COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Android Photos, Media and Metadata

The Gallery, the Media Store, Google Photos and the SD Card: Where an Android Image Lives, and What It Records

A photograph on an Android phone records the same things as one on an iPhone, when, on what device and often exactly where it was taken, and demands the same honest reading of its dates and location. But where it lives is more varied. Android keeps images as ordinary files in folders, indexes them in a system media store that tracks every image on the device, shows them through a gallery app that differs by manufacturer, syncs them to Google Photos, and may hold them on a removable SD card that has its own evidential character. Deleted images persist in trash folders, in the media store's index, in Google Photos and on the card. For the lawyer, this means an Android image is found by understanding these layers, and read by the same disciplines as any photograph: metadata from the original, location interpreted not assumed, dates read precisely, edits distinguished from originals. This guide sets out for UK lawyers where Android photos and media live, what the media store and Google Photos add, how removable storage is handled, and how images are recovered and read honestly.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Android media analysis is a core strand of its mobile work: locating images across the file system, the media store, gallery apps, Google Photos and removable storage, reading their metadata from the original, interpreting location and dates honestly, distinguishing edits from originals, and recovering deleted images from trash, index and cloud. The analysis places people and objects in time and place at honest confidence and is reported under CPR Part 35 and CrimPR Part 19.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | MEDIA STORE & GOOGLE PHOTOS ANALYSIS | SD CARD & REMOVABLE STORAGE | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

The headline point: an Android photograph records the same when, where and on-what as an iPhone's and demands the same honest reading, but it lives in more places, as a file in a folder, an entry in the system media store, an image in a manufacturer's gallery, a copy in Google Photos and sometimes a file on a removable SD card, so an Android image is found by understanding these layers and read by the same disciplines as any photograph.

Where it lives (§3): as ordinary files in camera and app folders, indexed by the system media store and shown by a gallery app that varies by manufacturer. **Media store and Google Photos (§4):** the media store indexes every image, including recently deleted ones, and Google Photos syncs the library to the account with its own trash and history. **The SD card (§5):** removable storage that may hold images and deleted remnants, imaged separately and often less protected than internal storage. **Honest reading (§6):** metadata from the original, location interpreted not assumed, dates read precisely, edits distinguished from originals. **Deployment (§7):** recovering deleted images from trash, index, cloud and card, and placing people and objects in time and place.

- **The same picture, more places:** file, media store, gallery, Google Photos, SD card.
- **The media store indexes everything:** including images since deleted.
- **Google Photos holds the library:** synced, with its own trash and history.
- **The SD card is its own source:** imaged separately, often weakly protected.
- **Read like any photograph:** original metadata, honest location, precise dates.

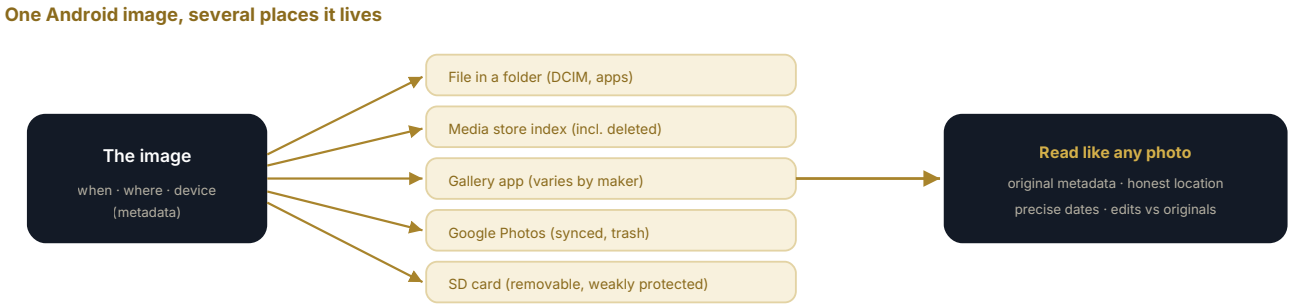

Figure 1 - an Android image carries the same metadata as any photograph but lives in several places at once, file, media store index, gallery, Google Photos and SD card, and is read by the same honest disciplines.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the same picture, more places

