



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 App Data and Third-Party Application Forensics

Every App Is Its Own World: Dating Apps, Marketplaces, Rideshare, Banking and the Rest

Beyond messaging and photos, a phone is a collection of apps, and each app is its own small world of evidence. A dating app records matches, conversations and meetings; a marketplace records listings, purchases and sellers; a rideshare app records journeys, times and drop-off points; a banking or payment app records transactions; a notes or journal app records the user's own words. There is no single method for all of them, because every app stores its data differently, in its own databases and files, with its own structure and its own quirks. The forensic task is to identify which apps matter, to recover and understand each one's particular data, and to interpret it correctly, because a misread field in an unfamiliar app produces confident nonsense. This guide sets out for UK lawyers how iOS apps store their data, how third-party app data is recovered and interpreted, why each app must be understood on its own terms, and how app evidence is corroborated and reported 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. Third-party app analysis is a demanding, high-value strand of its mobile work: identifying the apps that matter, recovering and understanding each one's own databases and files, and interpreting unfamiliar app data correctly rather than guessing. The analysis reaches evidence in dating, marketplace, rideshare, payment and countless other apps, corroborates it across the estate and the app providers, and is reported under CPR Part 35 and CrimPR Part 19, with each app understood on its own terms.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

THIRD-PARTY APP FORENSICS

APP DATABASE INTERPRETATION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: every app is its own world
- 03 How iOS apps store their data
- 04 What different apps record
- 05 Recovering and understanding app data
- 06 Interpretation, attribution and honest limits
- 07 Deployment: the evidence inside the apps
- 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: a phone is a collection of apps, each its own world of evidence, dating, marketplace, rideshare, payment, journal and more, and because every app stores its data differently there is no single method, so the task is to identify the apps that matter, recover each one's particular data, and interpret it correctly rather than guess.

How apps store data (§3): each app keeps its data in its own databases and files, with its own structure, on the phone and often in the cloud. **What they record (§4):** dating apps record matches and conversations; marketplaces record listings and purchases; rideshare records journeys and times; payment apps record transactions; journals record the user's own words. **Recovering and understanding (§5):** each app's data is recovered at the right depth and understood on its own terms, since an unfamiliar structure is easily misread. **Interpretation (§6):** fields are read for what they truly mean, attributed to a person with care, and corroborated. **Deployment (§7):** the evidence inside the apps, matches, meetings, journeys, transactions, listings, deployed honestly.

- **Every app is its own world:** different storage, structure and quirks, with no single method.
- **Rich, varied evidence:** matches, journeys, transactions, listings and the user's own words.
- **Identify what matters:** the relevant apps are found and prioritised for the matter.
- **Understand each on its terms:** a misread field in an unfamiliar app is confident nonsense.
- **Corroborate and attribute:** app data is tied to a person and confirmed across sources.

Every app is its own world of evidence, each stored differently



Figure 1 - each app stores its data in its own database with its own structure; understood on its own terms it yields reliable evidence, misread it yields confident nonsense.

The problem in plain English: every app is its own world

A modern phone is not one thing but dozens: a screen full of apps, each doing something different and, for evidence, each keeping its own private world of data. The messaging and photo apps have their own guides because they are so common, but the point generalises to every app on the device. A dating app records who a person matched with, what they said, and when they arranged to meet. A marketplace app records what they listed for sale, what they bought, and from whom. A rideshare app records the journeys they took, the times, and where they were dropped. A banking or payment app records their transactions. A notes or journal app records their own words, often unguarded. Each of these can be decisive in the right case, and each holds it in its own way.

