COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Preserving Evidence After a Cyber-Attack or Ransomware Incident

Recovering the Business Without Destroying the Case

In the hours after a cyber-attack, two imperatives collide: the business must recover: systems rebuilt, backups restored, operations resumed: and the evidence must survive: because the same organisation will shortly face regulators asking what happened, insurers testing the claim, counterparties alleging negligence, data subjects bringing claims, and possibly litigation against suppliers whose failures let the attacker in. Recovery destroys evidence by default: reimaging erases the attacker's traces, restoring overwrites the encrypted estate, and well-meant IT triage tramples the timeline. This guide gives UK lawyers and incident teams the discipline that serves both masters: what to preserve in the first hours and how, the evidence map of an intrusion, coordination with insurers and incident-response firms, the legal audiences and their clocks (ICO's 72 hours above all), and the litigation uses the preserved estate must eventually support.

⏱ 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. Incident work sits alongside its investigation practice: evidential preservation during live response, intrusion-timeline reconstruction, exfiltration assessment for notification decisions, and the reporting that serves regulators, insurers and courts from one preserved estate: with CPR Part 35 evidence where incidents become litigation.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | INCIDENT EVIDENCE PRESERVATION | INTRUSION TIMELINE RECONSTRUCTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: PRESERVE BEFORE YOU REBUILD: IMAGES, VOLATILE DATA AND LOGS CAPTURED IN THE FIRST HOURS SERVE EVERY AUDIENCE THE INCIDENT CREATES: AND THE RECOVERY THAT SKIPS PRESERVATION ANSWERS REGULATORS, INSURERS AND COURTS FROM MEMORY

The first hours (§3): before reimaging anything: forensic images of representative compromised systems (including at least some in their encrypted state), volatile captures (memory, connections, processes) where systems are still live, and the log estate exported at once: firewall, VPN, endpoint, identity-provider, cloud-platform and backup-system logs, all on rolling retention that the incident does not pause. Isolation beats power-off where containment allows: pulling cables preserves memory; pulling power destroys it. **The map (§4):** an intrusion's evidence follows its phases: entry (phishing artefacts, exploited services, credential-stuffing traces), movement (lateral authentication patterns, tool deployment, privilege escalation), exfiltration (staging archives, egress volumes, cloud-transfer logs: the question the ICO decision turns on), and impact (encryption events, deletion, the ransom artefacts): preserved per phase so the narrative is provable, not surmised. **The coordination (§5-§6):** insurer-appointed IR firms prioritise containment and recovery: legitimate, and not the same as evidence: so the preservation mandate is stated explicitly in the engagement, with legal privilege structured over the investigation (guide 98 §7's disciplines) and the ICO's 72-hour clock, subject-notification duties and sector regulators served from the preserved facts. **The litigation (§7):** the same estate later supports insurance recovery, supplier claims, defence of data-subject actions and: run per this guide: the disclosure exercise those proceedings demand, rather than a guide 95 gap inquiry into the response itself.

- **Image before reimage:** representative systems preserved in compromised state: the attack scene photographed before the cleanup.
- **Volatile first, always:** memory and live-state captures cannot be repeated: §3's ordering is physics, not preference.
- **Logs are the spine:** the multi-source log export in hour one: retention clocks do not respect incidents.
- **Preservation is a stated mandate:** IR engagements instructed to preserve as well as recover: §5's gap closed in writing.
- **One estate, every audience:** ICO, insurers, claimants and courts answered from the same preserved facts: or from memory, expensively.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: recovery eats evidence

Incident response and evidence preservation want different things from the same machines. Response wants the attacker out and the business up: which means isolating, wiping, reimaging, restoring and patching at speed. Every one of those verbs destroys evidence: the reimaged server loses the webshell and the tool cache; the restored share overwrites the encrypted files whose headers identified the strain; the rotated credentials close the account whose sign-in history mapped the intrusion; the rebuilt domain controller takes the authentication logs with it.

