COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

SaaS Platforms as Undiscovered Repositories

Finding, Preserving and Collecting the Business Records That Live Inside Applications

Modern businesses run on applications: a CRM holding every customer interaction, a project tool holding the record of who decided what and when, an HR system holding the disciplinary file, a support desk holding the complaints, a finance platform holding the transactions, a messaging tool holding the conversations that used to be emails. Each is a repository of exactly the material litigation wants, and almost none of it appears in a disclosure exercise built around email and shared drives. These are the undiscovered repositories: subscribed to by departments, administered outside IT, holding structured records and comment threads and audit trails that answer the case directly, and routinely missed because nobody asked the custodian what applications they actually work in. This guide sets out for UK lawyers how to find the SaaS platforms a business uses, what each kind holds and records, how to preserve and collect from applications that were never designed for disclosure, and how to deploy their contents: because the record that decides the case increasingly lives inside an app, not a file.

⏱ Estimated reading time: 25 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. Its eDiscovery arm, **e-discovery.uk**, routinely finds and collects from the SaaS platforms disclosure exercises miss: CRM, project, HR, support, finance and collaboration applications: mapping them from endpoints, network and expense records, preserving them against their own retention, and collecting their structured records and audit trails defensibly for CPR Part 35 and PD 57AD disclosure.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | SAAS DISCOVERY & COLLECTION | API & AUDIT-TRAIL COLLECTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: BUSINESS RECORDS INCREASINGLY LIVE INSIDE SAAS APPLICATIONS THAT NO EMAIL-AND-DRIVES DISCLOSURE EXERCISE WILL FIND: MAP THE ESTATE FROM ENDPOINTS, NETWORK AND EXPENSES; PRESERVE EACH PLATFORM AGAINST ITS OWN RETENTION; AND COLLECT ITS STRUCTURED RECORDS AND AUDIT TRAILS, WHICH FREQUENTLY ANSWER THE CASE MORE DIRECTLY THAN ANY DOCUMENT

Finding them (§3): the SaaS estate is mapped not from the IT asset register alone (which misses departmental and shadow subscriptions) but from custodian interviews that ask what applications people work in, endpoint examination of installed apps and browser histories, single-sign-on and identity-provider logs listing connected applications, network and CASB logs, and expense and card records: the platforms found before they can be missed. **What they hold (§4):** CRM systems (customer interactions, notes, the sales narrative), project and task tools (decisions, assignments, timelines), HR systems (the personnel and disciplinary record), support desks (complaints and their handling), finance and ERP platforms (transactions and approvals, guide 98), and messaging and collaboration tools (the conversations that replaced email): each a repository of case-relevant material. **The structured record (§5):** SaaS data is not documents but records: fields with values, change histories showing who altered what and when, comment threads, and audit trails: the audit trail in particular often recording exactly the who-did-what-when the case turns on, more reliably than any narrative. **Preservation and collection (§6):** the platform's own hold and export features where they exist, API collection for completeness and structure, and the format problem: how to render a database of linked records into something reviewable and disclosable without losing the structure that gives it meaning. **Deployment (§7):** the PD 57AD and CPR 31 duty reaching these sources, proportionality shaping their collection, and the recurring value of the audit trail as the neutral record that settles disputes the documents leave open.

- **The record is in the app:** CRM, project, HR, support and finance platforms hold what the case wants, and email disclosure misses it.
- **Map before you collect:** endpoints, SSO logs, network and expenses find the platforms interviews alone do not.
- **Records, not documents:** fields, histories and comments need collecting as structure, not flattened to paper.
- **The audit trail is the prize:** the platform's own who-did-what-when often answers the case directly.
- **The duty reaches them:** SaaS platforms are disclosable sources, and missing them is a disclosure failure.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the record moved into the app

A decade ago the record of a business was its email and its files. Today much of it has moved into applications. The sales team does not email about a customer; they log the call in the CRM. The project is not run over email; it is run in a task tool where each decision is a comment on a card. The complaint is not a letter; it is a ticket in the support desk. The disciplinary process is not a folder; it is a workflow in the HR system. These applications hold the record precisely because they replaced the email and the folder, and a disclosure exercise that collects email and drives and stops has collected the shadow of the business, not the business.

