



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

CRM Evidence: Salesforce, HubSpot and Customer Systems

Pipelines, Field Histories and the System That Watched the Relationship

In client-poaching claims, restrictive covenant disputes, commission fights and misrepresentation cases, the CRM is the witness that was in every meeting: who owned the relationship, when the pipeline moved, which contacts were exported the week before resignation, what the sales notes candidly said while the formal correspondence stayed polite. Salesforce, HubSpot, Dynamics and their kin are guide 71's databases wearing a sales interface: object models instead of plain tables, field-history tracking instead of generic audit trails, and login and export logs that record exactly the conduct departing-employee cases turn on. This guide maps CRM evidence for UK lawyers: the object anatomy of accounts, contacts, opportunities and activities, field history and audit capabilities across the major platforms, export and report logs as exfiltration evidence, deletion and recycle-bin behaviour, collection routes from native exports to API acquisition, and the pipeline analyses that turn a sales database into a chronology of the disputed relationship.

🕒 Estimated reading time: 26 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. CRM evidence anchors its restrictive covenant, team-move and commission casework: field-history and login-log analysis across Salesforce, HubSpot and Dynamics, export-event investigation in departing-employee matters, and pipeline chronologies that date when relationships really moved. Its eDiscovery arm, **e-discovery.uk**, hosts CRM extracts beside the correspondence estate in review.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

CRM & CUSTOMER-SYSTEM FORENSICS

EXPORT & LOGIN-LOG ANALYSIS

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: the system that watched the relationship
03	Anatomy: objects, activities and the notes layer
04	Histories and logs across the platforms
05	Exports, reports and the exfiltration record
06	Deletion, recycle bins and recovery
07	Collection routes and pipeline analysis
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

Executive summary

THE HEADLINE POINT: THE CRM RECORDS THE RELATIONSHIP AND, SEPARATELY, RECORDS WHO TOUCHED THE RECORD: DEPARTING-EMPLOYEE CASES ARE USUALLY DECIDED IN THE SECOND LAYER

CRM platforms hold two evidence strata. **The relationship record:** accounts, contacts, opportunities and activities: who the customer's people were, what was pitched and promised, how the pipeline moved stage to stage, what the free-text notes said when nobody was drafting for disclosure: the layer that proves (or disproves) the pleaded relationship story in covenant, commission, misrepresentation and agency disputes: with the notes and activity streams frequently supplying the candour the email estate lacks, because salespeople write CRM notes the way they talk. **The conduct record:** what users did to the system: field histories tracking who changed which value when (ownership reassignments, stage regressions, contact detail edits), login histories with timestamps, IPs and client types, report executions and: critically: **export events:** the logged act of pulling contact lists and pipeline data out: which in team-move and data-theft cases is the case: the sales director who ran a full-contact export at 22:14 nine days before resigning has written the claimant's chronology for them (guide 57's method on a sales-shaped log estate, and guide 41's exfiltration patterns with the CRM as source). Capability varies by platform and edition and is audited before promising: Salesforce's field history tracks selected fields with retention that expands on higher tiers (and archive add-ons extending it), its setup audit trail records administrative acts, and event monitoring (edition-dependent) records exports and API pulls in detail; HubSpot logs property histories per record and account-level activity including exports; Dynamics carries auditing that must be enabled per entity: so the first technical question in every CRM matter is the guide 66 lattice question retooled: **which histories does this org actually keep, since when, and what is rotating away while we correspond.** Collection follows guide 71's discipline: the slice defined by objects, fields and date ranges; native or API extraction with the reproducibility bundle; the histories and logs collected as first-class evidence beside the records they judge; and provider-side trash and archive layers (recycle bins with their windows, soft-deleted records) checked before any deletion is conceded. The distinctive analytical deliverable is the **pipeline chronology:** the disputed relationships reconstructed as dated sequences: created, worked, advanced, reassigned, exported, gone quiet, resurfaced at the competitor: interleaved with the correspondence estate per guide 70, which is how a database of sales admin becomes the narrative spine of a covenant injunction.

