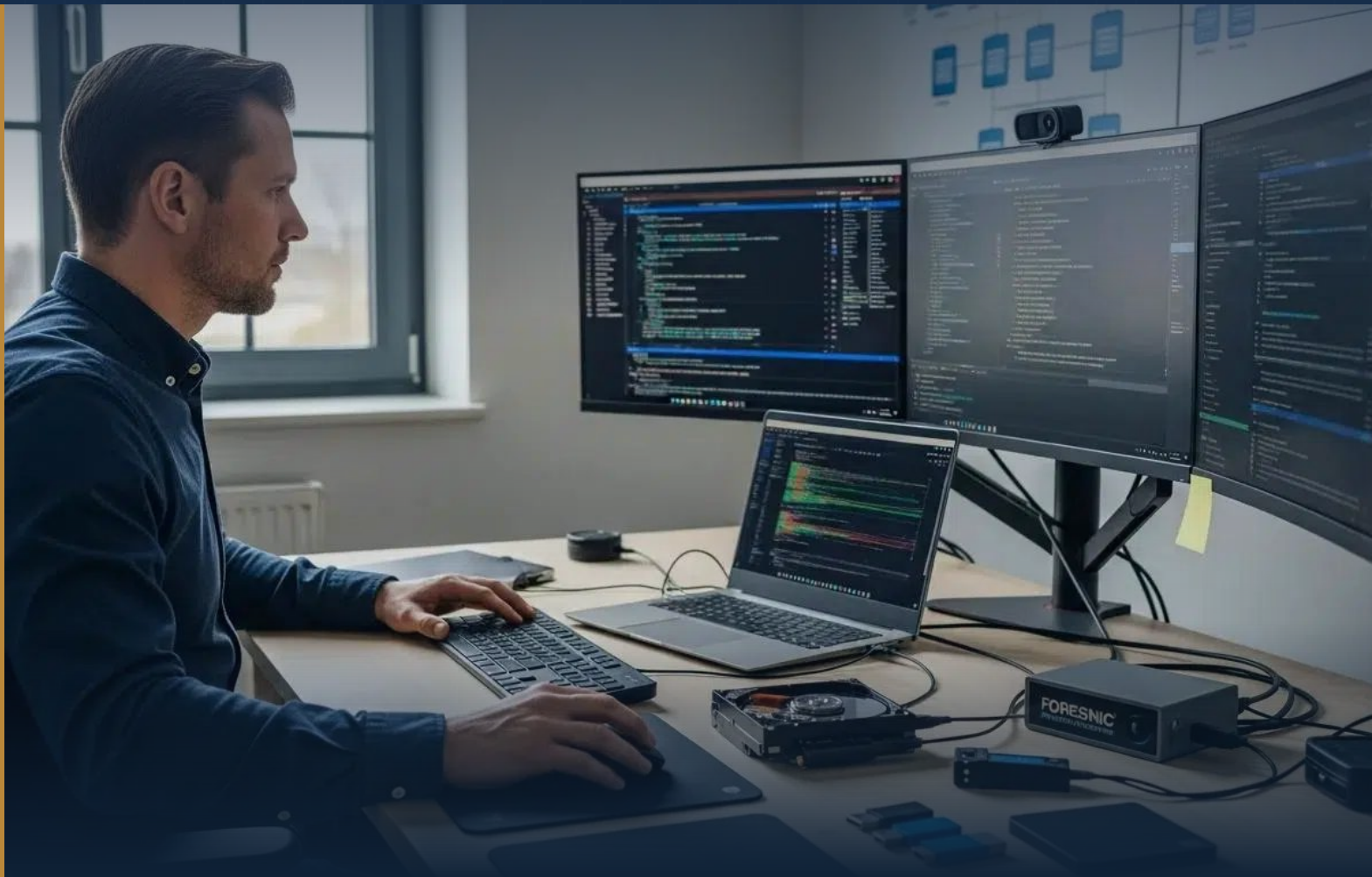




Computer Forensics Lab
CFLAB.UK · LONDON



DIGITAL FORENSICS · E-DISCOVERY · EXPERT WITNESS

Digital evidence you can rely on in court.