The organisation then spends months answering questions the destroyed evidence answered: What did they access? (the ICO's question); When did it start? (the insurer's policy-period question); Did data leave? (everyone's question); Whose failure let them in? (the supplier-litigation question). Answered from preserved images and logs, these are findings; answered from reconstruction and recollection, they are estimates that harden into exposure. The discipline of this guide costs hours inside the response; its absence costs the next two years. The resolution is not to slow recovery: it is to preserve in parallel, by the §3 ordering, with the mandate stated: the same both-masters logic every incident-capable organisation eventually adopts, usually after the incident that teaches it.

§ 0 3 · THE FIRST HOURS

The first hours: what to preserve before anything is rebuilt

- **Triage the estate for preservation:** the compromised population mapped fast; representative systems selected for full forensic imaging (patient zero candidates, domain controllers, key servers, a sample of encrypted endpoints): imaged before reimaging, with the encrypted state itself preserved on at least some: it carries the strain, the timestamps and sometimes the recovery route.
- **Volatile data while it lives:** memory captures, network-connection and process listings from still-running compromised systems: isolation by network disconnection rather than power-off where containment permits: because RAM holds the injected tools, keys and sessions that disk never sees, and shutdown erases it.
- **The log harvest, immediately:** firewall, VPN and proxy logs; identity-provider sign-in records; endpoint detection telemetry; cloud-platform audit trails (guides 51-58, 105); backup-system logs (which backups the attacker touched matters twice over); email-gateway records for the phishing question: all exported in hour one, because rolling retention is the incident's quiet second attacker.
- **The response's own record:** the incident log: actions, times, actors, decisions: kept contemporaneously from the first alert: the document every later audience reads first, and the one guide 96's timeline of the response is built from.
- **Ransom-communication preservation:** notes, portals, negotiation exchanges and payment artefacts preserved forensically (screenshots plus source capture): evidence for attribution, sanctions analysis and the insurance file: handled under advice, per §6's frameworks.

§ 0 4 · THE INTRUSION'S STORY

The intrusion evidence map: entry, movement, exfiltration, impact

- **Entry:** the phishing email and its artefacts (guide 80's header and domain work), the exploited service's logs, the stuffed or purchased credentials' first anomalous sign-ins, the vendor connection abused (the supply-chain route): the negligence and supplier-claim questions live here.
- **Establishment and movement:** persistence mechanisms, tool deployment traces, lateral authentication patterns across the identity logs, privilege-escalation artefacts: the dwell-time question (how long were they in?) answered here, with policy-period consequences §6 explains.
- **Reconnaissance and staging:** directory enumeration, search activity, staging archives assembled (the multi-gigabyte ZIP in a temp folder): the strongest pre-egress indicators of what was targeted.
- **Exfiltration:** egress volumes against baselines, transfers to attacker infrastructure, cloud-storage abuse, the staging archives' fate: the single most consequential question (notification scope, subject claims, leak-site risk) and the one §3's log harvest exists to answer: including, sometimes, in the negative: provable non-exfiltration is valuable.
- **Impact and cleanup:** encryption events and their sequence, deletion and log-clearing (guide 110's artefacts: the attacker's anti-forensics documented as such), backup destruction attempts: the impact narrative for insurers and the aggravation evidence for everyone else.

§ 0 5 · THE CROWDED BRIDGE

Working with insurers, IR firms and the preservation gap

- **The insurer's machinery:** cyber policies bring panel IR firms, breach counsel and negotiators at speed: valuable, and optimised for containment, recovery and claim management: evidential preservation for future litigation is nobody's default mandate: the gap this section closes.
- **State the preservation mandate:** the IR engagement instructed, in writing, to preserve per §3 alongside response: images retained (and owned by the organisation, not the vendor), log exports delivered, actions documented: the §11 wording exists for this letter.
- **Privilege structured early:** the investigation run under legal direction where litigation is realistically in contemplation (guide 98 §7, guide 91's dominant-purpose lessons): with the honest caution that dual-purpose incident reports have fared badly, so the structure is real, not cosmetic: separate workstreams where the facts support them.
- **Custody and access agreed:** who holds the images, who may examine them, what the IR firm's report will and will not cover, and how the organisation's own forensic adviser plugs in: settled at engagement, not discovered at disclosure.
- **The organisation keeps its own record:** the §3 incident log and preservation inventory maintained by the client side regardless of vendors: the estate's map in the owner's hands when the panel rotates off.