The difficulty is compounded because these platforms are invisible to the traditional map. They are subscribed to by departments on cards, administered by a team lead rather than IT, and never appear on the asset register. The custodian who "does not have many relevant documents" spends their whole day in three applications that hold the case. So the work has two parts that this guide takes in turn: first finding the platforms, which is a discovery exercise in itself; and then collecting from them, which means treating structured records, change histories and audit trails as the evidence they are, rather than forcing them into the document-shaped hole disclosure was built for.

§ 0 3 · FINDING THE PLATFORMS

Finding the platforms: mapping the SaaS estate a business actually uses

- **Custodian interviews, asked correctly:** not "what documents do you have?" but "what applications do you work in, all day, and where do you record what you do?": the question that surfaces the CRM, the project tool and the messaging app the document question misses (guide 101's lesson, generalised).
- **Single sign-on and identity provider:** the SSO or identity provider (Entra, Okta, Google) lists the applications users authenticate to: the single most efficient map of the sanctioned SaaS estate, exported at the outset.
- **Endpoint examination:** installed applications, browser histories and bookmarks, saved credentials and desktop clients on custodians' machines (guides 111-112's method): the platforms people actually use, including the shadow ones SSO does not cover.
- **Network, CASB and DNS logs:** web-proxy, cloud-access-security-broker and DNS records of connections to SaaS domains: the estate observed from the network, catching sanctioned and unsanctioned alike (guide 111 §5).
- **Expense and procurement records:** card statements, expense claims and procurement records for SaaS subscriptions: the departmental and shadow platforms paid for outside IT, found where the money went (guide 112 Example 2's method): triangulated across all five sources into a defensible estate map.

§ 0 4 · WHAT EACH KIND HOLDS

What each kind holds: CRM, project, HR, support, finance and messaging

- **CRM and sales platforms:** customer and contact records, interaction and call logs, notes, opportunity and pipeline history, emails logged against records, and the change history of each: the sales narrative and the customer relationship, central to commercial, employment (the departing salesperson) and misrepresentation disputes.
- **Project, task and knowledge tools:** cards, issues and tasks with their assignments, statuses, due dates, comment threads and full change history; wikis and knowledge bases with page histories: the record of who decided what, when, and who did the work: often the clearest account of a project's real chronology (guide 96).
- **HR and people systems:** personnel records, performance and disciplinary workflows, absence and leave, compensation, and the audit trail of changes: the employment case's documentary spine, with UK GDPR special-category sensitivity (guide 97's data-protection frame) shaping its handling.
- **Support and service desks:** tickets, their conversations, resolutions and satisfaction records, and the timeline of each: the complaint record for consumer, product-liability and service disputes, and the pattern evidence across many tickets.
- **Finance, ERP and messaging:** finance and ERP transaction and approval records with their audit trails (guide 98's fraud territory); and messaging and collaboration platforms (Slack, Teams-adjacent tools) holding the conversations that replaced email (guides 63-66, 101): each a first-class repository, not an afterthought.

§ 0 5 · THE STRUCTURED RECORD

The structured record: fields, history, comments and audit trails

- **Records, not documents:** a SaaS entity is a set of fields with values (a customer record, a ticket, a task), linked to other records and to people: collecting it means capturing the fields, the links and the context, not printing a screen that loses them.
- **Change history:** most platforms record the history of each record's changes: who altered which field, from what value to what, and when: the equivalent of a version ladder (guide 102) for structured data, and frequently the evidence that a value was changed after the fact.
- **Comment and activity threads:** the discussion attached to a record (the notes on a CRM contact, the comments on a task, the internal notes on a ticket): the narrative around the structured facts, and often where the candid statements live.
- **The audit trail:** the platform's own log of user actions: logins, record views, edits, exports, permission changes: the neutral who-did-what-when record (guide 105) that settles disputes the substantive records leave open, and that proves access, alteration and deletion within the platform.
- **Deletion and retention within the platform:** soft-deleted records in the platform's recycle store, retention and archival settings, and the audit trail's record of deletions (guide 106): what was removed from the app, by whom, and whether it is recoverable: established per platform.