That last point is the crux, and it is what makes third-party app forensics both powerful and demanding. There is no single method that reads all apps, because there is no single way apps store data. Each app keeps its information in its own databases and files, with its own structure, its own field names, its own conventions, and its own quirks, and much of it is undocumented. So the forensic task has three parts. First, identify which apps matter: a phone may have a hundred apps, and the enquiry must find the few that bear on the case. Second, recover each relevant app's data, at a depth sufficient to reach it (guide 146). Third, and most important, understand each app on its own terms: work out what its data structure actually means, so that a timestamp is read as the right kind of timestamp, a status field as what it really signifies, a record as the event it truly represents. This third step is where the danger lies, because an unfamiliar app misread produces confident nonsense, conclusions that look authoritative but are wrong because a field meant something other than assumed. The discipline is to treat each app as its own world, to understand it properly before drawing conclusions, and to corroborate and attribute the evidence honestly. This guide sets out how iOS apps store their data, how it is recovered and understood, and why each must be read on its own terms.

§ 0 3 · HOW APPS STORE DATA

How iOS apps store their data

- **Each app in its own container:** every app keeping its data in its own storage area on the phone, separate from others, so each app's data is a self-contained world examined in its own right (§2): the per-app store.
- **Databases and files:** apps storing data in their own databases and files with their own structure, so understanding a given app means understanding its particular schema and conventions (§5): the varied structures.
- **Local and cloud:** much app data on the phone, but often also in the app's own cloud service and account, so the app provider is a further source reachable by lawful process (guides 111 to 114): the on-device and cloud data.
- **Caches, media and logs:** apps keeping caches, downloaded media and internal logs alongside their main data, so the full app record includes more than the obvious database (guide 138): the wider app footprint.
- **Depth-dependent:** much app data reached only by a fuller extraction (guide 146), so the deeper method is used where an app's detailed or deleted data matters: the depth question.

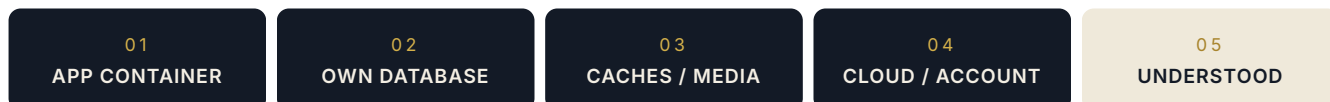


Figure 2 - each app's data lives in its own container, database, caches and often a cloud account, and must be understood on its own terms before it is relied on.

What different apps record

- **Dating apps:** matches, conversations, profiles viewed, and arrangements to meet, with timing, so contact, communication and meetings between people can be evidenced (guide 148): the who-met-whom record.
- **Marketplaces and commerce:** listings, purchases, sales, sellers and buyers, so transactions in goods, and the parties to them, can be established, relevant to fraud and dealing (guide 98): the trading record.
- **Rideshare and travel:** journeys, pick-up and drop-off points, times and routes, so a person's movements can be traced, corroborating location (guide 124): the travel record.
- **Payment and banking:** transactions, transfers, balances and counterparties, so the flow of money, including through payment apps, can be evidenced (guide 128): the money record.
- **Notes, journals and productivity:** the user's own words, plans, lists and records, often candid, so a person's own account of events, intentions and admissions can be recovered (guide 135): the self-recorded material.

Recovering and understanding app data

- **Identify the relevant apps:** the apps that bear on the matter identified from the many installed, so effort is directed at the few that matter rather than every app (§2): the targeted enquiry.
- **Recover at sufficient depth:** each relevant app's data recovered at a depth that reaches it, including deleted app data where needed (guide 146), so the record is complete for the matter: the sufficient extraction.
- **Understand the structure:** each app's database structure and conventions understood, what its fields, statuses and timestamps actually mean, before conclusions are drawn (§6): the understanding step.
- **Recover deleted app data:** deleted records within an app's databases recovered from remnants, backups and snapshots (guides 4, 132, 147), so material a party removed is restored: the deleted app data.
- **Preserve integrity:** the recovery hashed and documented, and the source of each item recorded, so the app evidence is accountable and reproducible (guides 2, 3): the sound recovery.