§ 0 6 · THE CLOCKS

The legal audiences and their clocks: ICO, regulators, subjects, courts

- **The ICO's 72 hours:** personal-data breaches notifiable to the ICO without undue delay and within 72 hours of awareness where risk thresholds are met: with staged notification (initial report, supplementary detail) expressly available: the preserved §4 evidence is what turns the report from speculation into assessment, and the exfiltration analysis is its core.
- **Data subjects:** high-risk breaches notified to affected individuals without undue delay: scope and content driven by what the exfiltration evidence actually shows: over-notification and under-notification both carry costs, and the evidence arbitrates.
- **Sector and market regulators:** FCA-regulated firms' notification duties, NIS-regime obligations for relevant operators, listed-company disclosure considerations: mapped per client, served from the same preserved facts.
- **Law enforcement and sanctions:** Action Fraud and NCSC engagement; ransom-payment decisions taken under advice with sanctions screening (attacker attribution against designated entities): the payment question is legal and strategic, and the preserved ransom artefacts inform it.
- **The preservation duty proper:** litigation contemplation (supplier claims, subject actions, insurance disputes) engages PD 57AD's preservation duty over the incident estate itself: hold notices covering the response's records, per guide 95 §6: the incident is a disclosure event in waiting.

§ 0 7 · THE LONG TAIL

From incident to litigation: the uses the estate must support

- **Insurance recovery:** policy-period and dwell-time evidence, impact quantification, mitigation documentation: the claim proved from images and logs, and the coverage dispute (late notification, condition compliance, war and sanctions exclusions) fought on the same record.
- **Supplier and vendor claims:** the entry-phase evidence (§4) grounding claims against the MSP whose credentials were abused, the software whose vulnerability was unpatched, the vendor whose connection was the route: contractual and negligence theories, built on preserved specifics.
- **Defending subject claims and group actions:** the exfiltration analysis bounding what happened to whom; the response record evidencing reasonableness; the security posture documented before-and-after: the defence file the §3 discipline creates.
- **Regulatory follow-through:** ICO investigations tested against the preserved narrative; undertakings and remediation evidenced: the difference between an assessed incident and an unanswerable one, priced in penalties.
- **The disclosure exercise itself:** when proceedings come, the incident estate enters this series' machinery: preserved sources, documented chain of custody, guide 96 timelines and CPR Part 35 reporting: the incident litigated like any other matter, because the evidence was kept like any other matter's.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: incident evidence is layered, and the layers fail differently: which is the preservation plan's organising fact. The endpoint layer (disk images, memory, the encrypted estate) is richest and most fragile: recovery destroys it first. The identity and platform layer (sign-in logs, cloud audit trails per guides 51-58 and 105) survives reimaging but sits on rolling retention. The network layer (firewall, VPN, proxy, DNS) sees movement and egress independently of compromised hosts: the attacker can clear a server's logs but not the firewall's memory of its connections. The security-tooling layer (EDR telemetry, email-gateway records, backup-system logs) holds detections and touches with its own clocks. The external layer: the attacker's infrastructure as seen in threat intelligence, the leak site's postings, the ransom portal, counterparty and provider records: lies beyond the estate and beyond the attacker's cleanup. When one layer is lost: logs cleared (guide 110), endpoints wiped by response, retention expired: the map names the survivors: exfiltration proved from network egress when the staging host is gone; dwell time from identity logs when the entry server was rebuilt; impact from backup-system records when the encrypted estate was restored over. Redundancy is the incident investigator's whole method; §3 exists to preserve enough layers for it to work.