- **Two strata, always:** the relationship record and the conduct record: collected together, because the second authenticates and dates the first.
- **Export logs are the smoking gun class:** departing-employee matters turn on logged pulls: preserved day one, before rotation.
- **Capability is org-specific:** field-history scope, audit depth and log retention vary by platform, edition and configuration: audited before anything is promised.
- **Notes are the candour layer:** free-text and activity streams say what emails would not: collected at full fidelity, reviewed early.
- **The pipeline chronology is the deliverable:** relationships as dated sequences, interleaved with the estate: the CRM's answer to guide 70.

The problem in plain English: the system that watched the relationship

Covenant and team-move litigation is a contest of stories: the departing team says the clients followed them unprompted; the employer says the book was solicited and taken. Emails are drafted knowing they may be read; witness statements arrive after advice. The CRM was written before anyone was careful: the note that says "Jim wants us wherever I land", the ownership transferred to a junior the week before notice, the export at midnight, the pipeline that froze the day the plan formed. It is the contemporaneous, unguarded, timestamped account of the relationships in dispute: which is why the first disclosure request in these cases increasingly names the CRM before the mailbox.

The corollary is preservation urgency of a specific kind: CRM logs rotate on short, edition-dependent schedules, recycle bins empty on fixed windows, and the departing team often had admin rights until the door closed. The matter-open sequence: freeze the org's logs and bins, export the histories that are aging out, and only then argue about scope: because in this evidence class, the conduct layer's half-life is measured in weeks, and it is the conduct layer that wins the injunction.

Anatomy: objects, activities and the notes layer

OBJECT / LAYER	WHAT IT HOLDS · WHY IT MATTERS
Accounts & contacts	The customer organisations and their people: ownership fields, created dates, source fields, contact details: the book of business in record form, and the unit of the covenant fight.
Opportunities / deals	Pipeline records: value, stage, close dates, owners: their stage histories dating when deals moved, stalled or quietly regressed: the commercial chronology.
Activities	Logged calls, meetings, tasks and synced emails: the contact-frequency record proving who was actually working the relationship, and when working stopped.
Notes & free text	The candour layer: unguarded contemporaneous commentary: collected at full fidelity, never summarised away.
Ownership & teams	Assignment fields with their change histories: the reassignments that precede departures, and the shared-team visibility that answers "who could see this".
Custom objects & fields	Org-specific structures (commission calculators, renewal trackers): mapped via the schema per guide 71 §3, because the dispute's key field is often a custom one.
Attachments & files	Quotes, contracts and pitch decks stored against records: documents with CRM-side context (which deal, which stage) their file-share copies lack.

Histories and logs across the platforms

- **Field / property history:** per-record change tracking: field, old value, new value, user, timestamp: scope and retention edition-dependent (tracked-field limits, history windows, archive add-ons): the reassignments, stage changes and detail edits dated from here.
- **Login histories:** who signed in, when, from which IPs and clients: the presence layer that brackets after-hours activity and post-resignation access: retention windows short on lower tiers, exported early.
- **Administrative audit trails:** setup and configuration acts: permission changes, user deactivations, tracking switched on or off: the trail-integrity layer, read for mid-dispute changes per guide 72 §4's rule.
- **Event and activity monitoring:** the deep layer where licensed: report runs, exports, API calls, record views: edition-dependent and transformative when present: its availability is the first lattice question.
- **Integration logs:** connectors syncing email, calendars and marketing tools: their own histories dating what flowed between systems, and attributing connector-posted records past the service account per guide 72 §10's join.

Exports, reports and the exfiltration record

- **Export events as primary evidence:** logged data exports: who, when, which report or object, how many rows where captured: the direct record of the book leaving the building: correlated with resignation chronology, device artefacts (guide 41's USB and upload patterns) and the new employer's sudden reach.
- **Report creation and execution:** the custom report built to list "my accounts with contact details" days before an export is its own exhibit: report definitions and run logs collected together.
- **API and connector pulls:** bulk access via integrations and personal API tokens: visible in event logs where licensed, and in token issuance records regardless: the quiet route checked alongside the obvious one.
- **The absence case handled fairly:** thin logging editions cannot prove a negative: "no export logged" on an org without event monitoring means the question is open, not answered: the finding stated per this series' standing fairness rule.
- **Downstream correlation:** the exported file's afterlife: device presence, cloud uploads, attachment to personal email (guide 69's trail), reappearance in the competitor's material: the export log starts the chain; guides 41, 54 and 111 finish it.

