COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

# iOS Knowledge and Biome: The Device Activity Record

## The Phone's Own Diary of What Was Done, and Why It Must Be Read by an Expert

Just as a Mac keeps a detailed record of its own use, an iPhone keeps a rich diary of device activity in a set of internal databases, the KnowledgeC store and the newer Biome system among them. These record, at a fine grain, what the device was doing and when: which apps were used and for how long, when the screen was on or the phone locked and unlocked, notifications, connections, and much more. For the lawyer, this is one of the most powerful sources on the phone for reconstructing user activity, showing whether the device was in use at a given moment and what was being done with it. But it is also among the most technical and specialist to interpret, undocumented, cryptic, and easily misread, and, like all such records, it ages out over time. This guide sets out for UK lawyers what the iOS activity databases record, how they reconstruct a device-activity timeline, why they demand expert interpretation, and how their evidence is corroborated 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. The iOS activity databases, KnowledgeC, Biome and related stores, are a specialist, high-value part of its mobile work: reconstructing a fine-grained record of app use, device state and interaction, interpreting these cryptic, undocumented stores by expertise rather than guesswork, and corroborating the picture across the estate. The analysis shows what a device was doing and when, at honest confidence, and is reported under CPR Part 35 and CrimPR Part 19, with the technical limits and log rotation stated plainly.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | KNOWLEDGEC & BIOME ANALYSIS | DEVICE-ACTIVITY RECONSTRUCTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

# In this guide

§ 0 1 · ORIENTATION

# Executive summary

The headline point: an iPhone keeps a fine-grained diary of its own use in internal databases such as KnowledgeC and Biome, recording which apps were used and when, screen and lock state, notifications and connections, a powerful source for reconstructing user activity, but cryptic, specialist to interpret, and subject to ageing out.

**What they record (§3):** app usage and duration, device state (screen on, locked, unlocked), notifications, connections and interactions, at fine time resolution. **The timeline (§4):** combined, these reconstruct a detailed record of what the device was doing and when, showing whether it was in use and what was being done. **Expert interpretation (§5):** the databases are undocumented and cryptic, so they demand specialist interpretation, and are easily misread by the untrained. **Rotation and limits (§6):** like all such records, older entries age out, so a gap is not proof of inactivity, and findings are corroborated. **Deployment (§7):** proving whether a device was in use and what was being done at a time, at honest confidence.

- **The phone keeps a diary:** a fine-grained record of app use, device state and interaction.
- **Powerful for activity:** whether the device was in use and what was being done, and when.
- **Cryptic and specialist:** undocumented databases that demand expert interpretation.
- **Ages out:** older entries rotate, so a gap is not proof of inactivity.
- **Corroborate honestly:** the activity record is cross-checked and read at honest confidence.

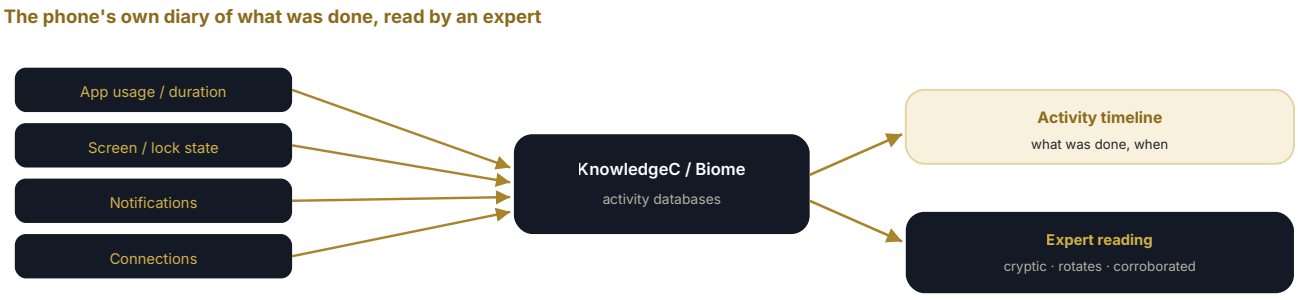


*Figure 1 - the iOS activity databases (KnowledgeC, Biome) record app use, device state, notifications and connections, reconstructing an activity timeline that demands expert, corroborated interpretation.*

§ 0 2 · FIRST PRINCIPLES

# The problem in plain English: the phone keeps a diary

An earlier guide in this series explained that a Mac keeps a detailed record of its own operation in its system artefacts (guide 134). An iPhone does the same, and if anything more intimately. Beneath the visible apps and data, iOS maintains a set of internal databases that quietly record, at a fine grain, what the device is doing moment to moment. The best known is the store often called KnowledgeC, a database of device and user activity; alongside and increasingly in place of it is a newer system, Biome, which records a stream of activity events. Between them, and with related stores, they capture which apps were used and for how long, when the screen was on and when the phone was locked and unlocked, which notifications arrived, what the device connected to, and a great deal more, all timestamped. It is, in effect, the phone's own diary of what its user did with it.

