COMPUTER FORENSICS LAB

LONDON · DIGITAL FORENSICS · SINCE 2007

London, UK · Established 2007

§ 01 · CAPABILITY OVERVIEW · FOR US COUNSEL

UK digital evidence, handled like part of your trial team.

Specialist collection, forensic analysis and cross-border evidence support for US litigation teams. We preserve and interpret the technical evidence in London, then hand it into your firm's existing eDiscovery, review and litigation workflow — including Relativity.

Designed to complement — not replace — your eDiscovery team.

- UK custodians & onsite collections
- Mobile, cloud & endpoint forensics
- Trade-secret & employee-departure investigations
- Deleted data & difficult evidence
- Relativity-ready review handoff
- Declarations, reports & expert support

✓ ICO ZB395023 ✓ NPCC · ISO 17025 aligned practice ✓ UK Gov Digital Marketplace ✓ GDPR / UK DPA

cflab.uk · e-discovery.uk info@cflab.uk +44 (0)20 7164 6971

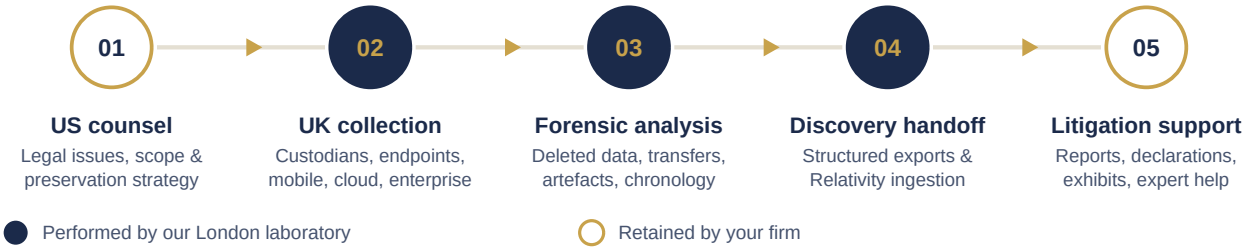
Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom

§ 02 · WHERE WE FIT

A forensic extension of your trial team, not another vendor to manage.

Computer Forensics Lab supports US counsel when a matter reaches beyond conventional document discovery — when the evidence sits in the United Kingdom, lives on physical devices or cloud platforms, or needs forensic interpretation before it can be reviewed effectively. Your lawyers keep control of strategy, privilege, review and production; we handle the technical evidence on the ground.

HOW A MATTER FLOWS



● Performed by our London laboratory ○ Retained by your firm

YOUR FIRM RETAINS

- Legal strategy, scope and preservation decisions
- Privilege calls, review and production
- Choice of review platform and vendors
- Case presentation and the client relationship

WE DELIVER

- Defensible UK acquisition, on site where needed
- Forensic interpretation: deleted data, transfers, artefacts
- Documented provenance, hashing and chain of custody
- Relativity-ready exports into your established workflow
- Declarations, technical explanations, expert assistance

You do not need a London office to have a defensible forensic capability in London.

§ 03 · CORE CAPABILITIES

Specialist support for evidence that does not fit neatly into ordinary discovery.

01
UK collection

Onsite or coordinated collection of custodians and devices across the United Kingdom, with documented acquisition, preservation, hashing and chain of custody. Practical where shipping original devices to the US is impractical or disproportionate.

02
Mobile & endpoint forensics

Forensic acquisition and examination of computers, laptops, iPhone and Android devices, removable media and other storage — using Cellebrite, Magnet GrayKey and comparable law-enforcement-grade tooling. Targeted analysis answers specific evidential questions.

03
Cloud & collaboration evidence

Collection and analysis across Microsoft 365 — Outlook, OneDrive, SharePoint, Teams — and other cloud or collaboration sources, scoped to your legal-hold, custodian and date-range requirements.

04
Trade secret & employee departure

Was confidential information accessed, copied, downloaded, synced, transferred, deleted or retained? We correlate file-system, browser, USB, cloud and communications artefacts into an evidential chronology.

05
Difficult & unusual data

An escalation path for damaged storage, deleted evidence, forensic images, proprietary datasets, archives, CCTV, servers and NAS — sources conventional processing workflows may not handle well.