The iPhone photo guide (guide 149) explained that a photograph is far more than its image: it records when it was taken, on what device and, if location was on, exactly where, and the library around it tracks how it was handled. All of that is equally true of an Android photograph, and the same disciplines of honest reading apply without change: metadata is read from the original, not a stripped shared copy; location is interpreted and corroborated, not assumed; a photo's several dates are read for what each means; and an edited image is distinguished from the original that often survives. What differs on Android is where the picture lives, and that difference is the reason this guide exists. Where iOS keeps photos inside a single Photos library, Android keeps them in several layers at once.

An Android image is, first, an ordinary file in a folder, in the camera's DCIM directory or in the folder of whichever app created or received it. It is, second, an entry in the system media store, a database that Android maintains to index every image, video and audio file on the device so that apps can find them; that index records paths, dates and attributes, and it can retain entries for images since deleted. It is, third, what the user sees through a gallery app, and gallery apps differ by manufacturer, with their own albums, trash folders and features. It is, fourth, very often a copy in Google Photos, synced to the Google account (guide 164) with its own trash, history and, for some users, the only surviving copy after the device was cleared. And it may be, fifth, a file on a removable SD card, which many Android phones still accept and which has its own evidential character: it is imaged separately, it may have been used in other devices, and it is often less protected than the phone's encrypted internal storage. Deleted images, correspondingly, persist in gallery trash folders, in the media store's index, in Google Photos' trash and history, and as remnants on the card. For the lawyer, then, an Android image is found by understanding these layers and pursuing all of them, and read, once found, by the same disciplines as any photograph. This guide sets out both.

§ 0 3 · WHERE IMAGES LIVE

Where Android images live

- **Files in folders:** images stored as ordinary files, in the camera's DCIM folder and in the folders of apps that created, downloaded or received them, so the file system is the first place to look (guide 162): the image as file.
- **App-created and received images:** messaging and social apps saving images to their own folders or caches, so an image received in a conversation lives in that app's space (guides 165, 167): the app-held image.
- **The gallery view:** a gallery app, Google Photos or a manufacturer's own, presenting the images with albums and a trash folder, differing by maker, so the gallery in use is identified as the messaging app was (guide 165): the maker-dependent gallery.
- **Screenshots and downloads:** screenshots and downloaded images in their own folders, often revealing what the user viewed, so they are recovered alongside camera images (guide 136): the captured-and-downloaded images.
- **Reached at depth:** the folders, caches and index reached by a file-system or deeper extraction, since a logical extraction may return only a subset (guide 162): the depth-dependent view.

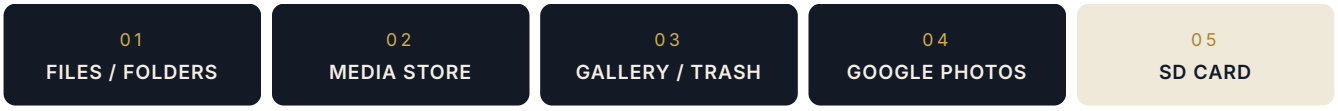

Figure 2 - the layers where an Android image lives: files in folders, the media store index, the gallery and its trash, Google Photos, and any removable SD card.

§ 0 4 · MEDIA STORE AND GOOGLE PHOTOS

The media store and Google Photos

- **The media store indexes everything:** Android's media store database recording every image, video and audio file with its path, dates and attributes, so it is a map of the device's media, including what apps saw (guide 138): the media index.
- **Deleted entries and trash:** the media store retaining entries for deleted or trashed items for a period, and modern Android keeping a system trash, so a deleted image can often be found through the index even when the file is gone (guide 155): the index remnant.
- **Google Photos syncs the library:** Google Photos backing the library up to the Google account with metadata, so the account holds the images, often including ones removed from the device (guide 164): the cloud library.
- **Google Photos trash and history:** Google Photos keeping deleted items in its trash for a period and recording edits and history, so a deleted or edited image survives in the account (guide 149): the cloud trash and edit record.
- **Reconcile device and cloud:** the device's images and Google Photos reconciled, since the cloud may hold more, or different, images than the device, and the same image is not double-counted (guide 130): the reconciled library.