For the lawyer this is one of the most powerful sources on the whole device for reconstructing user activity. Where content shows what a file or message contains, these databases show whether the phone was actually in use at a given moment, which app the person was in, whether they were interacting with the device or it was sitting locked, and how their activity flowed through the day. That can corroborate or contradict an account of what someone was doing, and when, with a precision little else offers. But two cautions define the discipline. First, these databases are among the most technical and specialist artefacts on the phone. They are largely undocumented, their structures are cryptic, their fields easily misunderstood, and a confident-looking conclusion drawn by someone who has not properly understood them can be simply wrong. This is expert territory, not something to be read at face value. Second, like the Mac's logs, these records age out: older entries are pruned over time, so how far back the diary reaches is bounded, and a gap in it is not proof that nothing happened. The task, then, is to recover and correctly interpret these databases, to reconstruct the device-activity timeline they support, to state their technical limits and rotation honestly, and to corroborate the picture. This guide sets out how.

§ 0 3 · WHAT THEY RECORD

# What the iOS activity databases record

- **App usage and duration:** which apps were used, when, and for how long, so the person's engagement with each app across the day can be traced, a detailed usage record (guide 151): the app-use diary.
- **Device state:** when the screen was on or off and the phone locked or unlocked, so periods of active use and of the device sitting idle can be distinguished (§4): the in-use record.
- **Notifications and interactions:** notifications received and interactions with the device, so what reached the user and how they responded can be evidenced (§4): the interaction record.
- **Connections and context:** connections, activity and contextual events the device recorded, adding to the picture of what was happening around the device (guide 152): the contextual layer.
- **Recovered at depth:** these databases reached by a fuller extraction (guide 146) from the acquired, decrypted device (guides 145, 133), with integrity preserved (guides 2, 3): the sound, deep recovery.

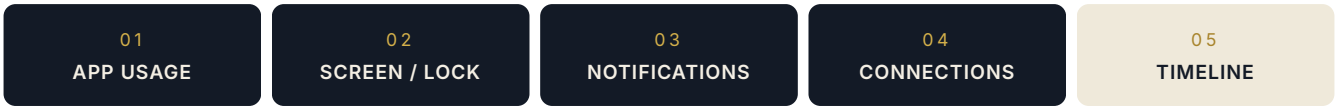


*Figure 2 - the activity databases record app usage, device state, notifications and connections, feeding a fine-grained device-activity timeline.*

§ 0 4 · THE ACTIVITY TIMELINE

# Reconstructing the device-activity timeline

- **Combine the databases:** the KnowledgeC, Biome and related records combined, so app use, device state, notifications and connections are read together as one activity stream rather than in isolation (guides 130, 134): the reconstruction.
- **Normalise the timing:** the timestamps reconciled to a common time base for time zone and any offset, so the activity aligns accurately (guides 108, 130): the aligned timeline.
- **Was the device in use?:** the record showing whether the phone was actively used at a given moment, or sitting locked, so presence at and use of the device can be established (§7): the in-use answer.
- **What was being done?:** the app-usage record showing which app the person was in and for how long, so the nature of the activity, not just its occurrence, is evidenced (guide 151): the what-was-done answer.
- **Corroborate across sources:** the activity timeline corroborated with messaging, location, health and other data (guides 148, 152, 150), so the device-activity picture rests on convergence (guide 130): the cross-checked timeline.

