COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Citrix, VDI and Remote Desktop: Where the Evidence Actually Resides

Session Hosts, Golden Images, Profile Stores and the Endpoint That Holds Almost Nothing

In remote-desktop and virtual-desktop estates, the computer on the desk is a window, not a workplace: the actual work happens on session hosts and virtual desktops in a data centre, the user's files and settings live in profile stores, and the desktop itself may be rebuilt from a pristine golden image at every logoff, discarding its traces nightly by design. Parties routinely image the laptop and find nothing, or image "the desktop" and find a machine born yesterday. This guide maps where evidence actually resides in Citrix, RDS and VDI environments: hosts, profiles, redirected folders, gateway and broker logs, and the thin trace the endpoint does keep: and how to preserve and collect each before the architecture's own hygiene erases it.

⏱ Estimated reading time: 27 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. Virtual-desktop estates appear in its casework wherever regulated and distributed workforces do: banks, insurers, outsourcers, call centres: with collection running across session hosts, profile stores and broker logs rather than the endpoints that first get offered. Its eDiscovery arm, **e-discovery.uk**, integrates VDI-derived sources into disclosure-scale processing.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | VDI & SESSION-HOST COLLECTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: FOLLOW THE SESSION, NOT THE SCREEN

In remote and virtual desktop computing, the user's keyboard and screen are in one place and their computer is in another. A thin client, laptop or home PC connects through a gateway to a session: on a shared Remote Desktop Services or Citrix session host serving many users at once, or on a personal virtual desktop (VDI) that may be **persistent** (the same machine every day, accumulating history like any computer) or **non-persistent** (rebuilt from a pristine golden image at every logoff, discarding all local change by design). The user's files, settings and much of their artefact trail are deliberately moved out of the desktop into **profile stores and redirected folders** on file servers, precisely so the desktop can be disposable: and those stores, being server shares, carry the whole of guide 43's three layers: content, snapshots, permissions and logs. Around every session sits the **connection record**: broker and gateway logs binding user, time, endpoint address and assigned host together: the attribution spine of the estate. The evidential consequences are mechanical. Imaging the physical endpoint yields a window's residue: client software traces, connection history, sometimes cached credentials and redirected-device records: valuable for proving who connected from where, nearly useless for what they did. Imaging a non-persistent desktop yields a machine born at last logoff. The evidence lives in the session hosts (for persistent estates and shared hosts), the profile and redirection stores (for the user's world), the brokers and gateways (for the who-when-from-where), and the file servers, mail systems and applications behind them (for the work itself): and the preservation letter must name each, because non-persistence is deletion on a nightly schedule that no litigation hold reaches by accident.

- **First question, always: persistent or non-persistent?** It determines whether "the desktop" is an evidence source or a fresh rebuild, and therefore where every other question goes.
- **Profile stores are the user's real hard drive:** roaming profiles, profile containers (FSLogix and equivalents: per-user virtual disks holding the entire profile), and redirected Documents/Desktop folders: collected as server sources with guide 43 disciplines, snapshots included.
- **Broker and gateway logs are the estate's logbook:** who launched what, when, from which address and device, to which host: preserved early, because rotation is short and the attribution chain runs through them.
- **Shared session hosts multiply the attribution care:** many users on one Windows machine means artefacts interleave; per-user profile separation and session-ID correlation do the untangling, and reports must show the work.
- **Client-side redirection is the exfiltration seam:** mapped local drives, clipboard and USB redirection let session content reach the endpoint; policies say what was possible, session logs say what was configured, and the endpoint says what arrived.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: imaging the window

A bank suspects a departed analyst of taking client data. Its solicitors demand his laptop; the laptop is imaged at cost and examined at length; it contains a Citrix client, a VPN, and essentially nothing else, because the bank's own architecture ensured work never touched it. Meanwhile the estate's real records: his virtual desktop (non-persistent, rebuilt nightly, now indistinguishable from anyone's), his profile container (holding his actual desktop, recent files and browser trail), the broker logs (every session, every source address, including three at 02:00 from a residential IP the week he resigned), and the file-server audit behind the sessions: sit unpreserved, aging on rotation schedules, because everyone was looking at the window.