Interpretation, attribution and honest limits

- **Read fields for what they mean:** each field, status and timestamp interpreted for its true meaning in that app, since an assumed meaning is often wrong and produces confident error (§2): the discipline against misreading.
- **Validate the interpretation:** the understanding of an app's data validated where possible, by testing, documentation or corroboration, so a reading is not merely assumed (guide 100): the checked interpretation.
- **Attribute to a person:** app activity coming from an account on the device, so it is attributed to a person with corroboration, since accounts and devices may be shared (guide 105): the who-did-it question.
- **Corroborate across sources:** app data corroborated with the app provider's records, the estate and other apps, so a finding rests on more than one source (guide 130): the corroborated finding.
- **State confidence and limits:** what an app's data shows, and the limits of interpreting an unfamiliar or undocumented structure, expressed at honest confidence (guide 100): the honest app account.

Deployment: the evidence inside the apps

- **Proving contact and meetings:** dating and social app data establishing contact, communication and arrangements to meet between people, in family, harassment and other matters (guide 148): the connection proved.
- **Proving transactions and dealing:** marketplace and payment app data establishing purchases, sales and transfers, and the parties, in fraud, dealing and commercial matters (guides 98, 128): the transaction evidenced.
- **Proving movement:** rideshare and travel app data establishing journeys and times, corroborating a person's movements and location (guide 124): the movement proved.
- **Recovering the user's own words:** notes, journal and productivity app data recovering a person's candid records, plans and admissions (guide 135): the self-account recovered.
- **Corroborated, honest presentation:** the app findings understood on their own terms, corroborated across the estate and providers, and presented at honest confidence with attribution stated, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the app evidence deployed defensibly.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: an app's data on the phone is one copy, and each app typically has its own cloud and its own provider records, so app evidence is corroborated and completed across those sources. The phone holds each app's local databases, caches and media, including deleted remnants. But most apps sync to their own cloud service and account, reachable by lawful process (guides 111 to 114), which may hold more, and older, data than the device; backups and iCloud (guide 147) hold copies and prior states; the paired Mac and iPad hold some apps' synced data; and the counterparts, the other parties to a match, a trade, a journey, hold their side, and the app providers hold authoritative records obtainable by disclosure. The discipline is to treat the phone's app data as one source among several, corroborating a finding with the app's own cloud, the provider's records and the counterpart, and to understand each app on its own terms wherever its data is found. When an app's local data is incomplete or deleted, its cloud, a backup or the provider may hold more; when a field's meaning is doubtful, the provider's records or the counterpart's copy can confirm the interpretation; and the sources together give a fuller, cross-checked account than any single app store.

EVIDENCE	APP ON PHONE	APP CLOUD / ACCOUNT	BACKUPS / ICLOUD	PAIRED MAC / IPAD	COUNTERPART	PROVIDER RECORDS
App activity	Y: local db	Y: often more	Y: in backup	Some synced	Their side	Y: by disclosure
Deleted app data	Remnants	Cloud copy	Pre-deletion backup	Device remnants	Their copy	Provider retention
Transactions / journeys	Y	Y: account history	In backup	Some	Counterparty	Y: authoritative
Media / attachments	Y: cached	Cloud	In backup	Some	Their copy	Provider
Field interpretation	Structure on device	Confirms meaning	n/a	n/a	Corroborates	Authoritative meaning

Fallback strategy in one line: corroborate app data across the app's own cloud, the provider and the counterpart, and understand each app on its own terms; when local data is deleted or a field is doubtful, the cloud, provider or counterpart resolves it.

Worked examples

EXAMPLE 1 · THE DATING APP THAT EVIDENCED THE MEETING

A matter turned on whether two people had been in contact and had arranged to meet. A §4 dating app on one party's phone held the answer: matches, conversations and an arrangement to meet, with timing (guide 148). The §5 app was understood on its own terms, its fields and timestamps read for what they actually meant, and the §6 conversation attributed to the account holder with corroboration. The §8 finding was corroborated with the counterpart's copy and the app provider's records. Deleted messages within the app were recovered from remnants (guide 4). The contact and the meeting were established from the app's own world of data. The lesson is §4's: dating and social apps record contact, communication and arrangements between people, and, recovered and understood on their own terms, they routinely evidence connections and meetings, provided the app's structure is properly interpreted and the finding corroborated.

