COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Mobile Phone Forensics

Extraction Levels, Encryption, App Evidence, Deleted Data and the Honest Limits of the Most Personal Device in the Case

The phone is the closest thing litigation has to a witness who was always there: messages in a dozen apps, photographs with coordinates, calendars, calls, browsing, payments, health data and the pattern of a life in app timestamps. It is also the most defended device in the case: encrypted by default, sealed by passcodes, governed by security architectures that change with every model year, and served by an extraction industry whose capabilities are real, uneven and routinely oversold. This guide gives lawyers the working model: what extraction levels exist and what each actually yields, how encryption and device state govern access, where app evidence lives and how it dies, what deleted really means on modern flash storage, the preservation moves that must happen before anyone touches the handset, and the questions that separate a realistic mobile strategy from an expensive disappointment.

⏱ Estimated reading time: 27 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. Mobile examination is core casework: iOS and Android extraction at every level the device and the law permit, app-evidence analysis, deleted-data recovery with honest boundaries, and the device-plus-cloud correlation that modern phones demand. Its eDiscovery arm, **e-discovery.uk**, renders mobile collections reviewable at disclosure scale.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | IOS & ANDROID EXTRACTION | APP & DELETED-DATA ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: MOBILE EVIDENCE IS GOVERNED BY THREE GATES: EXTRACTION LEVEL, ENCRYPTION STATE, AND APP ARCHITECTURE: AND STRATEGY IS SET BY WHICH GATES OPEN

Gate one, extraction level. Mobile collection is not one thing: **logical/advanced logical** extraction takes what the operating system offers (the backup surface: messages, contacts, media, many app stores: substantial, and bounded); **full file system (FFS)** extraction reaches the device's complete file structure including app sandboxes, databases with their deleted-record internals, system logs and location caches: the level at which mobile forensics earns its adjectives; **physical** extraction (bit-level) survives mainly on older or specific devices, its role largely absorbed by FFS on modern encrypted handsets. Each level yields a different evidence universe, and reports must say which was achieved: "we examined the phone" means nothing without it. **Gate two, encryption and state.** Modern devices encrypt by default; access turns on credentials (passcode known, or lawfully compelled, or recovered), device state (a phone that has been unlocked since power-on holds keys in memory that a rebooted one does not: the BFU/AFU distinction guide 148 will detail), and the shifting frontier of lawful access tooling: which is device-, version- and patch-specific and changes monthly: so capability statements are dated, device-specific and verified, never assumed from last year's case. **Gate three, app architecture.** Each app decides where its data lives (device, cloud, both), how it is protected, and what deletion does: WhatsApp's local databases, Signal's designed forgetting, iMessage's cloud sync: so "get the messages" decomposes into per-app answers, and the phone is always examined as one node of the app's wider architecture (the source-architecture discipline this series applies everywhere, at its most literal). Two standing rules govern everything: **preserve state before strategy** (isolate from networks, maintain power, change nothing: the handling errors of §7 are the ones no expert can undo), and **promise from the device in hand, not the marketing**: realistic expectations, set early, are the difference between mobile evidence deciding the case and mobile costs deciding the budget.

- **The level is the finding's foundation:** every mobile report states extraction level, tool and coverage: and every disclosure request asks the other side the same.
- **State is evidence:** powered, unlocked-since-boot, network-isolated or not: recorded at seizure, because it governs what is possible and proves the handling was competent.
- **Apps are architectures, not folders:** the per-app map (device store, cloud twin, backup presence, deletion behaviour) is drawn before promises are made.
- **Deleted is a spectrum:** database-internal recoverable records are routine; flash-level resurrection of truly purged content is largely mythology on modern encrypted phones: §6 draws the honest line.
- **The phone is never alone:** cloud accounts, backups, paired computers and counterpart devices carry much of what the handset holds: the ensemble is the strategy when the device gate stays shut.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the witness with a lock on its mouth

Everyone in the case knows the phone matters: it was in the room, in the pocket, in the hand, for every relevant event. What the profession consistently misjudges is the shape of the difficulty. The naive fear: "everything is encrypted, we'll get nothing": is wrong: with credentials or the right circumstances, modern extraction reaches deeper into a phone than any examination reached a decade ago. The naive hope: "the lab can get into anything": is equally wrong: access is gated by device, version, state and law, and the gate's position changes faster than any published guide. The truth is conditional, and the conditions are checkable: which device, which version, what state, whose credentials, what legal basis: five questions answerable in a first call, from which a realistic strategy follows.