Deletion, recycle bins and recovery

- **Recycle bins with windows:** deleted records sit provider-side for fixed periods (platform- and edition-dependent) before hard deletion: checked and exported immediately in any deletion-suspected matter: the guide 54 two-stage instinct, CRM edition.
- **Deletion events logged:** who deleted what, when: surviving the deletion itself in audit layers: the act datable even when content has aged out.
- **Field-level erasure:** details blanked rather than records deleted: caught by field history where tracked: the subtle variant that bin checks miss.
- **Backups and sandboxes:** org backups (native or third-party backup services), sandbox copies refreshed from production at datable moments: the point-in-time layer per guide 71 §8: enumerated in the census.
- **Mass-delete patterns:** bulk deletions clustering on notice dates: the conduct read: dated, counted and pleaded with the recycle-bin recoveries attached.

Collection routes and pipeline analysis

- **Native exports and APIs:** full-object exports, weekly export services, API acquisition for volume and fidelity: run per guide 71 §5 with query definitions, row counts and hashes: the reproducibility bundle regardless of route.
- **The slice for CRM:** objects, fields (including the custom ones the schema map surfaced), date ranges and: distinctively: the histories and logs as named components: a CRM collection without its field histories is the ledger without the trail.
- **Provider cooperation and org access:** collection runs on the client's own admin rights or ordered access to the opponent's org: with the agreed-queries model of guide 71 §7 adapting cleanly (agreed reports, run jointly, exports verified).
- **Pipeline chronology construction:** the disputed accounts rebuilt as dated sequences from records plus histories: creation, activity cadence, stage moves, reassignments, exports, silence: interleaved with mail and messaging per guide 70: the deliverable that turns admin data into narrative.
- **Presentation discipline:** per-account timelines for the load-bearing relationships, aggregate analyses (activity decay curves, reassignment clusters) for pattern, everything traced to the verified extract: guide 71 §13's reproducibility answer to "how do we show a tribunal a database".

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the org is the hub of an estate that extends well past it. CRM evidence also lives in: the histories and logs (in-platform but separately retained and separately dying); recycle bins and archive layers; org backups, sandbox copies and third-party backup services; synced email and calendar systems holding the activities' other copies (the meeting is in the CRM and in M365: guides 51-57); integration partners (marketing platforms, quoting tools, support desks) holding mirrored contacts and their own logs; exported files at rest across the device and cloud estate (guide 41, 54, 111 territory: the exfiltration afterlife); mobile CRM apps with device-side caches; and the correspondence estate discussing the records ("move my accounts to Dave before I hand my notice in"). When the org's layers have aged out, the mirrors, backups and counterpart systems rebuild the record: and the correspondence dates the intent the logs no longer can.

EVIDENCE	LIVE ORG	HISTORIES & LOGS	RECYCLE BIN / ARCHIVES	BACKUPS / SANDBOXES	INTEGRATED & MIRROR SYSTEMS	DELETED / RECOVERABLE
Relationship records	Y: current state	Change-dated	Deleted records, window-bound	Point-in-time states	Mirrored contacts & activities	Multi-layer, window-driven
Ownership / stage moves	Current values	Y: the core record	n/a	Before/after states	Sync-partner echoes	History retention decides
Export / access events	n/a	Y where licensed: rotation-bound	n/a	n/a	Connector logs	Exported early or lost
Notes & activities	Y	Edit histories where tracked	Deleted notes, window-bound	Y	Email/calendar originals	Counterpart systems rescue
Exported data at rest	n/a	The pull recorded	n/a	n/a	Devices, cloud, personal email	Guide 41/111's chain

Fallback strategy in one line: when the org's logs have rotated, date the conduct from backups, mirrors and the correspondence: and prove the book's contents from the synced systems that copied it all along.

