



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

ERP Evidence: SAP, Oracle and Enterprise Systems

Purchase-to-Pay, Change Documents and the System of Record at Enterprise Scale

When the dispute involves a large corporate, the facts live in the ERP: SAP, Oracle, Dynamics 365 and their kind run procurement, sales, inventory, finance and payroll as one integrated machine, and every disputed transaction: the order that was changed, the invoice approved against policy, the goods receipt that never matched a delivery: passed through it leaving structured traces at every step. ERP evidence is guide 71's method at its largest scale and richest logging: document flows linking order to receipt to invoice to payment, change documents recording every field edit with user and timestamp, workflow and approval trails showing who authorised what, and segregation-of-duties data showing who could have. This guide equips UK lawyers for enterprise-system disputes: the module and document-flow anatomy, change documents and audit logs in the SAP and Oracle worlds, approval workflows and authorisation evidence in fraud and procurement cases, the scoping and extraction disciplines that keep terabyte systems proportionate, and the joint expert model these systems demand.

© 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. Enterprise-system evidence features across its procurement-fraud, warranty and supply-chain casework: change-document and audit-log analysis in SAP and Oracle environments, document-flow reconstruction from order to payment, authorisation and workflow evidence, and the scoped extraction protocols that make terabyte systems litigable. Its eDiscovery arm, **e-discovery.uk**, hosts ERP extracts beside the correspondence estate.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ERP & ENTERPRISE-SYSTEM FORENSICS

CHANGE-DOCUMENT & WORKFLOW 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 machine that runs the company
03	Anatomy: modules, documents and the flow
04	Change documents, audit logs and the history layer
05	Approvals, workflows and authorisation evidence
06	Scoping and extraction at enterprise scale
07	Patterns: procurement fraud, warranty and supply-chain disputes
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 ERP LINKS EVERY DISPUTED TRANSACTION INTO A DOCUMENTED FLOW WITH A CHANGE HISTORY: FOLLOW THE FLOW, READ THE CHANGES, TEST THE APPROVALS

Enterprise systems reward litigation with three structures smaller platforms only gesture at. **The document flow:** ERP transactions are chains: purchase requisition to purchase order to goods receipt to invoice receipt to payment; sales order to delivery to billing to receivable: each link a numbered document referencing its predecessors, so the disputed invoice arrives with its whole ancestry attached: and gaps in the chain (payments without receipts, receipts without orders, the three-way match that never matched) are findings in themselves: the anatomy §3 maps and §7's fraud patterns exploit. **The change history:** the SAP world's change documents and the Oracle world's audit tables record field-level edits: object, field, old value, new value, user, date, time: across master data (vendor bank details, credit limits, price conditions) and transactions alike: the guide 72 two-date discipline delivered at enterprise depth, so the vendor whose bank account changed the week before a payment run, and changed back the week after, is a query away from exposure: with security audit logs, login records and (configuration-permitting) table-access logging behind it. **The authorisation layer:** role and profile data recording who could do what, workflow and approval records showing who did approve what, and segregation-of-duties analysis joining them: the evidence stratum that converts "the fraud happened" into "it required these permissions, held by these users, exercised in these logged approvals": decisive in procurement fraud, payment diversion and internal-control disputes. The practice realities scale accordingly. **Scoping is everything:** nobody images an ERP: the guide 71 slice discipline operates on company codes, document types, vendors, date ranges and the specific tables the issues touch, with the client's own basis and functional teams (or the laboratory's platform specialists) in the mapping conversation, and extraction by standard reports, table extracts and documented queries with the reproducibility bundle throughout. **Hosting eras matter:** on-premise estates offer database-level depth; cloud-era deployments (S/4HANA Cloud, Oracle Fusion Cloud) trade that for provider-mediated exports and standardised audit facilities: the lattice question, asked of a bigger lattice. And **the expert model is joint by necessity:** platform specialists who speak the system's transaction codes, digital examiners who own preservation, integrity and the change-layer analysis, and forensic accountants on meaning and quantum: guide 72 §7's division, at scale, under one chronology.