The second misjudgement is treating the handset as the whole story. The modern phone is a terminal onto accounts: its messages sync, its photos upload, its backups snapshot: and half of mobile practice is knowing when the cloud, the backup or the counterpart device answers the question the locked handset will not. This guide is the mobile block's foundation: guides 62-65 and the specialist series from 145 take each gate and each app in depth.

§ 0 3 · GATE ONE

Extraction levels: what each route actually yields

LEVEL	WHAT IT YIELDS · WHAT IT MISSES
Logical / advanced logical	The OS-offered surface: call logs, contacts, SMS/iMessage, media, many app stores via backup interfaces. Fast, least invasive, broadly available: and bounded: app sandboxes it cannot enter, deleted records it cannot see, system artefacts it never touches. The right level for many civil scopes; the wrong level to call "the phone examined" in a contested matter.
Full file system (FFS)	The complete file structure: app databases with internal deleted records, protected app data, system and diagnostic logs, location caches, usage patterns. The modern gold standard: device-, version- and access-dependent (credentials or lawful-access tooling required), and the level at which the interesting findings of this block live.
Physical (bit-level)	Full storage image including unallocated space: decisive on legacy and some specific devices; on modern encrypted handsets, largely superseded: encrypted unallocated space yields nothing FFS does not, which is why "we need a physical" is usually last decade's request.
Targeted / consent-scoped	Defined app sets or date ranges, often for proportionality or privacy (the extraction-from-witnesses concerns of the college guidance): smaller universe by design, with the scope documented as carefully as the findings.
Cloud-side collection	Not an extraction level but the constant companion: account-based collection of synced and backed-up content: frequently richer than a locked handset and always compared against the device where both exist.

§ 0 4 · GATE TWO

Encryption and device state: the access question

- **Default encryption is the baseline:** modern iOS and Android encrypt storage with keys derived from the passcode and hardware: without credentials, the storage is ciphertext, and the realistic access routes run through the passcode, the state, or the tooling frontier.
- **State decides more than lawyers expect:** a device unlocked at least once since power-on (AFU) holds working keys in memory that expand what tooling can reach; a rebooted or drained device (BFU) is at maximum defence: which is why §7's first rule is keep it powered and never reboot: guide 148 takes the full detail.
- **Credentials change everything:** a known passcode converts most questions into FFS answers: making the credential conversation (consent, contractual obligations, court compulsion where available) an early strategic track, not an afterthought: guide 117 covers collection without disclosing the password.
- **The tooling frontier moves monthly:** lawful-access capability is specific to device model, OS version and patch level, and neither side should assert or concede access without a current, device-specific check: capability statements carry dates.
- **Biometrics and repeated attempts carry risk:** lockouts, security escalations and data-destruction settings mean access attempts are planned, counted and executed by examiners, never improvised by clients or IT: guide 147's subject.

§ 0 5 · GATE THREE

App evidence: where it lives, how it dies

- **The per-app map:** for each app that matters: where is the device store (database, cache, media), is there a cloud twin (sync, backup), what does deletion do (flag, purge, propagate), and what do timestamps mean (sent, delivered, read, edited): four questions that scope every messaging dispute before promises are made.
- **Databases are the workhorses:** most app evidence sits in structured stores whose internals: including records flagged deleted but not yet vacuumed: are exactly what FFS extraction exists to reach: the recoverable-deleted layer of §6.
- **Ephemeral by design exists:** Signal-class apps and disappearing-message modes genuinely minimise residue: the honest answer is architecture-specific, and the ensemble (counterpart devices, screenshots, notification records) is the strategy: guides 64 and 152.
- **Attachments travel separately:** media caches, download folders and cloud stores hold message attachments after messages go: the photograph often survives the chat that carried it.
- **Usage artefacts frame everything:** system-level records of app installation, use patterns and notifications corroborate or contradict accounts of who used what, when: the framing layer around every app finding.