06
Expert & technical support

Methodology statements, forensic reports, technical chronologies, evidential exhibits and expert assistance for contentious proceedings — presented in language lawyers, clients and courts can understand.

LABORATORY TOOLING RELIED ON BY LAW ENFORCEMENT & GOVERNMENT AGENCIES

Cellebrite UFED • Magnet GrayKey • Magnet Axiom • EnCase • FTK • X-Ways • Oxygen Forensics • XRY

§ 04 · EVIDENCE SOURCES

From custodian devices to enterprise and cloud data.

The most useful forensic engagement often begins with a question, not a data volume: what happened, when, on which system — and what evidence supports that conclusion? Acquisition and analysis are targeted to the legal issues in dispute.

Computers & storage	Windows and macOS endpoints; HDD/SSD; USB and external drives; forensic images; deleted and residual data
Mobile devices	iPhone and Android; app data; messages; media; metadata; location and usage artefacts where available
Microsoft 365	Outlook, OneDrive, SharePoint, Teams and related account or tenant evidence within agreed scope
Cloud & web	Cloud-storage activity, browser history, downloads, account artefacts, logs and platform exports
Employee activity	File access, copying, USB use, downloads, sync, deletion, external transfer and chronology reconstruction
Communications	Email, collaboration and messaging evidence, including metadata and attachments where lawfully available
Servers & specialist media	Servers, NAS, CCTV and other technical sources requiring specialist acquisition or recovery

ILLUSTRATIVE FORENSIC QUESTIONS

- Was the confidential file present — opened, copied, deleted?
- Was removable media connected? Was data synced to cloud?
- What happened immediately before the employee left?
- Which artefacts support — or contradict — each narrative?

THE OVERNIGHT ADVANTAGE

Evidence scoped at your close of business progresses through a full London working day — findings on your desk by 9am ET.

§ 05 · DEFENSIBILITY & HANDOFF

Built to integrate with your litigation, not to create another silo.

1	**Preservation**	Scope agreed with counsel; original evidence protected; collection method documented.
2	**Integrity**	Forensic acquisition, SHA-256 / MD5 hashing, contemporaneous notes and chain-of-custody records.
3	**Proportionality**	Targeted collection and analysis reduce unnecessary data movement and focus effort on relevant sources.
4	**Transparency**	Clear account of what was collected, what was not, the methods used and any technical limitations.
5	**Review handoff**	Structured delivery to your preferred discovery workflow, including Relativity-oriented processing and review.
6	**Expert support**	Findings translated into reports, timelines, declarations or evidential exhibits when required.

AUTHENTICITY YOU CAN INDEPENDENTLY REPRODUCE

Hashed at capture, re-verified at every stage — any alteration, however small, is instantly detectable.

MODEL 01

Matter-specific instruction

Counsel instructs us for a defined collection, examination or expert issue.

MODEL 02

UK collection partner

On-the-ground collection and preservation whenever US matters involve UK evidence.

MODEL 03

Specialist escalation resource

Your eDiscovery team calls us when a source is damaged, unusual, mobile or otherwise difficult.

Cross-border note: international collections are scoped with counsel and undertaken subject to applicable law, client instructions, data-protection requirements and the circumstances of the matter. We provide technical implementation and forensic support; legal advice on cross-border discovery and privacy remains with counsel.

§ 06 · WHEN TO CALL US

Six situations where a London forensic team materially reduces risk.

1 A UK custodian must be preserved urgently

The device cannot conveniently be shipped to the United States and the case team needs a defensible local acquisition.

2 A departing employee is suspected of taking data

Counsel needs evidence of USB use, downloads, cloud sync, file access, deletion or transfer — before systems change.

3 The evidence is on a phone

The matter requires specialist mobile acquisition and interpretation rather than a conventional email or file collection.

4 The dataset is technically difficult

Damaged media, deleted evidence, unusual archives, CCTV, proprietary data or forensic images require specialist treatment.

5 The legal team needs a factual chronology

Artefacts from multiple systems must be correlated into a clear sequence that supports or challenges witness accounts.

6 You need a specialist partner, not another platform

Collection and analysis happen locally; the output is handed back into your firm's established review workflow.

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

Prepared as a capability overview for US litigation teams. Service availability, methods and deliverables depend on the source systems, legal authority, engagement scope and technical condition of the evidence.