- **Follow the flow:** every disputed transaction has an ancestry: collected whole, with its gaps read as findings.
- **Change documents are the case:** field-level history with users and times: the vendor-bank-detail edit is the classic exhibit.
- **Approvals are evidence, not process:** workflow records plus authorisation data answer who approved and who could have.
- **Scope by company code, document type and table:** the slice discipline keeps terabytes proportionate.
- **Three experts, one chronology:** platform, forensic and accounting expertise divided per guide 72 §7 and joined per guide 70.

The problem in plain English: the machine that runs the company

An ERP is the company's administrative nervous system: goods do not ship, invoices do not pay and journals do not post except through it. This totality is the litigator's gift: unlike the email estate, where relevant traffic hides among noise, the ERP's records are structured, linked and complete by design: if the transaction happened, it is in there, numbered, and connected to everything it touched. The same totality is the trap: the system is vast, its table names are hostile, its transaction codes are a language, and a mis-scoped request returns either nothing usable or a refusal armed with genuine burden arguments.

The resolution is fluency plus discipline: enough anatomy (§3) to name what the case needs in the system's own terms: the document types, the flows, the change-document objects: and the guide 71 disciplines to demand it verifiably: slices, dictionaries, reproducibility bundles, agreed queries. ERP disputes are won by the party whose requests read like they were drafted by someone who has seen the system: because such requests are cheap to comply with, expensive to refuse, and productive of exactly the tables that decide the case.

Anatomy: modules, documents and the flow

- **Modules as territories:** finance and controlling, materials management and procurement, sales and distribution, production, HR/payroll: integrated over one database: the dispute's home module named first, its neighbours mapped for the flow's crossings.
- **The purchase-to-pay flow:** requisition, purchase order, goods receipt, invoice receipt, payment: with the three-way match (order, receipt, invoice) as the control seam: procurement disputes live here, and §7's frauds are its evasions.
- **The order-to-cash flow:** sales order, delivery, billing document, receivable, receipt: warranty, supply and pricing disputes' territory, with pricing conditions and their change histories a frequent centrepiece.
- **Master data as the quiet layer:** vendor and customer masters (bank details, addresses, payment terms), material masters, price conditions: slowly changing, heavily controlled, and the highest-value target for both fraudsters and examiners: master-data change history is requested as standard.
- **Document numbering and linkage:** everything numbered, everything referenced: the flow reconstructable from any link in either direction: and number-range gaps, like guide 72's sequence gaps, visible and explicable or visible and telling.

Change documents, audit logs and the history layer

- **Change documents (the SAP idiom) and audit tables (the Oracle idiom):** field-level edit records: object, field, old and new values, user, timestamp: standard for master data and key transaction fields: the two-date engine of guide 72 §3 running at enterprise coverage.
- **Security audit and sign-on logs:** logins, terminal/IP context, critical transaction usage: configuration-dependent in depth: the presence layer bracketing the edits.
- **Table-level logging:** optional deep logging for designated tables: where enabled, the completeness backstop; where not, its absence bounds findings per the standing fairness rule.
- **Job, interface and batch logs:** scheduled runs, EDI and interface traffic, payment-run logs: dating the automated acts and attributing connector-posted documents past service accounts, per guide 72 §10's join.
- **History integrity:** the logging configuration's own change history: what was logged, since when, altered by whom: read first in any contested-history matter, per guide 72 §4's rule: the trail shortened mid-dispute remains the pattern it always is.

Approvals, workflows and authorisation evidence

- **Workflow records:** release strategies and approval chains on requisitions, orders and invoices: who approved, when, at which step, from which inbox: the authorisation narrative in system form.
- **Roles and profiles:** the permission map: which users held which authorisations across the period: reconstructed from role assignments and their change history: "who could have" answered structurally.
- **Segregation-of-duties analysis:** conflicting permissions held together (create vendor and approve payment; maintain master data and run payments): the control-failure evidence in negligence and audit-liability disputes, and the opportunity evidence in fraud.
- **Delegations and substitutions:** approval substitutes, delegated inboxes, shared duties during absences: the attribution complications enumerated before the trial discovers them: guide 53's delegation layer at ERP scale.
- **Emergency and elevated access:** firefighter/emergency user records: elevated access grants with their sessions logged: the high-privilege windows checked against the disputed acts' timing.