Independent forensic examination of computers, mobile devices and cloud accounts for law firms, corporate counsel, litigators and company directors across the United Kingdom.

Technically reliable. Legally defensible. Clearly communicated.

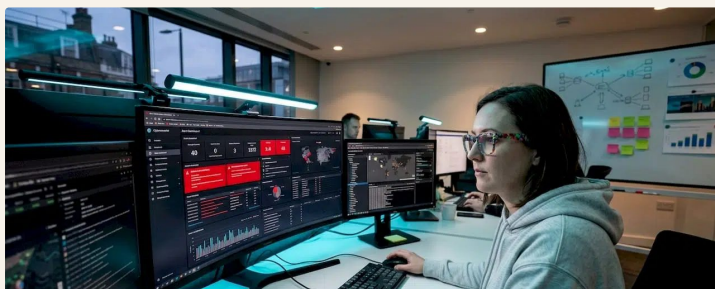
Computer Forensics Lab is a specialist provider of digital forensics, electronic discovery and cyber-investigation services for criminal defence, prosecution, corporate and civil litigation matters.

We support legal professionals, investigators, corporations, insurers, local authorities and government organisations throughout the UK. Our work covers the identification, preservation, collection, examination, analysis and presentation of digital evidence from computers, mobile devices, cloud platforms, servers, networks and other electronic systems.

Matters range from individual criminal investigations and employment disputes to complex corporate investigations, regulatory inquiries, fraud cases, intellectual property disputes and large-scale litigation.

What sets our reports apart

- ◆ Tailored to the legal and investigative issues in each matter
- ◆ Complex technical findings translated into clear, concise conclusions
- ◆ Methods, evidence examined and limitations stated openly
- ◆ Prepared to CrimPR Part 19 and CPR Part 35 expert standards
- ◆ Evidence handled to preserve integrity and continuity from day one



"Digital evidence must be technically reliable, legally defensible and clearly communicated. We work with clients from the earliest stage to define the issues and set the forensic strategy."