§ 0 5 · THE SD CARD

Removable storage: the SD card

- **A separate source:** a removable SD card holding images, videos and other files, imaged and analysed as a separate storage device with its own integrity record (guides 2, 3): the card as its own evidence.
- **Often less protected:** a card frequently formatted without the phone's encryption, or with weaker protection, so its contents and deleted remnants may be recoverable even when the phone is sealed (guide 163): the weakly protected store.
- **Deleted remnants on the card:** deleted images persisting in the card's unallocated space until overwritten, recoverable by carving (guide 4): the card's remnants.
- **A card's history:** a card possibly used in other devices or cameras, and its contents possibly predating the phone, so its provenance and history are considered (guide 141): the card's provenance.
- **Adoptable storage:** a card configured as internal ("adopted") storage encrypted and tied to the phone, so its evidential character depends on how it was set up (§5): the configuration check.

§ 0 6 · HONEST READING

Reading metadata, location and dates honestly

- **Metadata from the original:** the image's metadata (capture date, device, camera settings, location) read from the original file on the device, since shared and messaged copies are often stripped (guide 149): the authoritative source.
- **Location interpreted, not assumed:** a geotag read in context and corroborated with the phone's other location sources, since it may be absent, imprecise or altered (guides 149, 168): the honest where.
- **Dates read precisely:** the capture date, the file's modification date and the media store's dates each meaning something different, so they are read for what they specifically record and reconciled for time zone (guides 108, 149): the dates read precisely.
- **Edits and originals:** an edited image distinguished from the original, which gallery apps and Google Photos often retain, so both are recovered and compared (guide 149): the original beneath the edit.
- **Authenticity where it matters:** an image tested for authenticity, distinguishing a genuine capture from a manipulated or synthetic one, using metadata and provenance (guides 126, 127): the genuine image confirmed.

§ 0 7 · DEPLOYMENT

Deployment: recovering and placing images

- **Recovering deleted images:** deleted images recovered from gallery and system trash, the media store index, Google Photos' trash and history, and remnants on the card and device (guides 155, 4): the deleted image restored.
- **Placing a person or object:** a geotagged, timestamped image placing a person or object at a place at a time, corroborating or contradicting an account (guides 149, 168): the placement proved.
- **Evidencing what was seen and received:** screenshots, downloads and app-received images evidencing what the user viewed and was sent (guide 136): the viewed and received material.
- **Reaching images when the phone is sealed:** Google Photos and an unencrypted SD card supplying images when the phone itself gives up little (guides 163, 164): the estate's images.
- **Corroborated, honest presentation:** the image findings corroborated across device, cloud and card, read honestly for dates and location, and presented at honest confidence 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: an Android image exists in more places than an iPhone's, and each layer is both a place to find it and a place it may survive deletion. The phone holds the files, the media store index and the gallery trash. But Google Photos in the Google account (guide 164) holds the synced library, with its own trash and history, reachable regardless of the phone's lock; the manufacturer's cloud may hold gallery backups; a removable SD card holds its own files and remnants and may be readable when the phone is sealed; backups hold earlier states; the counterparts an image was shared with hold their copies, usually stripped of metadata; and the platforms it was posted to hold theirs. The discipline is to pursue all the layers, reading metadata from the device's original, and to reconcile them, so that an image deleted from the device is found in the media store index, the trash, Google Photos or the card, and an image whose shared copy has lost its metadata is matched to the original that retains it. When the phone is sealed, Google Photos and the card supply the images; when the file is deleted, the index, trash or cloud holds it; and the layers together give the fullest and most reliable account of the picture.