QUESTION	ENDPOINT LAYER	IDENTITY / PLATFORM LOGS	NETWORK LAYER	SECURITY TOOLING	EXTERNAL LAYER	ATTACKER-CLEARED / LOST
How they got in	Y: entry artefacts	First anomalous sign-ins	Inbound connections	Y: gateway + EDR detections	Phishing infrastructure	Survivors: gateway + network
How long they stayed	Tool + persistence dates	Y: the dwell-time spine	Session patterns	Detection history	Infrastructure age	Identity logs usually survive
What they took	Staging archives	Access + download trails	Y: egress volumes + destinations	DLP alerts	Leak-site postings	Network layer answers
What they broke	Y: encryption + deletion	Admin-action logs	n/a	Backup-system records	Ransom communications	Backup logs answer
Who they were	Tool signatures	Source IPs + patterns	Infrastructure links	Strain identification	Y: intelligence + portal	External layer persists

Fallback strategy in one line: preserve at least three layers in hour one: endpoint samples, the log estate, the network record: and when the attacker or the recovery erases one, prove the phase from the survivors.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE 72-HOUR REPORT WRITTEN FROM EVIDENCE

A distributor's estate was encrypted overnight. The response ran both tracks from hour one: containment isolated by disconnection, and the §3 preservation ran in parallel: memory and images from patient-zero candidates, two encrypted file servers imaged as-is, and the full log harvest before any rebuild. By hour 60 the exfiltration analysis had its answer: staging archives assembled but egress logs showing the transfer interrupted at 4% by the containment: and the ICO's 72-hour report stated assessed facts with supplementary detail promised and delivered. Subject notification was scoped to the archive's actual contents; the insurer's dwell-time question was answered from identity logs (nine days); and the follow-up ICO correspondence closed in one round. The counterfactual organisation: reimaged by dawn: files the same report as informed guesswork and spends a year defending it.

EXAMPLE 2 · THE REBUILD THAT ERASED THE SUPPLIER CLAIM

A manufacturer traced its ransomware entry, informally, to its managed-service provider's remote-access tooling: then rebuilt everything in a fortnight of heroic recovery: the jump server reimaged, VPN logs left to rotate out, the MSP's own connection records never requested. When the seven-figure supplier claim was pleaded a year later, the entry phase rested on recollection and one engineer's email. The MSP's defence: intrusion via the manufacturer's own phished credentials: was equally unprovable either way, and the claim settled at a fraction of loss, the litigation risk priced by the missing §4 entry evidence. The preservation letter to the MSP (§11's wording) and one hour of log export would have decided the question; the example is §2's economics in a single case: hours inside the response against the next two years.

EXAMPLE 3 · THE NEGATIVE THAT WAS WORTH PROVING

A professional-services firm suffered an intrusion with a ransom note claiming "all your client files" had been taken: leak-site listing threatened. The preserved estate supported a rare and valuable finding: the negative. Network egress for the dwell window showed volumes inconsistent with bulk exfiltration; the staging behaviour never progressed past enumeration; EDR telemetry bracketed the attacker's access to two departmental shares; and the leak site, monitored through the deadline, posted nothing. The firm notified the ICO with the evidenced assessment, informed the two departments' affected clients precisely, declined payment under advice, and answered the inevitable "how do you know?" from clients and the regulator with the §8 network-layer analysis. Provable non-exfiltration exists only when the logs were harvested in hour one: it cannot be reconstructed later, and it was worth more than everything else the response did.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Reimage first, questions later:** Example 2's fortnight: the estate's story erased by its own recovery.
- **Power pulled on live systems:** memory: tools, keys, sessions: destroyed by the instinctive shutdown: isolation was available.
- **Logs left to rotate:** the hour-one harvest deferred to week two: the network layer's answers expired on schedule.
- **Preservation nobody's mandate:** IR engaged for recovery, evidence assumed: §5's gap, discovered at disclosure.
- **Ransom artefacts lost:** notes deleted with the cleanup, negotiation portals expired unpreserved: attribution and sanctions analysis starved.
- **The incident log kept in heads:** actions and times reconstructed for the regulator months later, inconsistently.
- **Notification from guesswork:** scope asserted without the exfiltration analysis: over-notifying into panic or under-notifying into aggravation.
- **Privilege cosmetics:** a "legal" wrapper over a plainly operational report: guide 91's dominant-purpose lesson, relearned in the incident context.