The reflex this guide installs is architectural: when a matter touches a remote-desktop estate, the first document is not an imaging request but a map: which architecture, persistent or not, where profiles live, what the brokers log and for how long, what redirection policies allowed. Ten minutes with the estate's administrator answers all of it, and the preservation letter then lands on the places that hold evidence rather than the places that hold glass.

§ 0 3 · THE ESTATES

The architectures in plain English: RDS, Citrix, VDI

- **Remote Desktop Services (RDS):** Microsoft's shared-host model: many users log into the same Windows Server session hosts, each in their own session and profile. Evidence: the hosts themselves (guide 41 artefacts, per-user), the profile store, and the RDS licensing, broker and gateway logs.
- **Citrix (Virtual Apps and Desktops):** the same shared-host pattern, and/or published individual apps rather than whole desktops, with Citrix's own delivery machinery: StoreFront/Workspace, Delivery Controllers (brokering), Citrix Gateway (external access), and rich session logging and monitoring databases which, where deployed, record session timelines in unusual detail.
- **VDI (personal virtual desktops):** each user gets their own Windows VM: Citrix, VMware Horizon, Azure Virtual Desktop and peers: persistent or non-persistent per pool. Everything in guide 45 applies to these desktops as VMs: snapshots, hypervisor logs, backup catalogues: layered under everything in this guide.
- **Cloud PC variants:** Azure Virtual Desktop and Windows 365 move hosts and brokering into Microsoft's cloud: the same map, with platform sign-in and diagnostic logs playing the broker-log role and platform retention schedules setting the preservation clock.
- **Mixed estates are normal:** published apps for most staff, persistent VDI for executives, RDS for the call centre: the data map records which population the custodian belonged to before anything is requested.

§ 0 4 · THE DECIDING QUESTION

Persistent versus non-persistent: the question that decides everything

- **Persistent desktops accumulate:** the same VM serves the user daily; guide 41's artefact families build up exactly as on a physical machine; and guide 45's chain, backup and hypervisor layers preserve its history. Collection: acquire the VM whole-chain, plus profile store and logs.
- **Non-persistent desktops forget:** at logoff the machine reverts to the golden image; local artefacts of the session are discarded by design. What survives is what the architecture externalised: the profile container (which, on FSLogix-style deployments, quietly preserves much of what a physical machine would hold: registry hive, recents, browser data), redirected folders, application servers, and the logging layers. Collection: the stores and logs, not the desktop; plus, where a session is live or recently ended, the fleeting chance to capture the current machine before revert: a same-day decision, per guide 33's clock.
- **The golden image is evidence too:** it defines what every desktop contained at birth (installed tools, policies, agents): the baseline against which "how did that get there?" is answered, and occasionally the finding itself (the monitoring agent present, the control absent).
- **Ask the pool, not the user:** users rarely know which kind they have; the pool configuration answers, and the preservation letter differs accordingly: suspend revert/refresh on a specific desktop where a live state matters, versus proceed straight to stores and logs where nightly hygiene has already run for months.

§ 0 5 · THE USER'S REAL HARD DRIVE

Where the user's world actually lives: profiles and redirection

- **Profile containers (FSLogix and kin):** per-user virtual disks (VHD/VHDX on a share) mounted at logon, holding the whole profile: registry hive, AppData, browser profiles, Office caches, recent items. Forensically they are small user-centric disk images: collected from the share (with the share's snapshots supplying history), mounted read-only, and examined with guide 41's toolkit. In non-persistent estates they are, for most questions, *the* user machine.
- **Roaming profiles and redirected folders:** older and parallel patterns putting the profile and the visible folders (Documents, Desktop, Downloads) on file shares: guide 43 sources in every respect: content, previous versions, audit where enabled.
- **What lands where is policy-defined:** exclusion lists trim what profiles capture; the estate's profile policy is exported as an exhibit so the report can say what the container should hold and account for what it does not.
- **Application servers hold the work itself:** in published-app and session estates, documents live in DMS, mail in Exchange, data in databases: the session was only ever a viewport; the substantive disclosure sources are those systems, reached through this series' other guides.