§ 0 6 · THE HONEST LINE

Deleted data on modern phones: the honest position

- **Routine and real:** records deleted within apps but persisting inside databases (flagged, unvacuumed, in journals and write-ahead logs): recovered constantly at FFS level, with the deletion itself often datable: the layer most "recovered deleted messages" headlines actually describe.
- **Conditional:** content surviving in caches, thumbnails, notification stores and search indexes after the primary record went: app- and version-specific, checked rather than promised.
- **Largely gone:** flash-level recovery of content truly purged on modern encrypted storage: TRIM, encryption and wear-levelling have closed the unallocated-space romance of the spinning-disk era: claims to the contrary get the dated-capability scrutiny of §4.
- **The ensemble redeems:** what the device purged, the backup snapshot, the cloud twin or the counterpart phone frequently kept: deletion analysis is an architecture walk, not a single-device verdict: §8's matrix.
- **Deletion is evidence:** gaps, vacuum events, wiped conversations against intact neighbours: dated where possible and framed against duty chronologies: the conduct layer, mobile edition.

§ 0 7 · BEFORE ANYONE TOUCHES IT

Preservation and handling: before anyone touches it

- **Isolate:** airplane mode, Faraday protection where warranted: because a networked phone can be remotely wiped, and MDM-enrolled corporate devices (guide 160) can be wiped by policy or panic: the risk that has destroyed more mobile evidence than any technical failure.
- **Power:** keep it charged; never let it die; never reboot: the AFU state preserved is capability preserved.
- **Do not explore:** no scrolling by clients, HR or lawyers: every unlock and swipe writes records, alters last-access data and, in disappearing-message contexts, destroys content by reading it.
- **Record state at custody:** powered, locked status, network, battery, visible notifications: photographed and noted: the seizure record that answers handling challenges months later.
- **Freeze the ecosystem too:** cloud holds, backup preservation, paired-computer identification and MDM wipe-suspension instructions issued the same day: the phone's twins are as urgent as the phone.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the handset in isolation. Phone-borne evidence coexists in: cloud accounts (iCloud/Google syncing messages, photos, locations, app data: guides 149 and 170); computer backups (iTunes/Finder and Android equivalents: point-in-time phones, often reaching years back: guide 158); the paired computers themselves (sync artefacts, message mirrors, cached media); counterpart devices (the other end of every conversation: the standing rescue of messaging disputes); app providers' own platforms (business-tier exports and, via legal process, account records); mobile-network operators (call and cell records within their windows); MDM and corporate consoles (device state, compliance, wipe history: guide 160); and wearables and vehicles paired to the handset (guides 122-123, 156). When the device gate stays shut: locked, wiped, lost, destroyed: this map is the case: the destroyed-phone reconstructions of guide 260 are built entirely from it.

EVIDENCE	HANDSET (BY LEVEL)	CLOUD ACCOUNT	COMPUTER BACKUPS	COUNTERPART DEVICES	OPERATOR / PROVIDER	DELETED / RECOVERABLE
Messages	Y: app stores, FFS internals	Synced sets, app-dependent	Point-in-time copies	Y: the other end	Via legal process, app-dependent	Database layer routine; purge conditional
Media	Y + caches/ thumbnails	Photo libraries: Y	Y	As received/ shared	n/a	Attachments outlive chats
Locations	Caches, photos, app records	Timeline/ location services	Snapshotted stores	n/a	Cell records: window-bound	Varies; qualification mandatory (guide 153)
Calls	Y: logs	Synced logs sometimes	Y	Their logs	Y: the independent record	Operator records outlive handsets
App usage / state	Y at FFS	Account activity	Partial	n/a	Provider logs	Varies