Worked examples

EXAMPLE 1 · THE EXPORT AT 22:14

A recruitment firm's three-person perm desk resigned together on a Monday. The Salesforce event logs, frozen that afternoon, held the fortnight's story: a custom report ("All candidates + clients: KM desk") created the previous Tuesday; two export events the following evening at 22:14 and 22:31 totalling 11,400 rows, from the team leader's login, from a residential IP; and login histories showing her deputy browsing account records for firms he had never worked at 23:00 the same night. Device forensics (guide 41's patterns) found the CSVs' hashes on a personal USB; the new employer's mailshot three weeks later used contact details containing two seeded spelling errors unique to the claimant's data. The springboard injunction was granted on the logs' chronology, and the judgment quotes the 22:14 timestamp four times.

EXAMPLE 2 · THE REASSIGNMENTS THAT PRE-DATED THE PLAN

A covenant defendant claimed his clients had followed him spontaneously: no solicitation, no plan. HubSpot's property histories said otherwise: across the six weeks before his notice, ownership of nineteen key accounts had been reassigned from him to a junior colleague: each change logged to his own login: while the activity stream showed his contact cadence with those same accounts continuing unlogged-in-CRM but visible in the synced calendar (the integration mirror of §8). The pattern's meaning was the case: relationships moved off his book on paper while worked harder than ever in fact: pipeline camouflage, dated change by change. The tribunal called the reassignment schedule "a plan in administrative form" and the spontaneity defence did not survive it.

EXAMPLE 3 · THE RECYCLE BIN AND THE SANDBOX

A commission claimant alleged her biggest closed deal had been deleted from Dynamics and re-entered under a colleague's name after her dismissal, moving the commission. The live org showed only the colleague's version. The layers rebuilt hers: the recycle bin, exported inside its window, held her original opportunity record with its stage history intact to "Closed Won" under her ownership; the audit log dated its deletion to six days after her dismissal, under a sales-ops login; and a sandbox refreshed from production two months earlier held the pre-deletion state as independent corroboration. The re-entered version's created date, three days after the deletion, completed the sequence. The commission was awarded with uplift, and the sales-ops login's owner made an unhappy witness.

Common mistakes and technical limitations

Common mistakes

- **Logs left to rot:** the conduct layer's short half-life spent on correspondence: Example 1's evidence, lost by fortnight.
- **Records collected without histories:** the current state produced, the change record: the actual evidence: never requested.
- **The lattice unasked:** promises made before edition, tracking scope and retention are known: guide 66's lesson unlearned.
- **Recycle bins unchecked:** deletion conceded while the deleted records sat provider-side inside their window.
- **Departing admins unrevoked:** the suspects holding admin rights through the investigation's first week.
- **Notes summarised away:** the candour layer reduced to field extracts: the case's best sentences never collected.
- **Mirror systems forgotten:** synced calendars and email holding the activities' independent copies, unjoined: Example 2's rescue missed.
- **Absence overclaimed:** "no exports logged" pleaded from an org that never logged exports: the fairness rule broken, credibility spent.

Technical limitations

- **History scope is configured:** untracked fields have no history: what can be dated is an org-specific fact, established first.
- **Log retention is short and tiered:** weeks to months on common editions: the preservation race is genuinely urgent.
- **Event monitoring is a licence:** the deep conduct layer exists only where bought: its absence bounds the export question honestly.
- **Attribution ends at the login:** shared credentials and service accounts need guide 65 §7's ladder: the login's human is proved, not presumed.
- **Free text is unstructured:** notes need review, not just extraction: search strategies per guide 84 tuned for sales shorthand.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Platform, edition, tracking configuration and log retention: the lattice, in writing, today?
- Are the suspects' access rights revoked, the bins exported, and the aging logs frozen?
- Which accounts are the book in dispute: the slice the pipeline chronology will be built for?