§ 0 6 · THE LOGBOOK

The connection record: brokers, gateways and session logs

- **Brokers bind the session together:** Delivery Controllers, RDS Connection Brokers and their cloud equivalents log each launch: user, time, endpoint name and address, assigned host or desktop, session duration, disconnects and reconnects: the record that converts "someone did X on host Y" into "this account's session, from this device, occupied host Y then".
- **Gateways record the outside:** external access concentrates at Citrix Gateway, RD Gateway or the platform's front door: source IPs, times, authentication outcomes, failed attempts: the estate's border log, and the first place unusual-hours and unusual-geography stories appear.
- **Monitoring databases add texture where deployed:** Citrix's monitoring service and equivalents retain session timelines, application launches and endpoint details in a queryable store with longer memory than raw logs: worth asking for by name.
- **Session policies are part of the record:** what redirection (drives, clipboard, USB, printing) was permitted per group, session recording if any, idle and logoff behaviour: exported with the logs, because possibility framing (guide 43's map-of-possibility) depends on it.
- **Rotation is short; preservation is urgent:** broker and gateway logs commonly reach back weeks by default; the day-one letter names them, and the monitoring database where one exists.

§ 0 7 · THE THIN TRACE

What the endpoint does keep

- **Client connection history:** the Citrix/RDP/Workspace client's recent connections, cached configuration and log files: which estates, which stores, when: on personal devices, often the proof that a home PC was used for work access at all.
- **Session residue:** bitmap and glyph caches (RDP) occasionally preserving screen fragments; client logs of drive and device mappings; downloaded-through-redirection files in local folders with their guide 41 metadata.
- **The exfiltration landing zone:** where drive or clipboard redirection was allowed, the endpoint's own artefacts (recents, shellbags, USB history) record what crossed from the session to local storage and onward: the seam where session evidence and endpoint evidence meet, examined together.
- **Attribution corroboration:** the endpoint's presence records (its own logons, network joins, its address matching the broker log's entry) close the four-link chain from the client side: the reason the window is still worth imaging, just never first and never alone.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the desktop, or the endpoint, in isolation. A remote-desktop estate distributes one user's evidence across: the session hosts or personal desktops (as VMs, with guide 45's chains and catalogues beneath them); the golden image and pool configuration; the profile store and its share snapshots; redirected-folder servers; broker, gateway and monitoring databases; the identity provider (sign-in logs, MFA records: often the longest-retained access trail of all); the application and file servers behind the sessions; backup platforms covering hosts and stores; session recordings where policy made them; and the physical endpoints with their thin but corroborating trace. When the primary source is unavailable: the desktop reverted, the host rebuilt, the logs rotated: these paths are the recovery plan, and several usually still hold what the desktop forgot.

EVIDENCE	DESKTOP / HOST	PROFILE STORE	BROKER / GATEWAY LOGS	IDENTITY PROVIDER	ENDPOINT	DELETED / RECOVERABLE
User files and documents	Persistent: Y; non-persistent: n/a	Y (plus redirected folders)	n/a	n/a	Only if redirected out	Store snapshots and backups: often
User activity artefacts	Persistent: Y; shared host: per-profile	Y (container hive, recents, browser)	Session frame only	Sign-in trail	Client history	Container snapshots: varies
Who / when / from where	Host event logs	n/a	Y (the spine)	Y (long retention)	Y (corroborating)	Log rotation limits
Data leaving the session	Redirection events, host logs	Download traces in profile	Policy and mapping records	n/a	Y (landing artefacts)	Varies
Session content (screen)	n/a after logoff	n/a	Recording where enabled	n/a	Cache fragments: limited	Recordings per retention

Fallback strategy in one line: when the desktop has reverted, work outward in this order: profile container (the user's world), broker and identity logs (the who-when-where), application and file servers (the work), endpoint (the corroboration and the landing zone): and check the backup catalogue for the host or store state that predates the loss.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE EMPTY LAPTOP AND THE FULL PROFILE CONTAINER