Fallback strategy in one line: when the handset will not speak, ask its twins in order: cloud, backups, paired computers, counterparts, operators: and remember the seizure-day ecosystem freeze is what keeps those twins alive to ask.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE LEVEL THAT CHANGED THE ANSWER

An employment tribunal claim turned on whether a manager had sent harassing messages later deleted. A first examination: logical extraction by a generalist provider: reported "no relevant messages present" and the respondent pleaded accordingly. The claimant's expert asked the level question, then re-examined at full file system: the messaging database's internals held forty-one records flagged deleted but unvacuumed, spanning the pleaded period, with deletion timestamps clustered the evening the grievance was filed. The first report had been accurate about the surface and silent about the level; the second was accurate about the phone. The pleading was amended, and the tribunal's remarks about the first examination's description ("the phone was examined") have travelled well beyond the case.

EXAMPLE 2 · THE REBOOT THAT CLOSED THE GATE

In a fraud investigation, a suspect director's iPhone was seized powered-on and unlocked-since-boot: AFU, with substantial lawful-access prospects for its model and version. An IT staffer, meaning to be helpful, powered it off "for security" overnight. The device came back BFU: keys gone from memory, the access route closed for that model at that patch level, and the passcode unknown and uncompellable in the circumstances. The evidence was rebuilt the long way: iCloud collection under the account's own legal route, a fourteen-month-old iTunes backup on his home laptop, and counterpart phones of three correspondents: months of work replacing what state preservation would have delivered in days. The handling memo now taped inside that client's evidence cupboard is one line: do not turn it off.

EXAMPLE 3 · THE ENSEMBLE THAT OUTRAN THE WIPE

A departing executive's company phone arrived at the laboratory factory-reset: "it was slow, I wiped it before handing it back". The handset was honest ciphertext: nothing recoverable: and it did not matter. The ecosystem freeze had beaten him: the corporate backup taken by MDM eleven days earlier held the pre-wipe state; his iCloud account, preserved on day one, carried the message threads through the relevant quarter; the paired MacBook's message mirror duplicated the key conversations; and the wipe itself: timed by the device's activation records against his diary: became the conduct exhibit. The tribunal treated the reset as it read: not housekeeping but response: and the ensemble supplied everything the handset was meant to take with it.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Level-blind reports and requests:** Example 1's trap: "examined" without the word that defines the universe.
- **State destroyed by helpfulness:** Example 2's reboot; the client scroll-through; the IT "quick look" that fires the disappearing messages.
- **The ecosystem freeze skipped:** handset seized, cloud and backups left to their clocks: the day-one omission Example 3's opposite number would have prayed for.
- **Capability assumed from last year:** access promised or conceded without the dated, device-specific check.
- **Physical-extraction nostalgia:** demands for bit-level images of encrypted devices that FFS already answers.
- **App architecture ignored:** "get the WhatsApps" scoped without the per-app map: cloud twins and backups unpursued.
- **Deleted-data mythology:** flash-resurrection promises that §6's honest line exists to kill.
- **Privacy and proportionality unaddressed:** full extractions where targeted scopes were owed: the college-guidance concerns, invited.

Technical limitations

- **Access is conditional and dated:** device, version, patch, state, credentials: the five facts cap everything, and change.
- **FFS is not omniscience:** app-level encryption and designed-ephemeral architectures keep secrets even from full file systems.
- **Timestamps carry app semantics:** sent/delivered/read/edited mean what each app means: read before chronology is argued (guide 108's territory).
- **Attribution is the handset's oldest gap:** the phone proves itself, not the hand that held it: usage patterns, biometrics context and the series' join do the rest (guide 255).
- **Wear and damage have physics:** broken devices are guide 119's subject: recoverable more often than clients fear, less often than films suggest.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The five access facts per device: model, OS/patch, state, credentials position, legal basis: before any promise is made?
- What is the ecosystem: cloud accounts, backup habits, paired computers, MDM enrolment: and is the freeze issued today?
- Which apps carry the issues, and what does the per-app map say about cloud twins and deletion behaviour?