WHO WE WORK WITH



Law firms

Criminal defence, civil litigation, family and employment teams



Corporate counsel

Internal investigations, regulatory response, data theft



Litigators

E-discovery, disclosure, timeline and expert support



Company directors

Misconduct, fraud, breach response, forensic readiness

2007

ESTABLISHED

ISO 17025

ALIGNED PRACTICE

NPCC

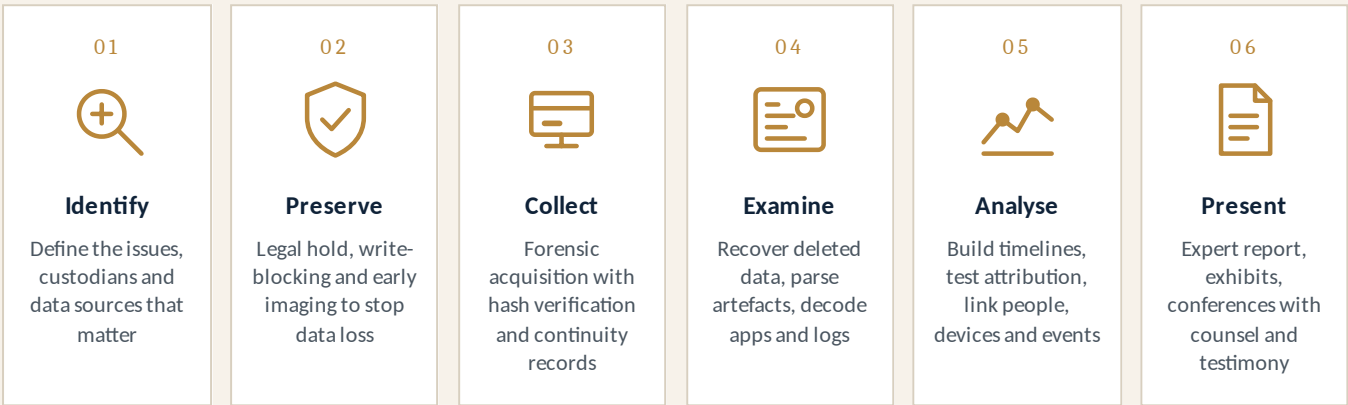
EVIDENCE GUIDANCE

UK-wide

INSTRUCTION
ACCEPTED

From seizure to courtroom: a defensible forensic process.

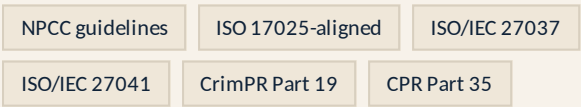
Every engagement follows a structured workflow designed so that each finding can be traced, reproduced and explained to a judge, jury or tribunal.



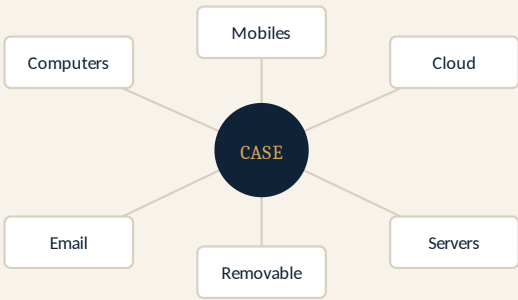
Standards we work to

Examinations follow the National Police Chiefs' Council (NPCC) Digital Evidence Guidelines, which emphasise integrity, reproducibility and accountability, alongside ISO 17025-aligned laboratory practice and the methodologies set out in ISO/IEC 27037 and ISO/IEC 27041.

Every image is hash-verified, every action is logged, and every conclusion is stated with its limitations. That discipline is what keeps evidence admissible when it is challenged.



Where the evidence lives



Emails and headers, chat apps, call logs, photos and EXIF, documents and metadata, browser history, cloud sync logs, USB and file-system artefacts, CCTV, network and server logs.

One lab. The full evidential lifecycle.



Computer forensics

Laptops, desktops and workstations: deleted file recovery, user activity, USB history, document metadata and anti-forensic traces.



Mobile phone and tablet forensics

Full and logical extractions, WhatsApp, Signal and Telegram decoding, location data, deleted message recovery and cloud backups.



Cloud, email and online accounts

Microsoft 365, Google Workspace, iCloud and social platforms: authenticated acquisition, header analysis and audit-log reconstruction.



Servers, networks and media

Server images, network logs, removable media and NAS devices examined for access, exfiltration and tampering.



E-discovery and disclosure

Defensible collection, processing, deduplication, keyword and date searches, review support and production for disclosure.



Incident response

Post-breach analysis establishing what was accessed, by whom and when, with evidence preserved for regulators and litigation.



Expert witness

Independent CrimPR 19 and CPR 35 reports, joint statements, conferences with counsel and oral evidence at trial.



Evidence strategy and review

Review of prosecution or opposing expert material, identification of gaps, and advice on what further examination could show.



Forensic readiness and training

Preservation policies, evidence-handling procedures and practical training for in-house teams and law firms.

Criminal defence and prosecution

Independent examination of seized devices, challenge or support of attribution, timeline verification, review of Streamlined Forensic Reports and defence-led examination of unallocated space and cloud data.

Civil, regulatory and employment

Breach of confidence, restrictive covenant and IP disputes, data-theft claims, regulatory inquiries, disciplinary proceedings and insurance investigations.

Establish the facts. Keep the evidence.

We assist organisations with sensitive internal investigations: suspected fraud, employee misconduct, data theft, unauthorised access, misuse of company systems, intellectual property theft and breaches of confidentiality.