Scoping and extraction at enterprise scale

- **The ERP slice:** company codes, plants, document types, vendor/customer ranges, date windows, and named tables and change-document objects: the guide 71 §4 discipline in the system's own vocabulary: precise enough that two specialists would extract the same rows.
- **Extraction routes:** standard reports and line-item displays for the readable layer; table extracts and documented queries for the analytical layer; archive retrievals for aged data: each with query text, run records, counts and hashes: the reproducibility bundle, non-negotiable at this scale.
- **Cloud-era mediation:** SaaS deployments constrain direct table access: provider export facilities, standard audit reports and API routes replace database queries: capability audited per deployment before methodology is promised.
- **Archiving and residence times:** ERP data archives off the live database on schedules: the disputed period may already be in archive files: retrievable, budgeted, and named in preservation letters so the archive run does not become the destruction event.
- **The agreed-queries model, scaled:** guide 71 §7 adapts directly: specialists settle the report and extract definitions, runs are verified by control totals against filed accounts and payment files, and the opponent's burden objection is answered by the protocol's precision: Example 3 of guide 71, with bigger tables.

Patterns: procurement fraud, warranty and supply-chain disputes

- **Vendor-master manipulation:** bank details edited before payment runs and reverted after: the classic, caught by master-data change documents joined to payment-run logs.
- **Fictitious vendor chains:** vendors created, orders raised, receipts confirmed and invoices paid by overlapping users: the SoD join of §5 finding the one pair of hands behind four roles.
- **Three-way-match evasions:** tolerances exploited, receipts posted without goods, invoice-only postings where matches were bypassed: the flow's gaps as the fraud's fingerprints.
- **Price and condition manipulation:** pricing conditions edited for chosen customers or periods: condition change histories dating the favouritism warranty and competition disputes allege.
- **Warranty and supply reconstructions:** what was ordered, shipped, received and rejected, when: the document flow as the dispute's agreed spine, with quality notifications and returns completing the story: often the least contentious and most decisive evidence in the case.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the production system is the centre of an estate with depth behind it. ERP evidence also lives in: archive files holding aged documents off the live database; database backups and system copies (the point-in-time layer, per guides 71-72); quality and test systems refreshed from production at datable moments (guide 73 §8's sandbox logic, enterprise edition); the data warehouse and reporting layers holding transformed history (sometimes longer than the source); interface partners: banks (payment files and statements: the external spine), EDI counterparties, logistics providers: each holding their side of the flow; printed and rendered outputs (the POs and invoices as sent: the downstream documents of guide 71 §8); the correspondence estate around the transactions; and the counterparty's own ERP, whose mirror-image flow is the ultimate convergence check in supply disputes. When the production system's history is contested, the backups bracket it, the bank files anchor the payments, and the counterparty's system tells the other half of every transaction.

EVIDENCE	PRODUCTION SYSTEM	ARCHIVES / BACKUPS	QA / TEST COPIES	WAREHOUSE / REPORTING	BANKS & COUNTERPARTIES	DELETED / RECOVERABLE
Document flows	Y: linked chains	Aged links in archive	Point-in-time states	Transformed history	Their mirror flow	Linkage survives archiving
Change history	Change documents / audit tables	Archived with objects; backups bracket	Config-era snapshots	Sometimes staged	n/a	Retention + backups decide
Approvals / authorisations	Workflow + role data	Historic role states in backups	Refresh-date states	SoD reporting extracts	n/a	Reconstructable per period
Payments	Payment runs + logs	Archived runs	n/a	Y	Y: files and statements, the spine	Bank layer persists
Master data states	Current + change docs	Prior states	Refresh snapshots	Dimension history	Their records of your details	Multi-layer, routine

Fallback strategy in one line: when the live system's story is contested, bracket with backups, anchor with the bank, and converge with the counterparty's mirror: the enterprise flow is too connected to rewrite everywhere at once.