EVIDENCE	PHONE FILES	MEDIA STORE / TRASH	GOOGLE PHOTOS	SD CARD	BACKUPS / MAKER CLOUD	SHARED COPIES / PLATFORMS
The image	Y: original	Index entry	Y: synced	Y: if stored there	Y: if backed up	Y: often stripped
Full metadata	Y: on original	Dates, path	Y: preserved	Y: on file	Y	Often stripped
Deleted images	Remnants	Y: retained entries, trash	Y: trash, history	Y: unallocated	Pre-deletion state	Their copy
Edits / originals	Both (often)	Entries for both	Y: history	File versions	Earlier state	Edited copy only
When phone sealed	Inaccessible	Inaccessible	Y: via account	Y: if unencrypted	Y: via cloud	Y

Fallback strategy in one line: pursue every layer, file, index, trash, Google Photos, card and backups, reading metadata from the original; when the phone is sealed or the file deleted, the cloud, index or card usually holds the image.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE DELETED PHOTOS FOUND IN THE INDEX AND THE CLOUD

A party deleted a set of photographs from their phone and believed them gone. The §4 layers said otherwise: the media store index still held entries for the deleted images with their paths and dates, the gallery's trash folder held some intact, and §4 Google Photos in the party's Google account held the full set, synced before the deletion, with its own trash and history (guide 164). The §6 metadata was read from the originals in the cloud, and the §6 dates and location interpreted honestly. The deletion had removed the files from one layer and left them in three others. The lesson is §2's and §4's: an Android image lives in several layers, and deletion from the device rarely clears them all, so the media store index, the gallery trash and Google Photos are pursued, and a deleted image is very often recovered with its metadata intact from a layer the party did not think to clear.

EXAMPLE 2 · THE SD CARD THAT THE SEALED PHONE COULD NOT PROTECT

A modern Android phone was locked and encrypted and yielded nothing (guide 163), but it held a §5 removable SD card. The card had been formatted as ordinary portable storage, without the phone's encryption, so it was §5 imaged separately and read in full: it held the camera images and, in its §5 unallocated space, deleted images recovered by carving (guide 4). Its §5 provenance was considered, since it might have been used elsewhere, and its images §6 read honestly for dates and location. The vault was shut, but the card in its side was open. The lesson is §5's: a removable SD card is its own evidential source, often unencrypted and readable even when the phone is sealed, so it is imaged and analysed separately, its deleted remnants carved, and its provenance considered, because the phone's protections frequently do not extend to the card.

EXAMPLE 3 · THE DATE THAT MEANT SOMETHING ELSE

An image's date was relied on as the moment a scene was photographed. The §6 dates-read-precisely discipline found the error: the date cited was the media store's date-added entry, recording when the image entered the index after being received in a messaging app, not the capture date, which the §6 original metadata showed was much earlier and on a different device (guide 149). The image was a received copy, not the party's own photograph, and the §6 stripped metadata of the shared copy had concealed this. Read correctly, the date and provenance changed the picture. The lesson is §6's: a photo carries several dates, capture, modification and media-store dates, each meaning something different, so they are read for what each specifically records, and an image's provenance, camera capture or received copy, is established from the original's metadata rather than from the date a copy appeared on the device.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Looking in one layer only:** the cardinal error, examining the gallery or files but not the media store, trash, Google Photos or card (Example 1, §2).
- **Ignoring the SD card:** not imaging removable storage that may be readable when the phone is sealed (Example 2, §5).
- **Confusing the dates:** reading a media-store or modification date as the capture date (Example 3, §6).
- **Using a stripped copy:** relying on a shared or messaged image that has lost its metadata (§6).
- **Assuming the geotag:** treating location as certain without interpreting or corroborating it (§6).
- **Missing app-received images:** not recovering images held in messaging and app folders and caches (§3).
- **Double-counting device and cloud:** treating the same image on the phone and in Google Photos as two (§4).
- **Shallow extraction:** a logical extraction returning only a subset of the media (§3, guide 162).