EXAMPLE 2 · THE MISREAD FIELD THAT NEARLY MISLED

An examiner unfamiliar with a marketplace app initially read one of its date fields as the time of a transaction, which appeared to support a party's case. The §6 discipline of understanding the app on its own terms caught the error: on proper analysis, that field recorded when a listing was last viewed, not when a purchase occurred, and the actual transaction time was held in a different field and confirmed by the §8 provider's records. Reading the field correctly reversed the apparent conclusion. Had the assumed meaning been relied on, the report would have been confidently wrong. The lesson is §2's and §6's: every app stores its data differently, and a field misread in an unfamiliar app produces confident nonsense, so each app must be understood on its own terms, its fields validated, and its interpretation corroborated, before any conclusion is drawn from it.

EXAMPLE 3 · THE RIDESHARE AND PAYMENT APPS THAT TRACED THE DAY

A dispute required reconstructing a person's movements and spending on a particular day. No single app told the whole story, but together they did: the §4 rideshare app recorded the journeys, pick-ups and drop-offs with times, and the §4 payment app recorded the transactions, and, per §7, both were placed on a timeline with the phone's location data (guides 124, 130). Each app was understood on its own terms and §6 attributed with care, and the §8 findings corroborated with the app providers' records. The day was reconstructed from several apps' worlds combined. The lesson is §7's: different apps hold different pieces, journeys, transactions, movements, and combining them, each understood and corroborated, reconstructs a person's day far more fully than any single app, so the enquiry identifies and assembles all the relevant apps rather than relying on one.

Common mistakes and technical limitations

Common mistakes

- **Misreading an unfamiliar app:** the cardinal error, assuming a field's meaning and producing confident nonsense (Example 2, §6).
- **Not identifying the relevant apps:** missing the apps that matter among the many installed (§5).
- **Relying on one app:** resting on a single app when several hold complementary pieces (Example 3, §7).
- **Shallow extraction missing app data:** a logical extraction relied on where a fuller one was needed for an app's detailed or deleted data (§3, guide 146).
- **Ignoring the app's cloud and provider:** examining the phone while overlooking the app's own cloud and the provider's authoritative records (§8).
- **Attributing to a person carelessly:** app activity attributed to an individual without corroboration (§6, guide 105).
- **Not validating interpretation:** a reading of app data assumed rather than tested or corroborated (§6).
- **Missing deleted app records:** not recovering deleted data within the app's databases (§5).

Technical limitations

- **No single method:** every app stores data differently, so each requires its own understanding: the core challenge (§2).
- **Undocumented structures:** many apps' data is undocumented, so interpretation carries uncertainty that is stated (§6).
- **Depth-dependent:** much app data is reached only by a fuller extraction (§3, guide 146).
- **Attribution needs care:** app data shows account activity; tying it to a person requires corroboration (§6).
- **Apps evolve constantly:** apps and their storage change with every update, so analysis is current-aware (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which apps might hold relevant evidence, dating, marketplace, rideshare, payment, journal, so the right apps are identified and prioritised?
- Is the deeper extraction needed for an app's detailed or deleted data, and are the app accounts available?
- Has the phone and estate been preserved promptly, so app remnants survive?

Ask your opponent

- Please preserve and disclose the data of the apps at Schedule 1 on the device, including deleted app records, and the associated app accounts, cloud data and any backups.
- Please confirm the app account details and provide access or disclosure for the relevant apps.
- Please confirm whether relevant app data has been deleted, and when.