§ 0 5 · EXPERT INTERPRETATION

# Why expert interpretation is essential

- **Undocumented and cryptic:** the databases largely undocumented, with cryptic structures and fields whose meanings are not obvious, so they cannot be read at face value (guide 138's precise-reading theme): the specialist nature.
- **Easily misread:** a field, event or timestamp readily misunderstood by the untrained, producing a confident but wrong conclusion, so interpretation is done by expertise (guide 100): the danger of the naive reading.
- **Meanings established, not assumed:** the meaning of each relevant event and field established through analysis and validation, not assumed, before conclusions are drawn (guide 151): the disciplined interpretation.
- **Evolving across versions:** the databases changing across iOS versions, KnowledgeC giving way to Biome, so the specific device and version are understood (§3): the current-aware analysis.
- **Conclusions to the evidence:** conclusions drawn only to the extent the correctly-understood data supports, with the interpretive uncertainty stated (guide 100): the honest, expert conclusion.

§ 0 6 · ROTATION AND HONEST LIMITS

# Log rotation, corroboration and honest limits

- **Older entries age out:** the databases retaining only a window before older entries are pruned, so how far back the activity record reaches is bounded (guide 134's log-rotation theme): the retention limit.
- **A gap is not inactivity:** an absence of entries for an earlier period reflecting rotation, not proof that nothing happened, so gaps are read honestly (guide 134): the crucial distinction.
- **Preserve promptly:** the record eroding with continued use, so prompt preservation and acquisition maximise how far back the diary reaches (guides 145, 95): the preservation consequence.
- **Backups extend the reach:** earlier states in backups and snapshots (guides 132, 147) preserving activity since aged out, so a backup can extend the record (guide 137): the recovered history.
- **Attribution and honesty:** the activity attributed to the device and, with care, to a person, and findings stated at honest confidence, distinguishing what the record shows from what it does not (guides 105, 100): the honest activity account.

§ 0 7 · DEPLOYMENT

# Deployment: proving what the device was doing

- **Proving the device was in use:** the activity record establishing that the phone was actively used at a given moment, or was locked and idle, relevant to presence, alibi and responsibility (guide 134): the use proved.
- **Proving what was being done:** the app-usage record showing which app the person was in and for how long, so the nature of their activity at a time is evidenced (guide 151): the activity characterised.
- **Corroborating or contradicting an account:** the device-activity timeline tested against a person's account of what they were doing, so a claim is supported or undermined by the phone's own diary (guide 98): the account checked.
- **Anchoring the wider timeline:** the activity record anchoring messaging, location and other evidence in a coherent account of the person's day (guides 130, 96): the day reconstructed.
- **Corroborated, honest, expert presentation:** the findings interpreted by expertise, corroborated, their rotation and limits stated, and presented at honest confidence under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the activity evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

# Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the iOS activity databases are a rich but time-limited node, and they are corroborated with the phone's other evidence and preserved through the estate. The phone holds KnowledgeC, Biome and related activity stores. But backups and iCloud (guide 147) hold earlier states of these databases from before rotation aged them out, extending the reach; the paired Mac and iPad (guides 131, 134) hold their own activity records for the same user's behaviour on those devices; and the phone's other data, messaging, location, health, app data (guides 148, 152, 150, 151), corroborates what the activity record indicates, and the activity record in turn corroborates them. The discipline is to reconstruct the device-activity timeline from these databases, interpreted by expertise, and to corroborate it across the phone's other sources and preserve its reach through backups, so that a gap from rotation is filled from a backup and an activity finding rests on convergence rather than a single cryptic store. When the live databases have rotated, a backup preserves the earlier activity; when an activity event is doubtful, the phone's other data corroborates or qualifies it; and the activity record anchors the wider account of the person's use of the device.

| EVIDENCE | LIVE ACTIVITY DATABASES | BACKUPS / ICLOUD | APFS SNAPSHOTS | PAIRED MAC / IPAD | OTHER PHONE DATA | AGED-OUT / RECOVERABLE |
|---|---|---|---|---|---|---|
| **App usage** | Y: KnowledgeC/ Biome | Y: earlier state | Y: at snapshot | Own activity | App data (guide 151) | Backup restores |
| **Device in use** | Y: screen/lock | Earlier records | At snapshot | Device activity | Messaging/ location | Backup |
| **Notifications** | Y | Backup copies | At snapshot | Some | App records | Backup |
| **Connections / context** | Y | Earlier | At snapshot | Some | Location (guide 152) | Backup |
| **Reach in time** | Limited (rotation) | Y: extends it | Y: at snapshot time | Own window | Varies | Backup extends |

Fallback strategy in one line: reconstruct the activity timeline from the databases, interpreted by expertise, corroborate it with the phone's other data, and where rotation has aged out the live record, a backup or snapshot preserves the earlier activity.