An insurer's leaver investigation began, conventionally, with the returned laptop: a thin client in all but name, holding a Workspace client and nothing evidential. The estate map redirected the exercise in an afternoon: his desktop pool was non-persistent, so the desktop was abandoned as a source; his FSLogix container was pulled from the profile share together with three weekly snapshots of it; and mounted read-only it behaved as his computer: browser history showing a personal cloud-storage session on his final Friday, recents and shellbags referencing a folder tree named for the book of business, and the container's own growth that week consistent with staged copies. Broker logs framed the sessions; the personal-cloud provider disclosure, obtained on that platform, completed it. The laptop had been a window; the container was the room.

EXAMPLE 2 · THE 02:00 SESSIONS AND THE BORROWED CREDENTIALS

A fund accused its operations manager of after-hours access to deal records. Gateway and broker logs confirmed sessions at 02:00-02:40 on three nights: his account, a residential IP: apparently conclusive. The four-link discipline kept going: the identity provider's records showed those logons used password-only authentication from a device never seen before, while his habitual pattern was MFA from two known devices; the residential IP resolved, on disclosure from the ISP, to a former colleague's address; and the endpoint trace on that colleague's seized PC held the Citrix client with the fund's store configured and connection timestamps matching. The manager's credentials had been shared months earlier and never changed. The claim re-aimed; the architecture's logbook had identified both the session and the wrong defendant.

EXAMPLE 3 · THE NIGHTLY REVERT AND THE EIGHT-HOUR WINDOW

A call-centre fraud was reported at 16:20: a specific agent, that day, on a non-persistent desktop reverting at logoff. The estate's own hygiene was hours from destroying the primary evidence. The response ran guide 33 at architecture speed: the desktop's pool refresh was suspended for that machine by the administrator on our phoned instruction; the live VM was snapshotted with memory at 17:05, logged; and the session host examination that evening captured the in-session state: the browser tab, the exported file on a redirected drive, the clipboard. By 18:30 the desktop could have been any desktop; because someone knew the revert clock existed, it was instead a complete exhibit. The disciplinary and the prosecution both ran on that hour's work.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Imaging the window:** the endpoint collected first, last and only: §2's founding error.
- **Imaging the reborn desktop:** a non-persistent machine acquired weeks later and reported as if it were the user's history.
- **Profile stores outside the notice:** containers and redirected folders unpreserved while their share snapshots prune.
- **Broker and gateway logs discovered after rotation:** the attribution spine lost to a fortnight's delay.
- **The live-session clock missed:** Example 3's window closed by ordinary logoff because nobody suspended the revert.
- **Shared-host artefacts attributed without session correlation:** forty users' interleaved traces read as one person's.
- **Redirection policy unexported:** exfiltration findings asserted without establishing what the session even permitted.
- **Credential-sharing unconsidered:** Example 2's near-miss; account is not person, in this estate least of all.

Technical limitations

- **Non-persistence is genuine loss:** what a reverted desktop held locally and the profile excluded is gone; the report says so and argues from the surviving layers.
- **Profile exclusions trim the record:** policy-excluded paths (commonly caches, sometimes downloads) never reach the container; the policy export defines the ceiling.
- **Log reach is configuration-dependent:** monitoring databases and SIEM forwarding extend it where deployed; raw broker logs alone are short-memoried.
- **Session recording is the exception:** screen-level evidence exists only where policy created it (regulated functions, some contractors); absence is normal, not sinister.
- **Cloud-hosted estates move the layers:** the same map applies, with provider retention schedules and export mechanisms governing: the cloud guides carry the mechanics.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which architecture served this custodian: RDS, Citrix, VDI, cloud PC: and was their desktop persistent or non-persistent?
- Where do profiles live (container technology, share, snapshot schedule), and what does the profile policy exclude?
- What do brokers, gateways and any monitoring database retain, for how long: and can rotation be suspended today?
- What redirection did this user's policies permit: drives, clipboard, USB, printing?