Ask your opponent

- Please state, per device examined: extraction level achieved, tool and version, credentials position, device state at examination, and coverage limitations: and produce the examination notes.
- Please confirm preservation of the associated cloud accounts, computer backups and paired devices, and that no device has been reset, rebooted or synchronised since [date].
- Where deleted content is asserted unrecoverable: please state the level examined and the database-layer analysis performed.

Ask your eDiscovery / forensic provider

- What does the current, dated capability position say for this exact device and state?
- What will each candidate level yield for the apps in issue: and what does the ensemble offer if the gate stays shut?
- What targeted scope satisfies proportionality and privacy while reaching what the case needs?

SUGGESTED WORDING · MOBILE LIMB FOR THE PRESERVATION INSTRUCTION

> "With immediate effect in respect of each device listed: (1) do not power off, reboot, unlock, browse, reset or synchronise the device; isolate it from all networks (airplane mode; SIM removal only on examiner instruction) and maintain charge; (2) record and photograph its state (power, lock, network, battery, visible notifications) and transfer it to the examiner under custody record; (3) suspend any MDM wipe, retirement or compliance action affecting it, confirming the console position in writing; (4) preserve the associated cloud accounts, computer backups and paired devices, making no deletion, sync or settings change; and (5) provide the device's make, model, OS version and credentials position to the examiner today. Extraction level and scope will be specified following the capability check."

§ 12 · QUICK CONTROL

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

The mobile checklist

- ☐ Five access facts documented per device before promises
- ☐ State preserved: powered, unrebooted, isolated: and recorded at custody
- ☐ Ecosystem freeze issued day one: cloud, backups, paired devices, MDM
- ☐ Per-app map drawn for the apps in issue
- ☐ Capability check current, dated and device-specific
- ☐ Extraction level chosen deliberately; stated in every report and demanded in every request
- ☐ Deleted-data findings tied to the database layer actually examined
- ☐ Targeted scopes used where proportionality and privacy demand
- ☐ Timestamps interpreted per app semantics before chronologies
- ☐ Attribution built by the join, never assumed from possession

Red flags

- "The phone was examined" with no level stated: Example 1's tell.
- A device rebooted, reset or synced after the duty arose.
- Absence findings from logical extractions in deleted-message disputes.
- Capability claims without dates or device specifics.
- A wiped handset with an unfrozen ecosystem: or a wipe timed against the dispute.
- Full-extraction demands where targeted scope was plainly owed.
- MDM consoles left able to wipe evidence devices.

When to involve a digital forensic expert

Before the device is touched: the state and ecosystem decisions of §7 are made in the first hours and unmade never; at the capability check, where the five facts meet the current frontier and strategy follows; at extraction, where level, tool and scope are matched to the issues and the law; and at analysis, where database-layer recovery, app semantics and the join turn extractions into findings: Examples 1-3's three directions. Reported under CPR Part 35 with levels, coverage and limits stated: and through **e-discovery.uk**, mobile collections rendered into review alongside the estate's other sources, threaded per guide 70's cross-platform method.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can the laboratory get into a locked phone?

The only honest answer is conditional: it depends on the model, OS and patch level, the device's state (AFU/BFU), the credentials position and the legal basis: five facts a first call establishes, against a capability frontier that moves monthly. Sometimes yes, quickly; sometimes yes, expensively; sometimes no, and the ensemble becomes the strategy. What no competent practice offers is the unconditional yes: guide 147 takes the full question.

Do we need the phone at all if everything syncs to the cloud?

Usually both, deliberately: the cloud carries breadth (and survives device loss), while the device carries what never synced: FFS-level app internals, deleted-record layers, system and location artefacts, and the local truth against which cloud copies are compared. Where only one is reachable, the other's absence is stated as a limitation. The comparison itself: device against cloud twin: is frequently the finding (deletions dated by divergence).