§ 0 9 · IN THE WILD

# Worked examples

**EXAMPLE 1 · THE DIARY THAT SHOWED THE PHONE WAS IN USE**

A party claimed not to have been using their phone at a critical time. The §3 activity databases said otherwise: the §4 device-state record showed the phone unlocked and actively used at that moment, and the §3 app-usage record showed which app they were in and for how long (guide 151). The §5 interpretation was done by expertise, the relevant events and fields understood, not assumed, and the §4 timeline corroborated with §8 messaging and location data (guides 148, 152). The §6 activity was attributed with care and the record's rotation stated. The phone's own diary contradicted the account. The lesson is §7's: the iOS activity databases can show whether a device was actively in use at a given moment and what was being done with it, so they can corroborate or contradict an account of activity, provided they are interpreted by expertise and corroborated, giving the phone's own diary real evidential force.

**EXAMPLE 2 · THE CRYPTIC FIELD THAT WAS NEARLY MISREAD**

An examiner without deep familiarity with the activity databases initially read one of their events as evidence of a particular action at a particular time, which appeared significant. The §5 expert-interpretation discipline caught the error: on proper analysis, the event did not mean what had been assumed, its true significance was different, and drawing the assumed conclusion would have been confidently wrong (guide 100). The meaning of the event was established through analysis and validation, not guessed, and the §6 honest conclusion stated. The naive reading was corrected before it misled. The lesson is §5's: the iOS activity databases are undocumented and cryptic, and a field or event misread by the untrained produces a confident but wrong conclusion, so these stores demand genuine expert interpretation, with the meaning of each relevant event established and validated rather than assumed.

**EXAMPLE 3 · THE GAP THAT WAS ROTATION, AND THE BACKUP THAT FILLED IT**

A party argued that the absence of activity records for an earlier period proved the phone had not been used then. The §6 rotation discipline corrected the inference: the databases retain only a window, and the period predated the surviving records, so the silence was rotation, not proof of inactivity (guide 134). Crucially, the §8 estate filled the gap, a backup taken during the earlier period preserved activity records since aged out of the live phone (guides 137, 147), and those older records showed the relevant use after all. The honest reading of the gap, and the recovery from backup, together defeated the false inference. The lesson is §6's: the activity databases age out, so a gap is not proof of inactivity, and the honest analysis says so, preserves promptly, and looks to backups, which frequently preserve activity the live phone has rotated away.

§ 10 · WHERE IT GOES WRONG

# Common mistakes and technical limitations

## Common mistakes

- **Reading the databases naively:** the cardinal error, drawing confident conclusions from cryptic records without expertise (Example 2, §5).
- **Reading a gap as inactivity:** treating an absence of records as proof nothing happened, when it may be rotation (Example 3, §6).
- **Assuming field meanings:** taking an event or field to mean what it appears to, without validating it (§5).
- **Not preserving promptly:** letting rotation age out the relevant period before acquisition (§6).
- **Ignoring backups:** not using backups and snapshots to recover aged-out activity (Example 3, §8).
- **Not corroborating:** resting an activity finding on the databases alone when other data could confirm it (§4).
- **Attributing to a person carelessly:** device activity attributed to an individual without care (§6, guide 105).
- **Shallow extraction:** a logical extraction relied on where the deeper method was needed to reach the databases (§3, guide 146).

## Technical limitations

- **Undocumented and cryptic:** the databases require specialist interpretation and carry interpretive uncertainty: the core limit (§5).
- **Rotation bounds the reach:** older entries age out, so the record has a limited window and gaps are not absences (§6).
- **Attribution needs care:** the record shows device activity; tying it to a person requires care (§6).
- **Depth-dependent:** the databases are reached only by a fuller extraction (§3, guide 146).
- **Evolving rapidly:** the databases change across iOS versions, so analysis is current-aware (§5).

§ 11 · INTERROGATORIES & DRAFTING AIDS

# Questions to ask · Suggested wording

## Ask your client

- Does the matter turn on whether the phone was in use at a time, or what was being done with it, so the activity databases are relevant?
- Has the phone been preserved promptly, before rotation ages out the relevant period, and are backups available to extend the reach?
- Is the deeper extraction available to reach these databases?