Worked examples

EXAMPLE 1 · THE BANK DETAILS THAT CHANGED FOR NINE DAYS

A manufacturer paid £612,000 to fraudsters after a supplier's bank details were "updated". The change documents told the whole story in four rows: vendor master IBAN changed by a procurement clerk's login on the 3rd; payment run on the 9th selecting the vendor's open items; IBAN reverted by the same login on the 12th; and the security audit log placing that login's sessions at a terminal in the accounts office, out of hours, on both change dates. The SoD analysis added the structural finding: the clerk's role combination (maintain vendor masters plus release payment proposals) was a conflict the control framework prohibited on paper and permitted in the role build. Recovery proceeded against the fraudster; the negligence case against the integrator settled on the role-build finding; and the four change-document rows did the work of forty witness statements.

EXAMPLE 2 · THE THREE-WAY MATCH THAT NEVER HAPPENED

An internal investigation into a depot's costs found a vendor paid £1.9m over three years for "maintenance consumables". The flow analysis found the shape: every invoice posted through an invoice-only route bypassing the goods-receipt requirement under a tolerance configuration changed: per the configuration's own change history: a month before the vendor's first invoice; no purchase orders referenced; no receipts anywhere. The approval layer completed it: every invoice released by the depot manager, whose emergency-access sessions coincided with the quarter-end postings. The vendor's registered address matched the manager's brother-in-law's. The document flow's absences: no orders, no receipts, no match: were the fraud's exact silhouette, and the configuration change that enabled them dated its beginning to the week.

EXAMPLE 3 · THE TWO ERPS THAT AGREED AGAINST THE PLEADING

A supply dispute turned on whether 40 containers of components were delivered short in 2024: the buyer's claim said yes; its own goods-receipt postings were equivocal after a chaotic warehouse migration. The convergence route settled it: the seller's order-to-cash flow (deliveries, shipping documents, billing) was extracted under the agreed-queries protocol; the buyer's purchase-to-pay flow likewise; and the logistics provider's records joined both. Container by container, the three datasets reconciled: delivered quantities matching the seller's deliveries and the carrier's manifests, with the buyer's receipt postings lagging weeks behind physical arrival during the migration window: recorded late, not delivered short. The claim was withdrawn on exchange of the joint schedule: two ERPs and a carrier, agreeing against the pleading, ended what witness recollection had sustained for a year.

Common mistakes and technical limitations

Common mistakes

- **Requests without fluency:** "all SAP data relating to the dispute": refused with justified burden arguments, where the named tables and document types would have been produced in a week.
- **The change layer unrequested:** current-state extracts accepted, the field histories: the actual evidence: never sought: guide 72's mistake at enterprise scale.
- **Archiving as ambush:** the relevant period archived mid-dispute under routine schedules nobody suspended.
- **Print-outs as production:** document displays screenshotted into PDFs: linkage, histories and verifiability all destroyed.
- **Authorisation evidence skipped:** "who approved" litigated on emails while the workflow records sat unread.
- **SoD unanalysed:** fraud pleaded without the permission map that shows opportunity: §5's structural layer wasted.
- **The bank spine borrowed:** payment evidence taken from the system under scrutiny rather than the bank's own files: guide 72 §10's error, larger.
- **Counterparty convergence forgotten:** Example 3's route: the other ERP's mirror flow, never requested.

Technical limitations

- **Change coverage is designed, not total:** not every field generates change documents: what can be dated is object-specific, mapped before promises.
- **Log configuration governs depth:** security audit and table logging vary by build: absences bound findings per the fairness rule.
- **Cloud deployments mediate access:** SaaS eras trade database depth for provider exports: methodology follows the deployment, not the textbook.
- **User is login, not hand:** shared IDs, service accounts and emergency users need the attribution ladder: the ERP names the credential; guide 65 §7 names the person.
- **Reconstruction has horizons:** archive retention, backup cycles and history residence times bound the reachable past: the horizon stated per source, per period, in every report.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which system, version and hosting era: and who are the basis and functional people who can map the issues to tables with the laboratory?
- Are archiving runs, log rotations and backup cycles suspended for the relevant scope: in writing, today?
- Which flows carry the dispute: and do we hold the counterparty-facing outputs (orders, invoices, payment files) that anchor them externally?