Technical limitations

- **Layers vary by maker and version:** gallery apps, trash behaviour and the media store differ (§3, §4).
- **Metadata can be stripped:** shared copies lose it, so the original is needed (§6).
- **Location may be absent:** if services were off, no geotag exists (§6).
- **Remnants are overwritten:** deleted images on the card or device are lost with use (§5, §7).
- **Cloud depends on settings:** whether images reached Google Photos depends on the user's backup choices (§4).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Does the matter turn on when, where or on what device an image was taken, or whether it is genuine or edited?
- Is there an SD card, and is Google Photos backup enabled, so images survive beyond the phone?
- Do we have the device's original images, or only shared copies that may have lost their metadata?

Ask your opponent

- Please preserve and disclose the images and media on the device at Schedule 1, including the media store, gallery trash, any SD card, and the Google Photos library, with full metadata and including deleted items.
- For any image relied on, please provide the device original with metadata, not a shared copy, and confirm its capture date, device and location.
- Please confirm whether relevant images have been edited or deleted, and when.

Ask your eDiscovery / forensic provider

- Which layers, files, media store, gallery, Google Photos, card, hold the images, and what do they add?
- What deleted images can be recovered, and from which layer?
- How are dates, location and edits read, and is the image genuine?

SUGGESTED WORDING · INSTRUCTION FOR AN ANDROID MEDIA ANALYSIS

> "We instruct you to examine the photographs and media on the Android device at Schedule 1 relevant to Schedule 2. Please, on the acquired device at sufficient depth and preserving integrity: (1) locate the images across every layer, the camera and app folders, the media store index, the gallery app and its trash, Google Photos in the associated Google account, and any removable SD card, imaging the card separately and considering its provenance and encryption state; (2) recover deleted images from gallery and system trash, retained media store entries, Google Photos trash and history, and remnants on the device and card; (3) read metadata from the device's original images rather than shared copies, interpret location honestly and corroborate it with the phone's other location sources, and read the capture, modification and media-store dates for their specific meanings, reconciled for time zone; (4) recover edited images with their originals and, where authenticity is in issue, test whether an image is genuine; and (5) reconcile device, cloud and card without double-counting, and state location, dates, provenance and completeness at honest confidence."

§ 12 · QUICK CONTROL

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

The Android media checklist

- ☐ Images located across files, media store, gallery, Google Photos and card
- ☐ SD card imaged separately; encryption state and provenance considered
- ☐ Extraction depth sufficient for folders, caches and index
- ☐ Deleted images recovered from trash, index, cloud and remnants
- ☐ Metadata read from the device's original, not a stripped copy
- ☐ Location interpreted and corroborated
- ☐ Capture, modification and media-store dates read precisely
- ☐ Edited images recovered with originals; authenticity tested where needed
- ☐ Device, cloud and card reconciled without double-counting
- ☐ Findings and limits stated honestly

Red flags

- Only one layer examined: Example 1.
- The SD card ignored: Example 2.
- A media-store date read as the capture date: Example 3.
- A stripped shared copy relied on.
- A geotag treated as certain.
- App-received images missed.
- Device and cloud copies double-counted.

When to involve a digital forensic expert

Whenever an image's time, place, provenance or authenticity matters on an Android device, because the picture lives in several layers and each must be found and read correctly: the expert locates the images across the file system, the media store index, the gallery and its trash, Google Photos and any SD card, imaging the card separately and reading it even when the phone is sealed (Example 2, §3, §5), and recovers deleted images from trash, retained index entries, the cloud's trash and history, and remnants (Example 1, §4, §7). The metadata is read from the device's original, location is interpreted and corroborated, the several dates are read for what each means so a media-store date is never mistaken for a capture date (Example 3, §6), edits are recovered with their originals, and authenticity is tested where it is in issue. Device, cloud and card are reconciled 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 media work finds the picture in every layer it lives in, and reads what it records beyond the image with the honesty any photograph demands.

§ 13 · COMMON QUESTIONS

Frequently asked questions

How is an Android photo different from an iPhone photo, forensically?

The picture records the same things; it lives in more places (§2). An Android image carries the same metadata, when, where and on what device, and is read by the same honest disciplines. But where iOS keeps photos in one library, Android keeps them as files in folders, indexes them in a system media store, shows them through a manufacturer-dependent gallery, syncs them to Google Photos and may store them on a removable SD card. So an Android image is found by pursuing all these layers, and deletion from one rarely clears the others.