## Ask your opponent

- Please preserve the device and its activity databases (KnowledgeC, Biome and related) without continued use that may cause rotation, and any backups and snapshots.
- Please disclose the device-activity records for the relevant period, and confirm whether the device was in use.
- Please confirm the device model and iOS version.

## Ask your eDiscovery / forensic provider

- What do the activity databases show about whether the phone was in use and what was being done, at the relevant time?
- How far back does the record reach given rotation, and what fills any gap?
- How is the cryptic data interpreted by expertise, and the activity corroborated and attributed?

### SUGGESTED WORDING · INSTRUCTION FOR AN ACTIVITY-DATABASE ANALYSIS

> "We instruct you to examine the iOS device-activity databases (including KnowledgeC, Biome and related stores) on the device at Schedule 1 relevant to Schedule 2. Please, on the acquired, decrypted device at sufficient extraction depth and preserving integrity: (1) recover and analyse the activity records, app usage and duration, device state (screen and lock), notifications, connections and interactions, reconstructing a device-activity timeline on a normalised clock; (2) establish whether the device was actively in use at the relevant time and what was being done with it, interpreting the cryptic, undocumented databases by expertise and establishing and validating the meaning of each relevant event rather than assuming it; (3) address log rotation honestly, stating how far back the surviving record reaches and treating gaps as rotation rather than proof of inactivity, and drawing on backups and snapshots to recover aged-out activity; (4) corroborate the activity with the phone's messaging, location, health and app data; and (5) attribute the activity to the device and, with care, to a person, and state conclusions, and the interpretive limits, at honest confidence."

§ 12 · QUICK CONTROL

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

## The activity-database checklist

- ☐ Phone preserved promptly, before rotation ages out the period
- ☐ Activity databases reached at sufficient extraction depth
- ☐ App usage, device state, notifications and connections recovered
- ☐ Device-activity timeline reconstructed on a normalised clock
- ☐ Whether the device was in use, and what was done, established
- ☐ Cryptic events interpreted by expertise; meanings validated
- ☐ Rotation addressed; gaps read as rotation, backups used
- ☐ Activity corroborated with the phone's other data
- ☐ Attributed to the device and, with care, to a person
- ☐ Conclusions and interpretive limits stated honestly

## Red flags

- Cryptic databases read naively for a confident conclusion: Example 2.
- A gap read as proof of inactivity: Example 3.
- Field or event meanings assumed, not validated.
- Delay allowing rotation to age out the period.
- Backups not used to recover aged-out activity.
- An activity finding not corroborated.
- Device activity attributed to a person without care.

## When to involve a digital forensic expert

Whenever a matter turns on whether a phone was in use or what was being done with it, and always for these particular databases, because they are among the most powerful and the most specialist artefacts on the device: the expert recovers the activity databases at sufficient depth and reconstructs the device-activity timeline, establishing whether the phone was actively used at a moment and what app the person was in (Example 1, §4), and, crucially, interprets these cryptic, undocumented stores by genuine expertise, establishing and validating the meaning of each relevant event rather than reading it naively (Example 2, §5). Log rotation is confronted so that gaps are read as rotation, not inactivity, and backups are used to recover aged-out activity (Example 3, §6), the picture is corroborated with the phone's other data, attributed with care, and reported at honest confidence, with interpretive limits stated, under CPR Part 35 or CrimPR Part 19. Prompt preservation is essential, since rotation erodes the record. This guide continues the iPhone and iPad block. Through **cflab.uk** and **e-discovery.uk**, activity-database work reads the phone's own diary of what was done, one of the most telling sources on the device, with the expertise it demands and the honesty its limits require.

§ 1 3 · COMMON QUESTIONS

# Frequently asked questions

### What are KnowledgeC and Biome?

Internal iOS databases that record device activity (§2, §3). KnowledgeC is a long-standing store of device and user activity; Biome is a newer system, increasingly used alongside or in place of it, recording a stream of activity events. Between them they capture, at a fine grain, which apps were used and for how long, when the screen was on and the phone locked or unlocked, notifications, connections and more, all timestamped. They are, in effect, the phone's own diary of what its user did with it, and one of the most powerful sources for reconstructing activity.

### What can these databases show?

Whether the phone was in use and what was being done, at a fine time resolution (§4, §7). They can show that the device was actively used at a particular moment, or was sitting locked and idle, which app the person was in and for how long, and how their activity flowed through the day. This can corroborate or contradict an account of what someone was doing, with a precision little else offers, which is why they are so valuable, provided they are interpreted correctly and corroborated.

