawing wrong conclusions (§5).
- **Taking an edit for the original:** presenting an edited photo without recovering and distinguishing the original (Example 2, §6).
- **Using a stripped shared copy:** examining a shared or exported photo that has lost its metadata instead of the device's original (§3).
- **Assuming deletion is final:** treating deleted photos as gone, ignoring the recently-deleted area, backups and remnants (Example 3, §6).
- **Ignoring authenticity:** not testing whether a photo is genuine or manipulated where it matters (§6, guide 127).
- **Not corroborating location:** resting a place on a single geotag when other location sources could confirm it (§8, guide 124).

Technical limitations

- **Location may be absent or imprecise:** if services were off, or the fix is coarse, so it is read honestly, not assumed (§5, guide 124).
- **Metadata can be stripped or altered:** shared copies lose it, and it can be altered, so the original is examined (§3, §6).
- **Dates are easily misread:** a photo's several timestamps require careful interpretation (§5).
- **Recovery is not guaranteed:** deleted remnants may be overwritten, so prompt preservation matters (§6, guide 132).
- **iOS evolves:** the Photos library and metadata change across versions, checked per version (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Does the matter turn on where or when a photo was taken, or on whether an image is genuine or has been edited?
- Do we have the device's original assets, or only shared copies that may have lost their metadata?
- Has the phone and estate been preserved promptly, so deleted photos and originals survive?

Ask your opponent

- Please preserve and disclose the Photos library and original assets on the device at Schedule 1, with full metadata, including deleted photos and the originals of any edited images, and any iCloud, backup and paired-device copies.
- For any photo relied on, please provide the device original with metadata, not a stripped shared copy, and confirm its capture date and location.
- Please confirm whether relevant photos have been edited or deleted, and when.

Ask your eDiscovery / forensic provider

- What do the metadata and library show about when, where and on what device the photos were taken?
- How are location and dates interpreted and corroborated, and any edit or deletion recovered?
- Is a photo genuine, and what does the estate corroborate?

SUGGESTED WORDING · INSTRUCTION FOR A PHOTO AND MEDIA ANALYSIS

> "We instruct you to examine the photographs and media on the device at Schedule 1, relevant to Schedule 2. Please, on the acquired, decrypted device and preserving integrity: (1) recover the Photos library and the original assets, reading from the device's own originals rather than stripped shared copies, and extract the full metadata (capture date, device, camera and location) and the library's record of albums, edits, favourites, additions and deletions; (2) interpret location honestly, corroborating it with the phone's other location sources, and read the several dates (capture, modification, library-added) for their specific meanings, reconciled for time zone and clock offset; (3) recover edited photos together with their surviving originals, and deleted photos from the recently-deleted area, backups, snapshots and remnants, distinguishing edits from originals; (4) where authenticity is in issue, test whether a photo is genuine or manipulated; and (5) corroborate across iCloud, backups, paired devices and the phone's other location data, and state location, dates, authenticity and completeness at honest confidence, distinguishing precise from absent or uncertain data."

§ 12 · QUICK CONTROL

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

The photo and media checklist

- ☐ Phone and estate preserved promptly; originals and deleted assets intact
- ☐ Photos library and original assets recovered
- ☐ Full metadata read from the device's original, not a stripped copy
- ☐ Location interpreted and corroborated with other sources
- ☐ Capture, modification and library-added dates read precisely
- ☐ Timestamps reconciled for time zone and clock
- ☐ Edited photos recovered with their originals, distinguished
- ☐ Deleted photos recovered from recently-deleted, backups, remnants
- ☐ Authenticity tested where it matters
- ☐ Findings corroborated; confidence stated honestly

Red flags

- Only the image examined; metadata ignored: §3.
- A geotag treated as certain without interpretation: Example 1.
- Photo dates conflated: §5.
- An edited photo presented without its original: Example 2.
- A stripped shared copy relied on instead of the original.
- Deleted photos assumed gone: Example 3.
- Location rested on a single geotag, uncorroborated.

When to involve a digital forensic expert

Whenever a photograph's time, place or authenticity matters, because the evidence lies in the metadata and library, not the image, and both are easy to misread: the expert reads the full metadata from the device's own original asset, mines the Photos library for each asset's history of edits, albums and deletions, and interprets location and the several dates honestly, corroborating location with the phone's other sources so a place rests on convergence rather than a single geotag (Example 1, §5). Edited photos are recovered with their surviving originals and distinguished from them (Example 2), deleted photos are recovered from the recently-deleted area, backups, snapshots and remnants with their metadata intact (Example 3, §6), and authenticity is tested where it is in issue (guide 127). The findings place people, objects and times, or contradict an account, corroborated across the estate and reported at honest confidence under CPR Part 35 or CrimPR Part 19. This guide continues the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, photo and media work reads what a photograph records beyond the picture, so that images become reliable evidence of when, where and on what device, rather than a source of confident error.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can a photo really show where someone was?