Ask your opponent

- Please preserve and produce the CRM records for [accounts/custodians] including all field or property histories, login histories, audit trails and export or event logs for [period], stating the platform, edition and each log's retention setting.
- Please identify all data exports, report executions and API access by [custodians] in [period], and produce the export logs and report definitions.
- Please confirm whether any records have been deleted, merged or reassigned since [date], and produce the recycle bin contents and deletion logs.

Ask your eDiscovery / forensic provider

- What does this org's configuration let us date: and what is rotating away this month?
- What do the export and access logs show against the resignation chronology?
- What does the pipeline chronology for the disputed accounts look like once the mirrors are joined?

SUGGESTED WORDING · CRM LIMB FOR THE PRESERVATION LETTER

"Your client must immediately preserve all CRM data relating to the issues, including: (a) all account, contact, opportunity, activity and note records for the customers and custodians in issue, which must not be edited, deleted, merged or reassigned other than in the ordinary course; (b) all field, property and stage histories, audit trails, login histories and event, export and report logs, whose rotation or purge must be suspended so far as within your client's control, and which should be exported forthwith where retention limits cannot be extended; (c) all recycle bin or deleted-record contents, which must be exported before any hard-deletion window expires; and (d) all backups, sandbox copies and third-party backup service data for the CRM. Please confirm within [3] days, stating the platform and edition, the field-history configuration, and the retention period applicable to each log."

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

The CRM checklist

- ☐ Lattice audit day one: platform, edition, tracking scope, log retention
- ☐ Aging logs exported immediately; bins captured inside their windows
- ☐ Suspect access revoked; admin acts since notice reviewed
- ☐ Collection includes histories and logs as named components
- ☐ Notes and activities collected at full fidelity
- ☐ Export, report and API events mapped against the departure chronology
- ☐ Mirror systems joined: synced mail, calendars, integrations
- ☐ Deletions and reassignments dated from histories and audit layers
- ☐ Pipeline chronologies built for the disputed book, interleaved per guide 70
- ☐ Absence findings bounded by the org's actual logging capability

Red flags

- Exports and custom reports clustering before resignation: Example 1's evening.
- Ownership reassignments preceding notice: Example 2's nineteen accounts.
- Deletions and re-entries moving value between owners: Example 3's commission.
- Activity cadence dying on the book while employment continues.
- Admin acts: tracking off, users repermissioned: mid-dispute.
- Contact details edited to personal addresses before departure.
- Productions of current state that resist the histories.

When to involve a digital forensic expert

At preservation, where the log half-lives set the clock and the bins have windows; at collection, where API acquisition, history capture and the reproducibility bundle are guide 71's craft on CRM structures; at analysis, where export chronologies, reassignment patterns and pipeline reconstructions are built and joined to the device and cloud afterlife (Examples 1-3's machinery, guides 41 and 111's chains); and at reporting, where conduct findings are stated to their evidenced rung under CPR Part 35. Through **e-discovery.uk**, CRM extracts, histories and the correspondence estate share one review: the book of business beside the messages about taking it.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can we see if a departing employee downloaded our client list?

Often, and quickly: export and report logs (where the edition keeps them) record the pull directly; report definitions show what was built to be pulled; login histories bracket the sessions; and the file's afterlife runs guide 41's device-and-cloud chain. The honest caveat is §5's: orgs without event monitoring may not log exports, in which case the answer comes from the periphery: device artefacts, personal-email trails, and the competitor's suspicious reach: rather than the platform.

Are CRM notes really disclosable? Our sales team wrote them assuming privacy.

Fully: they are business records within the party's control, and their unguarded tone is precisely their evidential value: no privacy expectation attaches to a company system's contents in disclosure. The practice point runs both ways: collect the opponent's notes at full fidelity, and advise your own clients: prospectively: that the CRM is a disclosure source, because "wants us wherever I land" reads very differently in a bundle than it did in a pipeline review.

The opponent produced a spreadsheet of "the relevant CRM records". Sufficient?

Almost never: it is guide 71's report-not-record problem: a current-state extract without histories, logs or the dictionary, shaped by unstated filters. The §11 questions ask for the platform's own layers: field histories, login and export logs, bin contents, the edition and retention facts: and a production that resists the history layer while offering the story is answering the wrong question, which is itself worth pointing out to the court.