Ask your opponent

- Please identify the ERP system, version and hosting model, and produce for [company codes / vendors / period]: the document flows for [document types], the change documents / audit records for the same and for the related master data, and the workflow and approval records: in table or structured form with the data dictionary.
- Please state the security audit, table-logging and change-document configuration for the period, including any changes to that configuration, and confirm suspension of archiving and log rotation for the relevant scope.
- Please produce the role and authorisation assignments of [users] for the period, including changes, delegations and any emergency or elevated access with its session records.

Ask your eDiscovery / forensic provider

- What does this build's history layer actually cover: and what must come from backups and archives instead?
- What does the flow analysis show for the disputed transactions: and where are its gaps?
- Does the authorisation map support the pleaded mechanics: who could, who did, in which sessions?

SUGGESTED WORDING · ERP LIMB FOR THE PRESERVATION LETTER

"Your client must immediately preserve all enterprise system (ERP) data relating to the issues, including: (a) all transactional documents and their document flows for [scope], together with the related master data; (b) all change documents, audit records, security audit logs, sign-on records and workflow or approval records for the same scope and period, whose deletion, rotation or truncation must be suspended; (c) the logging and change-document configuration applicable during the period, together with any changes to it; (d) all archive files, database backups and system copies covering the period, which must not be overwritten, and in respect of which any scheduled archiving or deletion runs affecting the relevant scope must be suspended; and (e) all authorisation, role and access records for the users concerned. Please confirm within [3] days, identifying the system, version and hosting model and the persons responsible for its administration."

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

The ERP checklist

- ☐ System, version and hosting era established; mapping session held with people who know the build
- ☐ Archiving, rotations and backup cycles suspended for scope, in writing
- ☐ Requests drafted in the system's vocabulary: document types, flows, objects, tables
- ☐ Change layer and configuration history collected beside the transactions
- ☐ Workflow, role and SoD data obtained for the authorisation questions
- ☐ Extraction by documented routes with the reproducibility bundle
- ☐ Payments anchored to bank files, not the system's own rendering
- ☐ Counterparty and carrier convergence pursued in supply disputes
- ☐ Archive and backup horizons stated per source in the analysis
- ☐ Expert roles divided: platform, forensic, accounting: under one chronology

Red flags

- Master-data edits bracketing payment runs: Example 1's nine days.
- Flows with structural absences: no orders, no receipts, no match: Example 2's silhouette.
- Configuration and tolerance changes dated to a scheme's beginning.
- Emergency-access sessions coinciding with disputed postings.
- Archiving runs or log-retention changes after notice.
- Productions of print-outs resisting table-level extracts.
- Role builds combining duties the control framework prohibits.

When to involve a digital forensic expert

At mapping, where platform fluency turns issues into table names; at preservation, where archive schedules and log rotations set real deadlines; at extraction, where documented routes and control totals make terabytes verifiable (§6's craft); at analysis, where flows, change layers and authorisation maps become the Examples 1-3 machinery; and at reporting, where system facts, accounting meaning and platform behaviour are divided among the right experts under CPR Part 35 and joined in one guide 70 chronology. Through **e-discovery.uk**, ERP extracts sit in review beside the correspondence: the transaction rows next to the emails that arranged them.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can we really get evidence out of something as vast as SAP?

Routinely: vastness is the storage, not the request: a well-scoped ERP demand (named flows, document types, vendors, periods, change objects) produces bounded, structured, verifiable extracts faster than most email exercises: the system's own discipline works for you. What fails is vagueness: §2's point: and the cure is drafting with someone who speaks the platform, which is a scoping call, not a project.

What is a change document, in one paragraph?

The ERP's field-level history record: when a tracked field on a tracked object changes, the system writes who changed it, when, from what value to what value: automatically, as part of the transaction. It is guide 72's entry-date discipline built into the platform's bones: and it is why enterprise-system backdating and master-data fraud cases so often reduce to a four-row exhibit, per Example 1.