Ask your opponent

- Please state the desktop architecture applicable to [custodian] in [period], including whether desktops were persistent, and preserve: the assigned desktop or host VMs (with snapshot chains and backups), the user's profile container and redirected folders with all share snapshots, broker, gateway and monitoring records, and applicable session and redirection policies.
- Please provide the session history for [custodian] in [period]: launch times, endpoint identifiers and addresses, assigned hosts, durations.
- If any assigned desktop has been reverted, refreshed or rebuilt since [date], please give particulars of the schedule and of any manual operations.

Ask your eDiscovery / forensic provider

- What does the estate map say, and where will each of our questions actually be answered?
- How will you acquire and examine the profile container, and reconcile it against the exclusion policy?
- Is there a live-session opportunity, and what is the suspend-and-capture plan if so?

SUGGESTED WORDING · DAY-ONE PRESERVATION EMAIL FOR A VDI ESTATE (ADAPT)

> "With immediate effect for [custodians/period]: (1) suspend automatic refresh, revert or rebuild for the desktops assigned to the named users, and take no manual resets; (2) suspend pruning and rotation of: profile-store snapshots, broker and gateway logs, the monitoring database, and backups of session hosts and profile stores; (3) preserve unaltered the named users' profile containers and redirected folders, the current golden image(s) for their pools, and the session and redirection policies applied to them; and (4) export now, and hold, the session history for the named users for [period]. Please confirm each step, identify the retention that applied before suspension, and copy this instruction to any outsourced provider operating the environment."

§ 12 · QUICK CONTROL

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

The VDI / remote desktop checklist

- ☐ Estate mapped before anything is imaged: architecture, persistence, profile technology, log layers, redirection policy
- ☐ Day-one email sent: reverts suspended for named desktops, log rotation and snapshot pruning held, session history exported
- ☐ Live-session opportunities assessed same-day; suspend-and-capture executed where the clock demands
- ☐ Profile containers and redirected folders collected as server sources, with snapshots, per guide 43
- ☐ Persistent desktops acquired as VMs per guide 45, whole-chain
- ☐ Broker, gateway, monitoring and identity-provider records collected as the attribution spine
- ☐ Golden image and policies exported as the baseline exhibits
- ☐ Endpoints imaged for the thin trace and the landing zone, in that supporting role
- ☐ Shared-host findings session-correlated; credential-sharing tested before names are pleaded
- ☐ Report states persistence losses, profile exclusions and log horizons as limitations

Red flags

- An investigation that begins and ends with the endpoint.
- A "user's desktop" image taken from a non-persistent pool weeks on.
- Rotation still running a fortnight into the dispute.
- Session findings with no broker correlation.
- Exfiltration claims with the redirection policy unexamined.
- An opponent offering the laptop and silence about the estate.
- Password-only logons from unknown devices in an MFA estate.

When to involve a digital forensic expert

At the map stage, immediately: the ten-minute architecture conversation reroutes the entire exercise, and the day-one email needs its contents. At any live-session moment, by phone: Example 3's window is measured in hours. At collection, for the container, host and log work this guide distributes across guides 41, 43 and 45's methods. And at analysis, where session correlation, policy reconciliation and credential-sharing tests separate the estate's real story from its plausible one: reported under CPR Part 35 with the architecture explained in terms a court can hold. Against opponents, the review question writes itself: they disclosed the window; where is the room?

§ 13 · COMMON QUESTIONS

Frequently asked questions

The employee only ever used a company laptop. Why isn't imaging it enough?

Because in these estates the laptop is deliberately kept empty: work happens on hosts, files live in profile stores and application servers, and the endpoint holds a client and a connection history. Image it for the corroborating trace and the landing zone, but direct the substantive requests at the session layer: container, hosts, brokers, identity logs. The architecture was designed so the laptop could be lost without losing anything; treat its evidential emptiness as the design working, not the trail ending.

The desktop rebuilds itself every night. Has the evidence been destroyed?