Ask your eDiscovery / forensic provider

- Which apps hold the relevant evidence, and what does each record?
- How is each app's data structure understood and its fields validated, and the interpretation corroborated?
- What does the app's cloud, the provider and the counterpart add, and how is the data attributed?

SUGGESTED WORDING · INSTRUCTION FOR A THIRD-PARTY APP ANALYSIS

"We instruct you to examine the third-party application data on the device at Schedule 1 relevant to Schedule 2. Please, on the acquired, decrypted device and preserving integrity: (1) identify the apps that bear on the matter from those installed, and recover each relevant app's data, its databases, caches, media and logs, at a depth sufficient to reach it, including deleted app records from remnants, backups and snapshots; (2) understand each app on its own terms, working out what its fields, statuses and timestamps actually mean before drawing conclusions, and validate that interpretation by testing, documentation or corroboration; (3) recover the substantive evidence each app holds (for example matches and meetings, listings and purchases, journeys and times, transactions, or the user's own records); (4) corroborate the findings with the app's own cloud, the provider's records, the estate and the counterpart, and attribute app activity to a person with corroboration; and (5) state what each app's data shows, and the limits of interpreting unfamiliar or undocumented structures, at honest confidence, so no conclusion rests on an assumed field meaning."

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

The third-party app checklist

- ☐ Relevant apps identified from those installed
- ☐ Each relevant app's data recovered at sufficient depth
- ☐ Deleted app records recovered from remnants and backups
- ☐ Each app's structure understood on its own terms
- ☐ Field, status and timestamp meanings validated
- ☐ Substantive evidence recovered per app
- ☐ App cloud, provider and counterpart consulted
- ☐ Activity attributed to a person with corroboration
- ☐ Findings corroborated across sources
- ☐ Confidence and interpretive limits stated honestly

Red flags

- An unfamiliar app's field read on an assumed meaning: Example 2.
- Relevant apps not identified among the many installed.
- Reliance on one app when several hold pieces: Example 3.
- A shallow extraction relied on for deep or deleted app data.
- The app's cloud and provider records overlooked.
- App activity attributed to a person without corroboration.
- An interpretation assumed rather than validated.

When to involve a digital forensic expert

Whenever the evidence may lie inside an app, which is to say in most modern matters, because each app is its own world and reading one wrong produces confident error: the expert identifies the apps that matter among the many installed, recovers each one's data at sufficient depth, including deleted records, and, crucially, understands each app on its own terms, working out what its fields and timestamps actually mean and validating that interpretation before drawing any conclusion (Example 2, §5, §6). The substantive evidence, matches and meetings, listings and purchases, journeys and transactions, the user's own words, is recovered, attributed to a person with care, and corroborated with the app's own cloud, the provider's records and the counterpart (Examples 1 and 3, §8). Findings are reported at honest confidence, with the limits of interpreting unfamiliar structures stated, under CPR Part 35 or CrimPR Part 19. This guide continues the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, third-party app work reaches the evidence inside the apps that so often decides a case, treating each app as its own world, understood properly and read on its own terms, so that what the apps hold becomes reliable evidence rather than confident nonsense.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Why isn't there one method for reading all apps?

Because every app stores its data differently (§2, §3). Each app keeps its information in its own databases and files, with its own structure, field names and conventions, much of it undocumented, so there is no single technique that reads them all. The task is to identify the apps that matter, recover each one's data, and understand each on its own terms, working out what its particular structure means. This per-app understanding is what makes third-party app forensics both powerful and demanding.

What kind of evidence do apps hold?

An enormous range, depending on the app (§4). Dating apps hold matches, conversations and arrangements to meet; marketplaces hold listings, purchases and sellers; rideshare apps hold journeys, times and drop-offs; payment apps hold transactions; notes and journal apps hold the user's own candid words. Each can be decisive in the right matter, evidencing contact, dealing, movement, spending or intention. The enquiry identifies which apps bear on the case and recovers the specific evidence each one holds.

How do you avoid misreading an unfamiliar app?