§ 0 6 · PRESERVATION AND COLLECTION

Preservation and collection: holds, exports, APIs and the format problem

- **Preservation within the platform:** legal-hold and retention-extension features where the platform offers them; suspension of auto-deletion and archival policies; and, where no hold feature exists, the practical preservation of exporting the relevant records at once, per guide 105 §6's retention discipline.
- **Native export and reporting:** the platform's own export and reporting tools, capturing records, histories and audit trails in the platform's format: the first-line collection method, with its completeness and any field omissions documented.
- **API collection:** where native export is incomplete or unstructured, the platform's API enumerates records, change histories, comments and audit entries for targeted, documented, reproducible collection (guide 71): the method of choice where structure and completeness matter, run by an examiner who records the queries and hashes the results.
- **The format problem:** a database of linked records does not become a reviewable document set by flattening: the collection must preserve the structure (relationships, field labels, history) and render it into a review platform in a form that keeps meaning: load files, structured exports, or a hosted copy, chosen so that the record's context survives disclosure (guide 84's processing discipline, for structured data).
- **Proportionality and scope:** SaaS platforms can hold vast structured data; collection is scoped by custodian, record type, date and relevance under the DRD (guide 94), with targeted API queries rather than wholesale extraction where proportionality demands: the collection defensible in scope as well as method.

§ 0 7 · DEPLOYMENT

Deployment: disclosure obligations, proportionality and the audit trail's power

- **The duty reaches SaaS:** PD 57AD and CPR 31 make no exception for data that lives in an application: relevant records in a CRM, project tool or HR system are disclosable, and a Disclosure Review Document that omits the sources the business actually uses is incomplete (guide 94): the known-sources discipline applied honestly.
- **Proportionality both ways:** the volume and structure of SaaS data invite proportionality argument: targeted collection of relevant record types and date ranges, not wholesale extraction: with the same proportionality protecting a party from a disproportionate demand and requiring it to reach the sources that matter (guide 20's balance).
- **The audit trail as neutral evidence:** the platform's audit trail: who created, viewed, edited, exported or deleted a record, and when: as the objective record that resolves factual disputes the substantive data leaves open (guides 105-106): frequently the single most valuable artefact a SaaS platform yields.
- **Change history as authenticity evidence:** the record of a field's alteration after a key date (guide 109's backdating tests, for structured data): the CRM note added after the dispute, the HR record amended before disclosure: exposed by the history the editor forgot the platform kept.
- **The undisclosed-source problem:** where an opponent's disclosure omits a SaaS platform the estate map shows they use, the specific application for its contents (guide 95's missing-evidence method), with the platform's audit trail as the proof it holds relevant material.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a SaaS platform is a repository whose contents are also reflected, partially, across the estate, and the examination reads the platform and its reflections together. The platform itself holds the records, histories, comments and audit trail. The integration layer reflects it: the CRM's emails also in the mailbox, the project tool's notifications also in Slack, the HR system's letters also in the document store, the finance platform's exports also in spreadsheets: so a record deleted from the app may survive in what it fed. The endpoint holds the local traces: the browser history proving use, the cached data, the downloaded exports. The identity and network layers prove who used the platform and when. The provider holds the server-side record reachable by process where the account is adverse. And the counterparties: the customer in the CRM, the contractor in the project tool: hold their side. When the platform record is denied, deleted or unmapped, the integration layer's reflections, the endpoint's traces and the network's logs prove the platform was used and often what it held; and the audit trail, which users rarely think to alter, proves what happened inside.

QUESTION	THE PLATFORM ITSELF	INTEGRATION REFLECTIONS	ENDPOINT TRACES	IDENTITY + NETWORK	PROVIDER RECORDS	COUNTERPARTIES
Does the business use it	Y: the account	Notifications in mail/chat	Y: installed app, browser	Y: SSO + proxy logs	Account existence	They interacted through it
What does it hold	Y: records + comments	Emailed and exported copies	Downloaded exports	n/a	Server-side data	Their copy of the interaction
Who did what, when	Y: audit trail + history	Notification timestamps	Local access times	Y: login records	Y: server-side audit	n/a
Was a record changed / deleted	Y: change history, recycle	The pre-change copy in mail	Cached prior state	n/a	Server-side prior state	What they were originally told
Who accessed it	Y: audit trail	n/a	Endpoint session	Y: authenticated identity	Access records	n/a