We work discreetly and proportionately, helping you establish what happened while preserving evidence for any disciplinary, civil, criminal or regulatory step that follows.

Typical questions we answer

- ◆ Did a departing employee copy client data to a USB drive or personal cloud?
- ◆ Who accessed the finance share on the night the payment was altered?
- ◆ Was this email genuinely sent by the person it names?
- ◆ Were files wiped or back-dated before the device was handed over?
- ◆ What did the attacker reach, and is the regulator notification justified?

Illustrative case timeline

Departing employee - data exfiltration

- Mon 18:42**
Resignation email sent to HR
- Mon 21:15**
Unregistered USB device first connected
- Mon 21:16 to 21:48**
1,284 client files opened from CRM export
- Mon 22:03**
Personal webmail login; 3 attachments sent
- Tue 07:50**
Disk cleaner executed; Recycle Bin emptied
- Recovered**
Shellbags, LNK files and USB registry keys survive

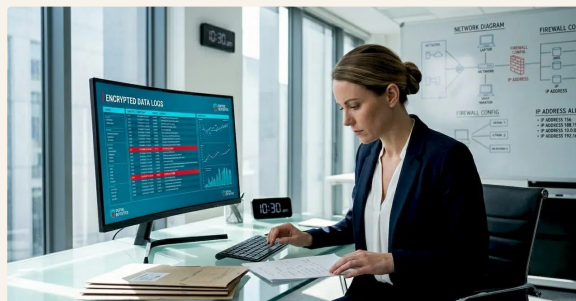
Composite example of common case patterns, not an identifiable matter.

LITIGATION SUPPORT AND ELECTRONIC DISCOVERY

Large data. Defensible process. Practical scope.

We provide end-to-end support for cases involving significant volumes of electronically stored information, including matters with multiple custodians, international data sources, cloud systems, mobile devices, messaging applications and structured business data.

Our aim is a proportionate, defensible e-discovery strategy that stands up to scrutiny from the court and opposing experts without inflating cost.



Early case assessment

Legal hold

Forensic collection

Processing and deduplication

Keyword and date searches

Review support

Disclosure production

Timeline and link analysis

Expert schedules and exhibits

Mid-market matters. Full-scale rigour.

The projects below show the shape of corporate e-disclosure and investigation work we support for law firms, in-house counsel and boards: matters that are substantial in value and volume, but where proportionality and precision matter more than sheer scale. Each is an illustrative composite of common case patterns.

CASE A

Departing director, clients and trade secrets

A privately owned engineering company (turnover £200m) discovers its Commercial Director has resigned and joined a competitor. The board suspects that confidential pricing, customer lists and sales forecasts were copied before departure, and external solicitors need evidence fit for injunction proceedings.

COLLECTED Company laptop, mobile phone, Microsoft 365 account, OneDrive, SharePoint access logs and Teams communications, with custodian interviews to identify witnesses and further data sources.

REVIEW USB, external email, cloud upload and last-access activity in the final months; searches on competitor names, customer accounts, pricing, proposals and future employment; email threading, near-duplicate analysis and timeline reconstruction in Relativity.

DELIVERABLES Forensic report, disclosure database, chronology of events, communication analysis and evidential exhibits.

CASE B

Shareholder dispute in a PE-backed business

A software company valued at around £750m is in litigation between majority shareholders and minority investors, who allege that financial information was withheld during a funding round that diluted their holding.

COLLECTED Around 3TB from 20 custodians over three years: board members, finance teams, external advisers and senior management. Outlook mailboxes, Teams chats, board packs, financial models, accounting systems and document repositories.

REVIEW Issue-based workspaces allowing solicitors to examine valuation discussions, fundraising strategy, investor communications and board decision making against published financial information.

DELIVERABLES Disclosure productions, privilege reviews, board communication chronologies and witness preparation bundles.