The desktop's local state, yes: nightly, by design, since long before the dispute: which is why no adverse inference attaches to routine non-persistence. The evidence was externalised as it was created: profile container, redirected folders, application servers, logs: and those survive on their own schedules. The urgent act is stopping the schedules (snapshots, logs, and the specific desktop's revert if a recent session matters), not mourning the desktop.

Can these environments show us exactly what the user saw on screen?

Only where session recording was deployed: some regulated functions and third-party-access setups record screens or keystrokes, retained per policy and worth requesting by name. Otherwise screen content is reconstructed inferentially: the application's own records of what was open, the profile's browser and recents trail, redirected-drive artefacts, and occasional client cache fragments. The honest framing is activity evidence rather than footage: usually sufficient, and claimed as nothing more.

How do we prove which person was behind a session, rather than which account?

The four links, with this estate's rich middle: broker logs bind account, time, endpoint identifier and address; the identity provider adds authentication method and device familiarity; the endpoint's own artefacts place a machine and often a person; and pattern evidence (habitual hours, devices, geographies) frames anomalies. Example 2 is the caution: the logbook is excellent at identifying sessions and neutral about who typed: the report keeps those separate and builds the human layer explicitly.

Work happened through published apps, not a desktop. What changes?

The desktop layer thins to almost nothing and the weight shifts: brokers still log every app launch (which app, when, from where); profiles still capture the app's user-side traces; and the substantive evidence concentrates in the application's own backend: the DMS, the finance system, the database: reached through this series' application and database guides. The request list changes shape; the follow-the-session principle does not.

Our opponent runs Citrix and says session data "is not retained". How do we test that?

Decompose it in correspondence: retention of what, where, since when: broker logs, gateway logs, the monitoring database (whose default reach is months, not days), identity-provider sign-ins (often a year or more), profile-store snapshots, host backups, SIEM forwarding. Blanket non-retention across all of those is an unusual estate and, if genuinely configured, was a choice with a date: which is itself disclosable. The §11 request names the layers individually precisely so that "not retained" has to be said, or not, about each.

§ 14 · REFERENCE

Glossary

Broker
The service assigning users to hosts/desktops and logging each session's frame.

Golden image
The pristine template from which non-persistent desktops are rebuilt.

Gateway
The external-access front door; source addresses and authentication outcomes.

Monitoring database
Citrix-style session-history store with longer memory than raw logs.

Non-persistent desktop
A VM reverted to the golden image at logoff; local change discarded by design.

Profile container
Per-user virtual disk (FSLogix and kin) holding the whole profile; the user's real hard drive.

Published app
A single application delivered remotely without a full desktop.

Redirection
Session-to-endpoint mapping of drives, clipboard, USB, printers; the exfiltration seam.

Session host
A shared server running many users' sessions (RDS/Citrix).

Thin client
An endpoint that is only a window; minimal local evidence by design.

VDI
Per-user virtual desktops, persistent or non-persistent, on a hypervisor or cloud platform.

Sources and authoritative references

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

- cflab.uk, digital forensics services (VDI and session-host collection, profile-container examination, attribution analysis, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (estate mapping and layered preservation at disclosure scale; "defensibility is built, not retrofitted"): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance · ISO/IEC 27037:2012: iso.org, 27037
- CPR Part 31 / PD 57AD (preservation and cooperation) and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- ICO, UK GDPR guidance (including employee monitoring): ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

VDI matters start at the laboratory with the map: the architecture conversation with your client's (or the outsourcer's) administrators, the day-one email that suspends reverts and rotation, and the same-day judgment on live-session capture. Collection then runs layer by layer with this series' methods: profile containers mounted and examined as user machines, persistent desktops acquired whole-chain, brokers, gateways, monitoring and identity records assembled into the attribution spine, endpoints imaged for the trace and the landing zone: reported under CPR Part 35 with the estate explained plainly and its losses and horizons stated. Against opponents, we review window-only disclosure for what the room must still hold. Through **e-discovery.uk**, estate-derived sources flow into disclosure-scale processing beside every other system. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a session is live or a revert is pending, call before the clock does its work.

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