Fallback strategy in one line: when a SaaS platform is unmapped, the SSO, network and expense records find it; when its records are denied or deleted, the integration reflections and the audit trail hold what happened; and the counterparties hold their side of every interaction.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE CUSTODIAN WITH NO DOCUMENTS AND A CRM FULL OF THEM

In a claim over a lost account, the key salesperson's email disclosure was thin, and he maintained he had "hardly any documents" about the customer. The §3 estate map, built from the SSO application list and his laptop's browser history, put him in the CRM for most of every working day. The §5-§6 collection of his CRM records changed the case: 400 logged interactions with the customer, a comment thread in which he recorded the customer's growing dissatisfaction months before the loss, and: decisively: a change history showing a key note about a service failure edited three weeks after the claim was intimated, softening its original wording. The §7 audit trail dated the edit and named his account; guide 109's backdating logic, applied to a structured field, did the rest. The salesperson had no documents because his record was not in documents; it was in the app, and the app remembered the edit he had not known it kept.

EXAMPLE 2 · THE PROJECT TOOL THAT HELD THE REAL CHRONOLOGY

A construction dispute turned on when a design defect had been identified. The parties' formal correspondence was equivocal, and each side's witnesses recalled the sequence differently. The answer was in a project-management platform the contractor used internally and had not included in disclosure: found through the §3 network logs and a subcontractor's reference to it. The §5 collection of the relevant cards and their comment histories fixed the chronology precisely: a task raising the defect, dated and assigned; a comment thread discussing it weeks before the date the contractor's case asserted; and the change history showing the task's status and dates as they had actually moved. The §7 audit trail confirmed the comments were contemporaneous, not added later. The project tool, never designed for litigation, held the neutral, timestamped record the correspondence and the witnesses could not supply: which is why the project platform is now on the map in every construction matter the firm runs.

EXAMPLE 3 · THE PROPORTIONATE COLLECTION THAT AVOIDED THE WHOLESALE ONE

An employer facing a discrimination claim was asked to disclose "all HR system data", a demand that, taken literally, meant extracting the entire personnel database. The §6 proportionality analysis, agreed through the DRD, narrowed it sensibly: the claimant's own records in full (including change history and audit trail); the disciplinary and performance records of the named comparators for the relevant period; and the audit trail of who accessed the claimant's record and when: targeted API queries, not a wholesale export, capturing exactly the relevant structured data with its history and context intact. The audit trail proved a manager had accessed the claimant's record shortly before a key decision, corroborating the claim's timeline; the change history showed a performance rating amended after the grievance. Proportionate, targeted SaaS collection produced the decisive evidence that a wholesale extraction would have buried and a document-only disclosure would have missed entirely.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The wrong custodian question:** "what documents do you have?" instead of "what applications do you work in?": Example 1's salesperson with no documents and a full CRM.
- **The estate mapped from IT only:** departmental and shadow SaaS missed because it was never on the asset register: Example 2's project tool.
- **SaaS omitted from the DRD:** the known-sources duty (guide 94) breached by a disclosure built around email and drives alone.
- **Records flattened to screenshots:** the structure, history and links lost by printing screens: §5's records reduced to pictures.
- **Audit trail and history ignored:** the platform's most valuable evidence: the who-did-what-when and the change record: never collected.
- **Wholesale extraction by default:** Example 3's literal demand: proportionality abandoned, review buried, cost multiplied.
- **Retention missed:** the platform's records or audit trail aging out under its own policy during deliberation.
- **Special-category data mishandled:** HR and other sensitive SaaS data collected without the UK GDPR care its content demands.