How long does mobile examination take and what does it cost?

Scoped work is days-to-weeks: capability check and preservation immediately; extraction hours-to-days once access exists; analysis scaling with apps and issues, not gigabytes. The budget-killers are avoidable: access adventures on hostile devices, full extractions where targeted scopes serve, and mythology-driven recovery quests past §6's line. Fixed-fee phases: preserve, assess, extract, analyse: keep the spend tied to decisions.

The other side's expert says deleted messages are unrecoverable. Do we accept that?

Ask the level question first: unrecoverable at logical extraction is a statement about the surface, not the phone (Example 1). Then the architecture questions: which app, what deletion behaviour, what cloud twin and backups exist, what do counterpart devices hold. Acceptance is sometimes right: §6's honest line runs both ways: but only after the report states level, database-layer analysis and the ensemble position. The request wording in §11 extracts exactly that.

What about the privacy of everything else on the phone?

Central, not peripheral: phones hold whole lives, and UK practice: the college extraction guidance, UK GDPR minimisation, proportionality under PD 57AD: expects targeted scopes, staged review, and handling that separates the relevant from the merely present. Targeted extraction, examiner-side filtering and protocol-agreed scopes are standard tools; "image everything and browse" is neither lawful practice nor good strategy. The specification carries the privacy architecture.

Company phone, personal phone, or both: what should the scope chase?

Follow the apps, not the ownership labels: work WhatsApp lives on personal handsets, personal Gmail on corporate ones, and the issues decide which stores matter. Corporate devices add MDM records and policy powers (guide 160); personal devices add the BYOD consent-and-proportionality track (guides 68 and 171). The per-app map across both, drawn early, is the scoping answer: and the ecosystem freeze covers whichever devices it names.

§ 14 · REFERENCE

Glossary

AFU / BFU
After/Before First Unlock; the memory-key state governing access (guide 148).

Capability check
The dated, device-specific access assessment; strategy's first document.

Ecosystem freeze
Day-one preservation of cloud, backups, paired devices and MDM state.

Five access facts
Model, OS/patch, state, credentials, legal basis.

FFS extraction
Full file system collection; the modern gold standard.

Logical extraction
The OS-offered surface; substantial and bounded.

Per-app map
Device store, cloud twin, deletion behaviour, timestamp semantics.

State record
The seizure-time note of power, lock, network and battery.

TRIM
Flash housekeeping that closes unallocated-space recovery.

Vacuum / WAL
Database housekeeping and journals; where deleted records persist.

Sources and authoritative references

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

- cflab.uk, digital forensics services (iOS and Android extraction, app and deleted-data analysis, capability assessment, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (device and ecosystem preservation; mobile collections into review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- College of Policing, extraction of material from digital devices: college.police.uk, extraction guidance · Forensic Science Regulator: gov.uk/forensic-science-regulator
- ISO/IEC 27037 and laboratory standards: iso.org, 27037 · iso.org, 17025
- PD 57AD and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35 · ICO: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Mobile matters at the laboratory begin with the two moves that cannot wait: state preservation (the §7 handling rules, communicated to whoever holds the device within the hour) and the ecosystem freeze (cloud, backups, paired devices, MDM: instructed the same day). The capability check follows: the five facts against the current frontier, in writing, with strategy and fixed-fee phases built on what is actually possible. Extraction runs at the level the issues and the law support; analysis delivers the database-layer recovery, per-app semantics and joins of Examples 1-3; and where the handset gate stays shut, the ensemble reconstruction: cloud, backups, counterparts, operators: is standing work, not improvisation. Reporting is CPR Part 35 with levels and limits stated; privacy architecture (targeted scopes, staged review) is built into every specification; and through **e-discovery.uk**, mobile evidence lands in review threaded with the rest of the case. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a relevant phone is in anyone's hands right now, the handling instruction comes before this paragraph finishes being read.

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