What is the media store?

Android's index of every media file on the device (§4). It is a database that records each image, video and audio file with its path, dates and attributes so that apps can find them, and it can retain entries for images since deleted or trashed, so it is both a map of the device's media and a source for recovering what was removed. Its dates are its own, recording when an item entered the index, and must not be confused with an image's capture date, which is read from the original file's metadata.

Can deleted photos be recovered from an Android phone?

Very often, from one layer or another (§4, §7, Example 1). Deleted images persist in the gallery's and system's trash folders for a period, as retained entries in the media store index, in Google Photos' trash and history in the Google account, and as remnants in unallocated space on the device or SD card until overwritten. Because a party rarely clears every layer, a deleted photo is frequently recovered with its metadata intact from one they did not think of, provided the phone, card and account are preserved promptly.

Does the SD card matter?

Often greatly (§5, Example 2). A removable card is its own storage device, imaged and analysed separately, and it is frequently formatted without the phone's encryption, so its images and deleted remnants may be fully readable even when the phone itself is locked and sealed. Its provenance matters too, since it may have been used in other devices and its contents may predate the phone. A card set up as encrypted "adopted" internal storage behaves differently, so its configuration is checked. Overlooking the card can miss the most accessible evidence on a sealed device.

Which date on a photo is the real one?

It depends what is being asked, because there are several (§6, Example 3). The capture date in the image's metadata records when the shutter was pressed; the file's modification date records when the file last changed; the media store's date-added records when the image entered the index, which for a received image is when it arrived, not when it was taken. Confusing these produces wrong conclusions. Each is read for what it specifically records, reconciled for time zone, and an image's provenance, own capture or received copy, is established from the original's metadata.

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

It is a start, but the device original is far better (§6). Sharing, messaging or posting an image usually strips or changes its metadata, so a received copy may have lost the location and capture date that matter, and may be an edited version. The device's original file, or the copy in Google Photos, retains the full metadata and, where the image was edited, the original beneath it. So the analysis works from the original wherever possible, which is why the phone, its card and its Google account are sought rather than a forwarded copy.

§ 14 · REFERENCE

Glossary

DCIM
The camera images folder on the device.

Media store
Android's index database of all media files.

Gallery app
The image viewer, varying by manufacturer.

Trash
A holding area for deleted images before removal.

Google Photos
Google's synced photo library in the account.

SD card
Removable storage, often unencrypted.

Adopted storage
A card configured as encrypted internal storage.

Carving
Recovering deleted files from unallocated space.

Capture date
When the photo was taken, in its metadata.

Stripped copy
A shared image that has lost its metadata.

Sources and authoritative references

The Android 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 (Android media analysis, media store and Google Photos, SD card imaging, 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
- Android developer documentation, MediaStore and scoped storage; Google Photos help (backup, trash): developer.android.com, MediaStore · support.google.com, Photos · EXIF standard (CIPA): 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

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Android media work at the laboratory finds the picture in every layer it lives in and reads what it records beyond the image. On the acquired device at sufficient depth (guide 162), the images are located across the camera and app folders, the media store index, the gallery app and its trash, Google Photos in the associated Google account (guide 164) and any removable SD card, which is imaged separately, its encryption state and provenance considered, and read even when the phone itself is sealed (Example 2, guide 163). Deleted images are recovered from gallery and system trash, retained media store entries, Google Photos' trash and history, and remnants on the device and card, so that a deletion from one layer is defeated by the others (Example 1, guides 155, 4). The metadata is read from the device's original rather than a stripped shared copy, location is interpreted honestly and corroborated with the phone's other location sources (guide 168), the capture, modification and media-store dates are read for their specific meanings so that a media-store date is never mistaken for a capture date (Example 3), edited images are recovered with their originals, and authenticity is tested where it is in issue (guides 126, 127). Device, cloud and card are reconciled without double-counting, and findings are reported at honest confidence 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 insight is that an Android image is the same picture in more places, found by pursuing every layer and read with the honesty any photograph demands.

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