CASE C

Supplier fraud and procurement investigation

A manufacturer with £400m annual revenue identifies unusual procurement spending and suspects collusion between employees and an external supplier. The findings may support civil recovery and a criminal referral.

COLLECTED Typically 1TB to 5TB from procurement managers, finance personnel, senior executives and supplier relationship managers: email, ERP systems, purchase orders, invoices, Teams and mobile devices.

REVIEW Inflated pricing, undisclosed relationships and unusual approval patterns, with analytics mapping communication frequency between employees and supplier contacts.

DELIVERABLES Transaction chronologies, communication maps, forensic findings report and disclosure datasets.

CASE D

Commercial contract dispute

A £1bn logistics company brings a £50m claim against a technology provider after a failed warehouse management system implementation spanning three years of project activity, consultants and third-party contractors.

COLLECTED Emails, Teams messages, project plans, meeting minutes, contracts, change requests and technical reports from internal stakeholders and external parties.

REVIEW When problems became known, how they were escalated and what was represented to the customer, with a chronology linking communications to project milestones so counsel can assess liability, obligations and mitigation.

DELIVERABLES Issue-coded document review, hearing bundles and project timelines on the disclosure platform.

Precision where it counts.

CASE E

Workplace misconduct and executive investigation

A privately owned company receives allegations against a senior executive involving harassment, retaliation and misuse of company resources. Unlike a large regulatory matter, the focus is precision rather than volume.

COLLECTED Around 10 custodians across Microsoft 365, Teams, mobile devices and HR systems.

REVIEW Communications between the executive and complainants, management discussions and HR case files, with extensive redaction and restricted access controls for sensitive material.

DELIVERABLES Investigation report, disclosure-ready document sets, communication timelines and evidence packs suitable for employment tribunal proceedings.

CASE F

M&A due diligence and post-acquisition dispute

A £900m healthcare business acquires a specialist medical technology company. After completion the purchaser alleges that material operational issues were concealed during due diligence.

COLLECTED Typically 2TB to 8TB across both businesses: executive teams, finance and operational management, due diligence portals, email, board papers, forecasting models and compliance records.

REVIEW Whether adverse information existed before the transaction and whether it was disclosed appropriately.

DELIVERABLES Transaction chronologies, disclosure reviews, key document identification and expert witness support.

Typical mid-market corporate e-disclosure scope

Our sweet spot is the substantial matter that does not reach the scale of a FTSE 100 or Fortune 500 disclosure exercise: the work national and regional commercial litigation practices instruct most often.

ORGANISATION SIZE	CUSTODIANS	DATA VOLUME	MATTER VALUE
£50m to £250m business	5 to 15	250GB to 2TB	£250k to £5m
£250m to £750m business	15 to 30	1TB to 5TB	£1m to £25m

Custodian interviews

Forensic collection

Relativity processing and review

Email threading

Near-duplicate analysis

Communication analytics

Privilege and redaction

Chronologies and hearing bundles

Expert witness support

"In a mid-market dispute the question is rarely whether the data can be reviewed. It is whether the right custodians, sources and issues were identified at the outset, so that the review is proportionate and the findings survive challenge."

Case examples are illustrative composites of common patterns and do not describe identifiable matters. Volumes and values are indicative.

Independent. Clear. Relevant.

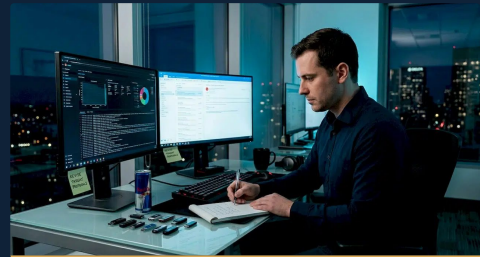
Joseph Naghdi, Chief Digital Forensics Expert at Computer Forensics Lab, provides independent digital-forensics expertise to legal teams and organisations.