By understanding it on its own terms and validating the interpretation (§6, Example 2). A field in an unfamiliar app is easy to misread, a date that is actually a last-viewed time, a status that means something other than assumed, and a misread field produces confident nonsense. So each app's structure is analysed to establish what its fields, statuses and timestamps actually mean, and that reading is validated by testing, documentation or corroboration with the provider's records and the counterpart, before any conclusion is drawn.

Can deleted app data be recovered?

Often yes (§5). Deleted records within an app's databases frequently persist in the database's free space and remnants, and in backups and snapshots (guides 4, 132, 147), so material a party removed from an app can often be recovered, provided the phone and estate are preserved before it is overwritten. A fuller extraction reaches deleted app data a shallow one cannot (guide 146). The app's own cloud and the provider may also retain data the device no longer holds.

Do we need to look beyond the phone for app data?

Usually yes (§8). Most apps sync to their own cloud service and account, which may hold more, and older, data than the device, and the app provider holds authoritative records obtainable by disclosure; the counterpart holds their side of a match, trade or journey. So app data on the phone is corroborated and completed across the app's own cloud, the provider and the counterpart. This both fills gaps, including deleted data, and confirms the meaning of a field, so the finding rests on more than the device alone.

Does app activity prove the phone's owner did it?

It shows account activity; attributing it to a person takes care (§6, guide 105). An app account and the device may be shared, so app activity is attributed to the account first and to a person only with corroboration from other evidence. This matters especially where the activity is contentious. Attribution is established, not presumed, and stated at honest confidence, so a match, a transaction or a journey is tied to a particular person only where the evidence supports it, not simply because it appears on their phone.

§ 1 4 · REFERENCE

Glossary

App container

An app's own separate storage area on the phone.

App database

An app's store of data, in its own structure.

Schema

The structure and field meanings of a database.

App account / cloud

An app's own online service and stored data.

Provider records

Authoritative data held by the app's provider.

Field interpretation

Working out what an app's fields truly mean.

Validation

Confirming an interpretation by test or corroboration.

Deleted app data

Removed records recoverable from remnants.

Counterpart

The other party to a match, trade or journey.

Attribution

Tying app activity to a real person.

Sources and authoritative references

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

- cflab.uk, digital forensics services (third-party app forensics, app database interpretation, deleted-app-data recovery, 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 (app data 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 (app data protection and sandboxing on iOS): support.apple.com, [Platform Security](#)
- Forensic Science Regulator, Code of Practice v2 (interpretation, validation 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 third-party application forensics as at August 2026. Apps and their data storage change constantly, and there is no single method for all of them: each app must be understood on its own terms, and a field misread in an unfamiliar or undocumented app produces confident error, so interpretations must be validated and corroborated. App activity must be attributed to a person with care. 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

Third-party app work at the laboratory reaches the evidence inside the apps that so often decides a case, treating each app as its own world. From the many apps on a device, the ones that bear on the matter are identified, and each is recovered at a depth sufficient to reach its data, including deleted records from remnants, backups and snapshots (guide 146). Crucially, each app is understood on its own terms, its fields, statuses and timestamps analysed to establish what they actually mean, and that interpretation validated by testing, documentation and corroboration, before any conclusion is drawn, because a field misread in an unfamiliar app produces confident nonsense (Example 2). The substantive evidence each app holds, matches and meetings from dating apps, listings and purchases from marketplaces, journeys and times from rideshare, transactions from payment apps, and the user's own candid words from notes and journals, is recovered, attributed to a person with corroboration, and cross-checked against the app's own cloud, the provider's authoritative records and the counterpart's copy (Examples 1 and 3). Findings are reported at honest confidence, with the limits of interpreting unfamiliar structures stated, under CPR Part 35 or CrimPR Part 19, and handled proportionately under the UK GDPR. This guide continues the iPhone and iPad block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding discipline is that every app is its own world, understood properly and read on its own terms, so that what the apps hold becomes reliable evidence.



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