Often yes, if read honestly (§3, §5, Example 1). A geotagged photograph records the precise location where it was captured, and with its timestamp it can place a person and their phone at a place at a time. But the geotag must be interpreted rather than assumed: it may be absent if location services were off, imprecise, or rarely altered, so it is corroborated with the phone's other location sources (guide 124). Read this way, with convergence, a photo's location is powerful and reliable evidence; taken at face value, it can mislead.

Why does it matter which date a photo has?

Because a photo carries several dates that mean different things (§5). The capture date records when the shutter was pressed; the modification date records when the file was changed; the library-added date records when it entered the Photos library. Confusing these produces wrong conclusions, for instance treating an import date as the capture time. So each date is read for what it specifically records, reconciled for time zone and clock offset, and the relevant one identified, rather than assuming a single date answers when the photo was taken.

The photo looks edited. Can you get the original?

Frequently yes (§6, Example 2). The Photos library very often retains the original of an edited photo, so both the edit and the original can be recovered and distinguished, showing what the image looked like before it was changed. The metadata is read from the device's own original asset rather than a shared, stripped copy. Where authenticity is in issue, the image is also tested for manipulation (guides 126, 127). So an edited photo is not simply accepted; the original is sought and, where found, presented alongside it.

Someone deleted photos. Are they gone?

Usually not (§6, Example 3). Deleted photos persist in the recently-deleted area for a period, and beyond that in backups, snapshots and remnants, so a deleted image is very often recoverable with its metadata intact, provided the phone and estate are preserved before the remnants are overwritten. The deletion itself, once established and dated, can also be relevant against a party's account. So deleted photographs are routinely recovered, and their removal may become evidence rather than a successful concealment.

We only have a photo someone sent us. Is that enough?

It is a start, but the device original is far better (§3, §6). Sharing, exporting or messaging a photo often strips or changes its metadata, so a received copy may have lost the very location and dates that matter, and may be an edited version. The device's own original asset retains the full metadata and, where the image was edited, the original beneath it. So wherever possible the analysis works from the device original rather than a stripped shared copy, which is why the phone or its backups are sought.

Can you tell if a photo is genuine?

Often, where it matters (§6, guides 126, 127). A photograph can be tested for authenticity using its metadata and provenance, distinguishing a genuine capture on the device from a manipulated or synthetic image or one imported from elsewhere. This is done with the same care as any provenance question: the device's original asset, its metadata, and its place in the library are examined, and the conclusion is stated at honest confidence. Where a photo's genuineness is contested, this testing is important before the image is relied on.

§ 14 · REFERENCE

Glossary

Metadata
Data a photo carries: dates, device, location, settings.

EXIF
Standard embedded image metadata.

Geotag
The location where a photo was captured.

Capture date
When the photo was taken.

Library-added date
When an asset entered the Photos library.

Photos library
The database tracking every photo and video.

Asset
A photo or video tracked by the library.

Original
The unedited image, often retained after editing.

Recently deleted
A grace-period area holding deleted photos.

Stripped copy
A shared photo that has lost its metadata.

Sources and authoritative references

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

- cflab.uk, digital forensics services (photo and media metadata analysis, location and timeline evidence, image authentication, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 05 · Processing and Phase 06 · Analysis (media metadata extraction and interpretation as practised): e-discovery.uk/edrm/processing · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple Platform Security guide and Photos documentation (photo metadata, the Photos library and iCloud Photos): support.apple.com, Platform Security · EXIF standard (CIPA/JEITA): cipa.jp, EXIF
- Forensic Science Regulator, Code of Practice v2 (interpretation, authentication and honest reporting) and ISO/IEC 27037: gov.uk, FSR Code · iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35 · UK GDPR: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · ico.org.uk

DISCLAIMER

This publication provides general information about iOS photo, media and location metadata as at August 2026. The Photos library, photo metadata and their handling change across iOS versions, and metadata must be interpreted precisely: location may be absent, imprecise or altered and must be corroborated, and a photo's several dates mean different things. Shared copies often lose metadata, so the device original is examined. 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

Photo and media work at the laboratory reads what a photograph records beyond the picture, so that images become reliable evidence of when, where and on what device rather than a source of confident error. On the acquired, decrypted phone (guides 145, 133), the Photos library and the original assets are recovered, and the full metadata, capture date, device, camera and location, is read from the device's own originals rather than stripped shared copies, alongside the library's record of albums, edits, favourites, additions and deletions (§3, §4). Location is interpreted honestly and corroborated with the phone's other location sources so a place rests on convergence rather than a single geotag, and the several dates, capture, modification, library-added, are read for their specific meanings and reconciled for time zone and clock (guides 124, 108). Edited photos are recovered together with their surviving originals and distinguished from them, deleted photos are recovered from the recently-deleted area, backups, snapshots and remnants with their metadata intact, and authenticity is tested where it is in issue (guides 126, 127). The findings place people, objects and times, or contradict an account, corroborated across iCloud, backups, paired devices and the phone's other location data, and are reported at honest confidence 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 insight is that on an iPhone the picture is only the surface, and the metadata beneath it, read honestly, is where the evidence lies.