Technical limitations

- **Attackers clear logs:** guide 110's anti-forensics is standard intrusion tradecraft: which is why §8's independent layers, not any single log, carry the method.
- **Encrypted estates limit reading:** imaged ciphertext preserves the scene but yields content only with keys or flaws: preserved anyway, honestly bounded.
- **Egress proves volume, not always content:** network evidence bounds what left; naming every file needs the staging and platform layers too: the finding graded to its sources.
- **Retention was set before the incident:** the log estate's depth is yesterday's configuration decision: harvested as-is, gaps stated, and the remediation lesson recorded.
- **Attribution is probabilistic:** strain and infrastructure indicate groups, not names in the dock: stated at intelligence grade, with sanctions screening run on what is supportable.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client (in the first hours)

- What has already been rebuilt, restored or wiped: so the preserved and lost layers are known before anyone promises findings?
- Which systems can be imaged now, and which logs export today: the §3 list, actioned against the retention clocks?
- When did awareness begin for the 72-hour clock, and who is drafting the ICO position from the evidence?

Ask the IR firm / insurer panel

- Please confirm that forensic images, memory captures and log exports made during the response will be preserved, inventoried and delivered to our client, and that no compromised system will be reimaged before preservation per the agreed protocol.
- Please provide the running incident log and identify all response actions taken to date that may have altered evidential state.
- Please confirm the scope of your report, its intended recipients, and the basis on which it is prepared, so privilege structure can be settled now.

Ask third parties (suppliers, MSPs, providers)

- Please preserve immediately all logs and records of connections to our client's systems for [period], including remote-access, authentication and support-session records, pending investigation of the incident of [date].

SUGGESTED WORDING · PRESERVATION MANDATE FOR THE IR ENGAGEMENT

> "In performing incident-response services, the provider shall, in parallel with containment and recovery and without unreasonable delay to either: (1) capture volatile data (including memory) from live compromised systems before isolation steps that would destroy it, preferring network isolation to power-off where containment permits; (2) create forensic images of systems designated by the client or its forensic adviser before those systems are reimaged, rebuilt or restored, including representative systems in encrypted state; (3) export and preserve the log sources listed in Schedule 1 [firewall, VPN, proxy, identity provider, cloud platform, EDR, email gateway, backup systems] as at the earliest practicable time; (4) preserve all ransom communications and artefacts; (5) maintain a contemporaneous log of response actions; and (6) deliver all preserved materials, with chain-of-custody records, to the client or its nominated forensic adviser. All preserved materials are the client's property. This preservation mandate forms part of the engagement and is not subordinate to recovery objectives."

§ 1 2 · QUICK CONTROL

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

The incident-preservation checklist

- ☐ Isolation by disconnection where containment permits; no reflex power-offs
- ☐ Volatile captures from live compromised systems first
- ☐ Representative systems imaged before rebuild, encrypted state included
- ☐ Log estate exported hour one across all §3 sources
- ☐ Backup-system records preserved; attacker touches documented
- ☐ Ransom artefacts captured forensically; advice taken on engagement
- ☐ Incident log contemporaneous; preservation inventory maintained
- ☐ IR engagement carries the §11 preservation mandate in writing
- ☐ Privilege structure settled early and honestly
- ☐ ICO position drafted from evidence; staged notification used properly

Red flags

- Recovery proceeding with no preservation inventory: Example 2 in progress.
- Compromised systems powered off "to be safe".
- Log retention shorter than plausible dwell time.
- IR reports drafted for everyone and privileged for no one.
- Notification scope asserted without exfiltration analysis.
- Ransom deadlines approaching with artefacts unpreserved.
- Supplier-route suspicions with no preservation letter sent: §11's third-party wording, unused.

When to involve a digital forensic expert

In the first hours, alongside the IR firm: the preservation mandate designed and executed while the estate still holds its story (§3), and the client's own adviser ensuring §5's gap stays closed; through assessment, where the §4 map is built to notification and insurance standard: Example 3's provable negative is hour-one work: and into the long tail, where supplier claims, coverage disputes, subject actions and regulatory follow-through are evidenced under CPR Part 35 from the preserved estate. Through **cflab.uk** and **e-discovery.uk**, incident evidence runs from live-response preservation to litigation disclosure as one chain of custody: and the first hours are the only ones in which that chain can begin.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Won't preservation slow down our recovery when every hour of downtime costs money?