The opponent says extraction would cost a fortune and disrupt production. Genuine?

Sometimes: wholesale demands genuinely burden these systems: which is why the answer is precision plus protocol: the named-scope request, standard reports and table extracts, runs from copies or quiet windows, agreed queries between specialists with control totals: guide 71 §7 scaled. Offer the protocol in terms; a burden objection that survives a precise, cooperative, verifiable proposal is rare, and its rarity is visible to the court.

Who actually did it, when the system only shows a user ID?

The ID is the first rung: behind it run sign-on logs (terminals, IPs, times), session and transaction usage records, delegation and substitution data, emergency-access grants, and: for the human join: the device and presence layers of guides 61 and 78 plus the correspondence. Shared and service accounts widen the pool honestly; the finding is pleaded to the rung reached, per the series' standing attribution method: and Example 1's out-of-hours terminal sessions show how far the rungs can climb.

The relevant years have been archived off the live system. Problem?

A retrieval, not a wall: archive files preserve documents with their linkage and are read back by the platform's own retrieval facilities; backups bracket what archiving predates; and the warehouse layer often holds the period in reporting form meanwhile. Cost and time are real and scoped honestly: and prospectively, the preservation letter's suspension of archiving runs (§11's wording) exists precisely so the dispute's period stops moving while you argue about it.

Our supply dispute is really about what physically shipped. Can the ERP say?

It says what was recorded: orders, deliveries, receipts, quality postings: which becomes what shipped when converged with the outside: the counterparty's mirror flow, the carrier's manifests, the bank's payments: Example 3's three-way agreement. The ERP is the best witness to the paper reality and a strong proxy for the physical one; the convergence protocol is how the proxy becomes proof: and it settles supply cases with a regularity witness evidence never matches.

§ 1 4 · REFERENCE

Glossary

Change document

The field-level edit record: object, field, old/new value, user, time.

Company code

The legal-entity unit of ERP finance; a scoping axis.

Document flow

The linked chain from requisition to payment or order to cash.

Emergency access

Logged elevated-privilege sessions; checked against disputed acts.

Master data

Vendors, customers, materials, prices: the slowly changing high-value layer.

Release strategy

The configured approval chain on procurement documents.

Residence time

How long data stays live before archiving; a reachable-past horizon.

Segregation of duties

The conflicting-permissions analysis: opportunity in structural form.

Three-way match

Order, receipt and invoice reconciled before payment; the control seam.

Transaction code

The platform's command vocabulary; fluency's unit.

Sources and authoritative references

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

- cflab.uk, digital forensics services (ERP forensics, change-document analysis, authorisation evidence, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDM Phase 01 · Identification, Phase 03 · Collection and Phase 04 · Processing (enterprise sources in the data map; scoped extraction into review): e-discovery.uk/edrm/identification · 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: SAP change documents and security audit log: help.sap.com · Oracle E-Business Suite and Fusion auditing: docs.oracle.com · Microsoft Dynamics 365 auditing: learn.microsoft.com
- PD 57AD, CPR Part 31 and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, 27037

DISCLAIMER

This publication provides general information about ERP evidence as at August 2026. Platform capabilities, logging coverage, archiving behaviour and hosting models vary by product, version and implementation and change on vendors' schedules; verify the current position for the system 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

Enterprise-system instructions at the laboratory begin with fluency: the mapping session that converts pleaded issues into company codes, flows, objects and tables: and with the clock: archiving runs and log rotations suspended before the period in dispute moves out of reach. Extraction follows §6's discipline: documented routes, control totals against bank files and filed accounts, the reproducibility bundle throughout: and analysis delivers the machinery of Examples 1-3: change-document chronologies, flow reconstructions with their telling absences, authorisation and SoD maps, and counterparty convergence in supply disputes. Expert roles divide per §1's model and join in one guide 70 chronology, reported under CPR Part 35 to the evidenced rung. Through **e-discovery.uk**, ERP extracts and the correspondence estate share one review. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if an archiving run is scheduled against your dispute's period, its suspension is today's letter.



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