### Why do these need an expert to interpret?

Because they are undocumented and cryptic (§5, Example 2). The databases' structures and fields are largely undocumented, their meanings not obvious, and they change across iOS versions, so a field, event or timestamp is easily misunderstood by the untrained, producing a confident but wrong conclusion. Genuine expertise is needed to establish and validate what each relevant event actually means before any conclusion is drawn. This is specialist territory, not something to be read at face value, and an incorrect interpretation can seriously mislead.

### If there are no activity records for a period, does that prove nothing happened?

No, that is the rotation trap (§6, Example 3). These databases retain only a window of activity before older entries are pruned, so an absence of records for an earlier period may simply mean they have rotated, not that the phone was unused. A gap is not proof of inactivity. An honest analysis says so, preserves the phone promptly to save what remains, and looks to backups and snapshots, which frequently preserve activity records since aged out of the live device, extending how far back the diary reaches.

### How reliable is this evidence?

Reliable when interpreted by expertise and corroborated (§5, §6). Correctly understood, these databases are among the most telling sources on the phone, but their value depends entirely on proper interpretation, the meaning of each event established and validated, not assumed, and on honest treatment of rotation and interpretive uncertainty. Findings are corroborated with the phone's other data, messaging, location, health, attributed with care, and stated at honest confidence. Read this way they are powerful; read naively they can be confidently wrong.

### How urgent is preserving the phone for this?

Genuinely urgent (§6). Because these databases rotate, ageing older entries out as the device keeps running, every day of continued use can erode the record of the period in issue. Preserving the phone promptly, and acquiring it at sufficient depth while the records survive, maximises how far back the activity diary reaches, and backups taken earlier can preserve activity since rotated away. As with iOS acquisition generally (guide 145), prompt handling directly determines how much of this valuable activity record survives to be analysed.

§ 14 · REFERENCE

# Glossary

**KnowledgeC**
An iOS database of device and user activity.

**Biome**
A newer iOS activity-event system.

**Activity database**
An internal store of device-activity events.

**App usage**
Which apps were used, when and for how long.

**Device state**
Screen on/off, locked/unlocked.

**Device-activity timeline**
The reconstructed record of use over time.

**Log rotation**
Ageing out of older activity entries.

**Expert interpretation**
Specialist reading of cryptic data.

**Validation**
Confirming the meaning of an event or field.

**Corroboration**
Cross-checking with the phone's other data.

## Sources and authoritative references

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

- cflab.uk, digital forensics services (KnowledgeC and Biome analysis, device-activity reconstruction, expert interpretation, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 06 · Analysis and Phase 04 · Collection (device-activity analysis as practised): e-discovery.uk/edrm/analysis · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple Platform Security guide (on-device intelligence and activity data protection): support.apple.com, Platform Security
- Forensic Science Regulator, Code of Practice v2 (interpretation, validation and honest reporting of specialist artefacts) and ISO/IEC 27037: gov.uk, FSR Code · iso.org, 27037
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

# Working with Computer Forensics Lab

Activity-database work at the laboratory reads the phone's own diary of what was done, one of the most telling sources on the device, with the expertise it demands and the honesty its limits require. On the acquired, decrypted device at sufficient extraction depth (guides 145, 146, 133), the activity databases, KnowledgeC, Biome and related stores, are recovered, and the device-activity timeline is reconstructed on a normalised clock, establishing whether the phone was actively in use at a moment and what app the person was in and for how long (Example 1, §4). Crucially, these cryptic, undocumented databases are interpreted by genuine expertise: the meaning of each relevant event is established and validated, not assumed, so a naive reading that would be confidently wrong is avoided (Example 2, §5). Log rotation is confronted honestly, gaps are read as rotation rather than inactivity, and backups and snapshots are used to recover activity since aged out of the live device (Example 3, §6, guides 137, 147). The picture is corroborated with the phone's messaging, location, health and app data, attributed to the device and, with care, to a person, and reported at honest confidence, with the interpretive limits stated, under CPR Part 35 or CrimPR Part 19. Because rotation erodes the record with use, prompt preservation is essential. This guide continues the iPhone and iPad block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the guiding principle is that the phone's activity diary is powerful precisely when it is read by an expert, established and validated event by event, and honest about what it does and does not show.

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