Marginally and in parallel, not serially: imaging designated systems and exporting logs runs alongside containment, and the §3 ordering exists precisely to avoid gating the rebuild: hours of examiner work against Example 2's two-year alternative. The expensive version of preservation is the one attempted retrospectively.

Should we pay the ransom, and does forensics bear on it?

That is a legal-strategic decision taken under advice: sanctions screening on the attribution evidence, insurer position, data-recovery realities and leak-site risk all feed it: and the preserved artefacts (strain, communications, exfiltration analysis) are its factual inputs: Example 3's firm declined from an evidenced position. Forensics does not make the call; it makes the call informed.

How can we possibly know within 72 hours what data was affected?

Often only partially: which the regime anticipates: the initial report states what is assessed, staged supplementation follows the analysis, and the §3-preserved logs are what let the assessment converge quickly: Example 1's hour-60 answer. What the clock punishes is not incomplete knowledge but unassessed assertion.

The attackers cleared the server logs. Is the investigation over?

No: log-clearing is expected tradecraft and §8's whole design answers it: the network layer, identity provider, EDR telemetry, backup systems and external sources each hold independent copies of phases the attacker could not reach: and the clearing itself, documented per guide 110, is evidence. Single-source dependence is the vulnerability; the layered harvest is the cure.

Our insurer's IR firm is handling everything. Do we need our own forensic adviser?

For evidence, prudently yes: the panel's mandate is containment, recovery and the claim, and §5's preservation gap is structural, not a criticism: your adviser states the mandate, takes custody of the preserved estate, and serves the audiences the panel does not: supplier claims, subject-action defence, the eventual disclosure exercise. One estate, two mandates, both staffed.

Can we prove data was NOT taken?

Sometimes, and it is precious when possible: bounded egress volumes, bracketed access, absent staging progression and a silent leak site: Example 3's finding: supportable only where the network and platform layers were harvested in hour one. The negative cannot be reconstructed later: it is the single best argument for treating §3 as non-negotiable.

§ 14 · REFERENCE

Glossary

Dwell time
The period between intrusion and discovery or eviction.

EDR telemetry
Endpoint detection records of processes, tools and touches.

Egress analysis
Outbound-volume and destination evidence of exfiltration.

Encrypted-state image
A forensic copy of a system as the ransomware left it.

Incident log
The contemporaneous record of response actions and times.

Isolation by disconnection
Containment preserving memory that power-off destroys.

Patient zero
The first compromised system: the entry phase's richest source.

Preservation mandate
The written instruction making evidence a response objective.

Staging archive
Data bundled by the attacker pending exfiltration.

Volatile data
Memory and live state lost at shutdown.

Sources and authoritative references

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

- cflab.uk, digital forensics services (incident evidence preservation, intrusion reconstruction, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 07 · Analysis (holds, log harvests and incident timelines as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- ICO, personal data breach reporting and UK GDPR guidance: ico.org.uk, report a breach · ico.org.uk, UK GDPR
- NCSC, incident management guidance: ncsc.gov.uk, incident management · Action Fraud: actionfraud.police.uk
- PD 57AD (preservation duties): justice.gov.uk, PD 57AD · CPR Part 35: justice.gov.uk, Part 35 · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Incident work at the laboratory runs the two mandates as one engagement: in the first hours, preservation alongside the IR firm's containment: volatile captures, designated images including encrypted state, the hour-one log harvest, and the §11 mandate put in writing before anything is rebuilt; through assessment, the §4 map built to the standard the 72-hour clock, the insurer and Example 3's provable negative each demand; and into the long tail, where the preserved estate: inventoried, chain-of-custody complete: serves supplier claims, coverage disputes, subject-action defence and the eventual disclosure exercise under CPR Part 35. The same-day response line exists for exactly this guide's subject. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if the incident is live now, the order of operations is §3's: disconnect rather than power off, image before reimaging, and harvest the logs this hour: the estate is still telling its story, and it only tells it once.

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