He has extensive experience presenting complex technical evidence in a clear and comprehensible manner, and supports clients through expert report preparation, conferences with counsel and courtroom proceedings. Where required, he gives oral evidence and responds to questions concerning the acquisition, authenticity, integrity, interpretation and significance of digital evidence.

Joseph is a member of the IEEE Computer Society and of BCS, The Chartered Institute for IT.

What every report contains

- ◆ The instructions received and the questions addressed
- ◆ The evidence examined, with hash values and continuity
- ◆ The tools and methods used, and why
- ◆ Findings, in plain English, with supporting exhibits
- ◆ The limitations of the analysis and alternative explanations
- ◆ Conclusions and the expert's declaration of duty to the court



Areas of specialist skill

- ◆ Computer, mobile-device and cloud forensics
- ◆ Corporate and internal investigations
- ◆ Criminal, civil, regulatory and employment matters
- ◆ Expert-witness reporting and courtroom testimony
- ◆ Evidence collection, continuity and handling
- ◆ Digital-evidence interpretation and presentation
- ◆ Leading complex, rapidly evolving investigations

Criminal

Review of prosecution digital evidence, independent re-examination of devices, attribution challenges, indecent image and fraud cases, cell-site context.

Civil and commercial

Single joint expert or party-appointed work in data-theft, restrictive covenant, IP and contract disputes; Part 35 compliant reports.

Tribunals and regulators

Employment tribunals, professional disciplinary bodies, ICO and FCA matters, and internal hearings requiring an independent technical voice.

Instruct early. Preserve first. Scope proportionately.

When to call

- ◆ A device, account or server is about to be seized, returned, reissued or wiped
- ◆ You have received prosecution digital evidence or an opposing expert's report
- ◆ An employee has left and data may have gone with them
- ◆ A breach has been detected and decisions on notification are pending
- ◆ Disclosure involves more data than the team can review by hand
- ◆ Authenticity of an email, document, photo or message is in dispute

How an instruction runs

1. **Initial call.** Free, confidential discussion of the issues and likely sources of evidence.
2. **Scoping letter.** Clear questions, fixed or estimated fees, timescales and deliverables.
3. **Preservation and collection.** On-site or in the lab, with full continuity documentation.
4. **Examination and interim findings.** Early feedback so strategy can adapt.
5. **Report and support.** Court-ready report, exhibits, conferences and testimony as required.

Preserve the evidence: first 24 hours

- ◆ Do not switch on, log in to or "have a look" at the device
- ◆ Do not reset passwords or revoke accounts before the audit log is exported
- ◆ Record who has had the device and when
- ◆ Suspend automatic deletion and retention policies
- ◆ Keep mobiles charged and in airplane mode, or in a Faraday bag
- ◆ Call us before anything else is done to the data

Legal aid and private funding

We prepare estimates in the format required for prior authority applications and work to agreed fixed fees on private and corporate instructions.

Secure, accredited handling

ISO 17025-aligned laboratory practice, ICO registration (ZB395023), encrypted transfer, secure storage and documented destruction at the close of a matter.

"The most common reason digital evidence fails is not the technology. It is what happened to the device in the days before anyone thought to call an expert."



Computer Forensics Lab

DIGITAL FORENSICS · E-DISCOVERY · EXPERT WITNESS

GET IN TOUCH

Talk to an expert before the evidence changes.

Initial discussions are confidential and without obligation. Instructions accepted from solicitors, counsel, in-house legal teams and directors throughout the United Kingdom.



TELEPHONE +44 (0)20 7164 6915



EMAIL info@cflab.uk
info@e-discovery.uk



WEB cflab.uk
e-discovery.uk



LAB Euro House, 133 Ballards Lane
Finchley, London N3 1LJ

ISO 17025-aligned laboratory practice

NPCC Digital Evidence Guidelines

ICO registration ZB395023

IEEE Computer Society

BCS, The Chartered Institute for IT