Technical limitations

- **Export capability varies wildly:** some platforms export richly, some barely, some only through the API: the collection method is platform-specific and its completeness stated.
- **Structure resists flattening:** linked, relational records lose meaning when forced into document form: the format problem (§6) is real and shapes what review can do.
- **Audit-trail depth differs:** some platforms log richly and retain long; some log little; some make the audit trail available only to administrators or higher tiers: established per platform.
- **Retention is the vendor's:** what survives depends on the platform's and the subscription's retention, not the litigant's wishes: preserved early or lost.
- **Integrations are partial mirrors:** the §8 reflections corroborate but rarely reproduce the full structured record: useful for proving use and catching deletion, not a substitute for collecting the source.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What applications does each relevant person work in all day, and where is the record of their work actually kept: beyond email and files?
- What does your SSO or identity provider list, and what SaaS appears in expense and card records outside IT's estate?
- What are the retention and audit-trail settings on each relevant platform, and can holds and exports be run now?

Ask your opponent

- Please identify all software-as-a-service and cloud applications used in connection with [the matter], including customer-relationship, project, HR, support, finance and messaging platforms, whether administered by IT or otherwise, and confirm whether each was placed under hold and reviewed for disclosable material.
- Please disclose the relevant records from [platform], including the records themselves, their change histories, associated comment and activity threads, and the audit-trail entries showing creation, access, editing, export and deletion, for [custodians / record types] during [period].
- Please confirm the retention and audit-trail configuration of each such platform and the date on which relevant data was preserved.

Ask your eDiscovery / forensic provider

- What does the estate map show once SSO, endpoints, network and expenses are triangulated?
- For each platform, what does native export capture, and where must the API fill the gap to preserve structure and history?
- What does the audit trail and change history show, and has it been preserved before its retention expires?

SUGGESTED WORDING · SAAS-SOURCES PARAGRAPH FOR THE DRD / DISCLOSURE PROTOCOL

> "The parties acknowledge that relevant material may be held within software-as-a-service and cloud applications (including customer-relationship, project and task, HR, support, finance and messaging platforms), whether or not administered by the party's IT function. Each party shall identify such applications by reference to identity-provider and single-sign-on records, endpoint examination, network and expense records, and custodian interviews directed to the applications in which work is performed; shall place relevant applications under hold and suspend applicable retention and deletion; and shall collect relevant material as structured data, preserving records, their change histories, associated comments and the platform audit trail, by native export or API as appropriate, with scope agreed by custodian, record type and date range on proportionality grounds. Collection shall preserve the relationships and context of the structured data, and the method and completeness of each platform's collection shall be documented."

§ 12 · QUICK CONTROL

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

The SaaS-discovery checklist

- ☐ SaaS estate mapped from SSO, endpoints, network, expenses and interviews
- ☐ Custodians asked what applications they work in, not just what documents they hold
- ☐ Relevant platforms placed under hold; retention and deletion suspended
- ☐ Per-platform export capability and audit-trail depth established
- ☐ Records collected with fields, links, history and comments intact
- ☐ Audit trails and change histories preserved and collected
- ☐ Structure preserved into review; not flattened to screenshots
- ☐ Scope agreed proportionately by custodian, record type and date
- ☐ Special-category and personal data handled per UK GDPR
- ☐ Collection documented, hashed and reproducible per guide 71

Red flags

- Custodians who "have few documents" but live in applications all day: Example 1.
- SaaS platforms in the network and expense records but not in disclosure: Example 2.
- Change histories showing edits to key records after the dispute arose.
- Audit trails showing access or export around key dates.
- Wholesale-extraction demands ignoring proportionality: Example 3's literal ask.
- Platforms with retention windows approaching expiry.
- HR and finance platforms omitted from the source map.

When to involve a digital forensic expert

At the mapping stage, where the estate is triangulated from SSO, endpoints, network and expenses so the platforms that hold the case are found before they are missed (Examples 1-2); at preservation, before each platform's retention deletes its records and audit trail; at collection, where structure, history and audit trail are captured by export or API and rendered into review without losing meaning (§6's format problem); at scoping, where proportionality is applied so the relevant records are collected without wholesale extraction (Example 3); and at deployment, where the audit trail and change history are read for the neutral who-did-what-when the documents leave open, under CPR Part 35 and PD 57AD. Through **e-discovery.uk**, SaaS discovery and collection are a standard part of scoping: because the record that decides the case increasingly lives inside an app that no email disclosure will ever open.

§ 13 · COMMON QUESTIONS

Frequently asked questions

A key witness says they have almost no relevant documents. Is that the end of it?