Our client's org only keeps login history for a few months and it has already rotated. Now what?

Work the map of §8: backups and sandbox refreshes preserve point-in-time states; integration mirrors (synced calendars, email, marketing platforms) hold the activities' independent copies; device-side artefacts date sessions the platform forgot; and the correspondence estate dates intent regardless. Rotation costs precision, not the case: and prospectively, the lesson is the standing one: freeze and export the short-lived layers in the first week, every time.

The suspect was an admin. Could they have covered their tracks?

Partially at best: admins can delete records and sometimes adjust configurations, but administrative acts land in setup audit trails, deletions transit recycle bins with windows, histories resist retrospective editing, backups and sandboxes hold prior states, and mirror systems never answered to them at all: Example 3's rebuild ran through exactly these layers. The examination checks trail integrity first (guide 72 §4's rule), and an admin's clean-up attempt usually adds a conduct chapter rather than removing one.

Can pipeline data prove solicitation, or only opportunity?

By itself it proves patterns: cadence, moves, timing: which is opportunity and preparation; solicitation usually needs the join: the CRM chronology interleaved with the messages (guide 70) where the approach itself lives, the counterpart layer (the client's side of the story, per guides 63-65), and the aftermath data (deals resurfacing at the competitor). The CRM supplies the skeleton and the dates; the estate supplies the words: which is why the pipeline chronology is built as an interleaved deliverable, not a standalone chart.

§ 1 4 · REFERENCE

Glossary

Activity stream

Logged calls, meetings, tasks and synced mail; the cadence record.

Event monitoring

The licensed deep-log layer: exports, views, API calls.

Export event

The logged act of pulling data out; the exfiltration record's core.

Field history

Per-record change tracking: field, old/new value, user, time.

Object model

The CRM's schema: accounts, contacts, opportunities, custom objects.

Ownership reassignment

The logged transfer of a record's owner; Example 2's pattern unit.

Pipeline chronology

Disputed relationships rebuilt as dated sequences; the deliverable.

Recycle bin (CRM)

The provider-side deleted-record store with its hard-delete window.

Sandbox

A copy org refreshed from production at datable moments; a point-in-time layer.

Stage history

An opportunity's dated movement through the pipeline.

Sources and authoritative references

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

- cflab.uk, digital forensics services (CRM forensics, export-log analysis, pipeline chronologies, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation, Phase 03 · Collection and Phase 04 · Processing (log-halflife preservation; CRM extracts into review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Platform documentation: Salesforce field history and event monitoring: help.salesforce.com, [field history](https://help.salesforce.com/field-history) · HubSpot property history: knowledge.hubspot.com · Microsoft Dynamics auditing: [learn.microsoft.com](https://learn.microsoft.com/auditing), [auditing](https://learn.microsoft.com/auditing)
- PD 57AD, CPR Part 31 and CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad) · justice.gov.uk, [Part 35](https://justice.gov.uk/part-35)
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, [27037](https://iso.org/27037)

DISCLAIMER

This publication provides general information about CRM evidence as at August 2026. Platform capabilities, history scope, log retention and recycle-bin windows vary by product, edition and configuration and change on vendors' schedules; verify the current position for the org in the matter at hand. 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

CRM matters at the laboratory start with the clock: the lattice audit, the immediate export of aging logs, and the bin captures inside their windows: because Example 1's 22:14 exists only for the party who froze it in week one. Collection runs guide 71's discipline on CRM structures: slices with their histories, API acquisition with the reproducibility bundle, notes at full fidelity: and analysis delivers the export chronologies, reassignment patterns and pipeline reconstructions of Examples 1-3, joined to the device and cloud afterlife per guides 41 and 111 and interleaved with the correspondence per guide 70. Absence findings are bounded by the org's real capability, and everything reports under CPR Part 35 to its evidenced rung. Through **e-discovery.uk**, the book of business and the estate around it share one review. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a team resigned this week and their org's logs rotate monthly, the freeze is this afternoon's instruction.



I N S T R U C T T H E L A B

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