Often it is the beginning: the question "what documents do you have?" misses the applications where modern work is recorded (§2). Ask what platforms they work in all day (§3): the CRM, the project tool, the messaging app: and the record is usually there in quantity (Example 1's 400 interactions), with a change history and audit trail the witness never thought about.

How do we even find out what SaaS platforms a business uses?

By triangulation (§3): the identity provider or SSO lists sanctioned applications, endpoint examination finds installed and browser-used ones, network and CASB logs catch the rest, and expense and card records reveal the departmental and shadow subscriptions IT never sees (Example 2). No single source is complete; together they map the estate the asset register does not.

Can data in a CRM or project tool really be collected for disclosure?

Yes, as structured data (§5-§6): through the platform's export or its API, preserving the records, their change histories, comment threads and audit trails, and rendering them into review in a form that keeps the structure and context (§6's format problem). Flattening them to screenshots loses the very history and links that make them valuable; proper collection keeps them.

What makes the audit trail so useful?

It is the platform's own neutral record of who did what and when: created, viewed, edited, exported, deleted (§5, §7): unaffected by anyone's later account of events, and frequently answering the factual dispute the substantive records leave open (Example 3's manager access, Example 1's edit). Users rarely think to alter it, which is exactly why it is often the most reliable evidence a SaaS platform holds.

The other side wants "all our HR system data". Do we have to extract everything?

No: proportionality applies to SaaS as to anything (§6-§7), and the sensible answer is targeted API collection: the relevant individuals' records, the relevant period, the change history and audit trail: agreed through the DRD (Example 3). Wholesale extraction is usually disproportionate, buries the relevant material, and mishandles special-category data; targeted collection produces the decisive records without it.

What if a record was changed or deleted in the app?

The platform usually remembers: change histories record who altered which field and when (guide 109's backdating logic for structured data, Example 1's softened note), and soft-deleted records sit in the platform's recycle store with the deletion logged in the audit trail (guide 106). What was removed from the app, by whom and whether it is recoverable, is established per platform, and the integration reflections (§8) may hold the pre-change copy besides.

§ 14 · REFERENCE

Glossary

Audit trail
A platform's log of user actions: access, edit, export, delete.

Change history
The record of a record's field alterations over time.

CRM
Customer-relationship-management platform holding the sales record.

Estate map
The triangulated inventory of applications a business uses.

Integration reflection
A partial copy of SaaS data in a connected system.

Native export
A platform's own tool for extracting its data.

Shadow IT
Applications used outside the IT function's control.

SSO
Single sign-on; a map of the sanctioned application estate.

Structured record
Data held as fields and relationships, not documents.

Undiscovered repository
A case-relevant platform a disclosure exercise misses.

Sources and authoritative references

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

- e-discovery.uk, EDRM Phase 02 · Identification and Phase 04 · Collection (SaaS estate mapping, API and structured-data collection as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- cflab.uk, digital forensics services (endpoint and audit-trail examination, structured-data analysis, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- PD 57AD (Disclosure Review Document and known adverse documents): justice.gov.uk, PD 57AD · CPR Part 31 and PD 31B (disclosure of electronic documents): justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- ICO, UK GDPR guidance and special category data: ico.org.uk · Sedona Conference, commentary on databases and structured data (persuasive, non-binding): thesedonaconference.org
- ISO/IEC 27037 (identification, collection and preservation): iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

SaaS discovery at **e-discovery.uk** begins where disclosure usually stops: with the question of what applications the business actually works in, answered by triangulating SSO, endpoints, network and expense records into an estate map that finds the CRM, the project tool and the HR system the asset register missed (Examples 1-2). Relevant platforms are placed under hold before their retention deletes the records and audit trails; collection captures the structured records, change histories, comments and audit trails by native export or API, preserving the relationships and context that give the data meaning rather than flattening it to screenshots; scope is agreed proportionately through the DRD so the decisive records are reached without wholesale extraction (Example 3); and the audit trail and change history are read for the neutral who-did-what-when that resolves what the documents leave open. Reports and disclosure run under CPR Part 35 and PD 57AD. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a matter is being scoped now, the first question is the one email disclosure never asks: what does the business actually run on?

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