COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Virtual Machines as Evidence

VMware, Hyper-V, Snapshots, Virtual Disks and the Recovery of Historical States

Most corporate servers are no longer physical machines: they are files. A virtual machine's entire existence: its disk, its memory, its configuration: lives as a handful of files on a hypervisor, which makes VMs simultaneously the easiest systems to acquire perfectly and the easiest to delete, copy, hide or roll back without trace on the guest itself. Snapshots preserve whole historical states; deleted VMs can survive on datastores and in backups; and an unauthorised VM can be a concealed second computer inside a laptop. This guide explains how virtual machines are collected and examined, how their snapshot and backup layers recover the past, what the hypervisor logs about their lifecycle, and where else their evidence lives when the VM itself is gone.

⏱ 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. Virtualised estates are standing work: hypervisor-level acquisition of production servers, snapshot-chain examination, recovery of deleted guests from datastores and backups, and the concealed-VM findings that fraud matters produce. Its eDiscovery arm, **e-discovery.uk**, processes VM-derived collections at disclosure scale.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | HYPERVISOR & VM ACQUISITION | DELETED DATA RECOVERY | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: A PERFECT COPY IS ONE FILE OPERATION AWAY, AND SO IS A PERFECT DISAPPEARANCE

Virtualisation turns computers into portable files, and that cuts both ways for evidence. In your favour: a VM can be acquired completely and non-disruptively: a hypervisor snapshot freezes the running machine, and copying its virtual disk files yields exactly the image that days of physical acquisition would produce, hashed and mounted in the laboratory like any disk, with the whole of guide 41 and 42's artefact examination available inside the guest. Snapshot chains and VM-aware backups preserve entire historical states of the machine: not file versions but the whole computer as it stood on a given day, bootable in an isolated laboratory environment where the disputed system can be operated, demonstrated and interrogated as it then was. Against you: the same portability serves concealment: a VM is deleted in seconds, rolled back to erase a period of activity (the guest's own logs vanish with the rollback, while the hypervisor's do not), copied onto a portable drive as a complete working system, or run covertly inside an ordinary laptop as a second computer whose activity leaves little trace on the host. The examiner's response is to work one level down: the hypervisor's datastores, logs and inventory record VM lifecycles: creation, snapshots, rollbacks, deletions, copies, per administrator account with timestamps: and deleted guests frequently survive on datastores and in backup catalogues. The lawyer's contribution is scoping and speed: name the VMs, their snapshot and backup layers, and the hypervisor's management logs in every preservation notice, and suspend the retention schedules before they prune the states that matter.

- **VM acquisition is often the easy, proportionate route to a server:** snapshot-and-copy from the hypervisor beats imaging physical iron on speed, disruption and completeness: guide 43's snapshot preference, formalised.
- **Snapshots are whole-machine time travel:** a snapshot chain holds the system at multiple past moments; the disputed database, the pre-tampering configuration, the mailbox server the week of the events: bootable and examinable.
- **Rollback is the virtual anti-forensic:** reverting a VM erases the guest-side record of the interval; detection lives in the hypervisor logs, snapshot metadata and the mismatch between guest time and world time.
- **Deleted VMs are files deleted from big disks:** datastore free space, orphaned disk files, backup catalogues and replication targets recover them more often than opponents expect.
- **Desktop virtualisation is the concealment pattern:** VirtualBox/VMware on a personal laptop hosting a hidden working environment (or a VeraCrypt container holding the VM) is a recurring fraud finding: host artefacts (guide 41's execution and file records) betray its existence even when the VM itself is encrypted or gone.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the computer that is a file

Ask where the finance server is, and in most companies the true answer is: it is three files on a storage array, executed by a hypervisor that runs forty such computers on four physical boxes. Nothing about the server's evidential richness changes: inside its virtual disk are the same Windows artefacts, databases and documents as ever: but everything about its handling does. It can be frozen mid-operation without downtime; copied perfectly in minutes; moved between countries over a wire; retired to an archive; or deleted by one administrative action that leaves no trace inside any machine still running. The physical instincts (seize the box, pull the drive) grip nothing: the box runs forty computers, and the drive belongs to all of them.

The examiner's world therefore has two floors. The **guest floor** is the VM's interior: ordinary operating-system forensics on the mounted virtual disk. The **hypervisor floor** is the management layer: datastores, snapshot machinery, inventory and logs: which records what was done to machines: created, snapshotted, reverted, cloned, exported, deleted, by whom, when. Cases about what happened inside a system are argued on the guest floor; cases about what happened to a system: the vanished VM, the rolled-back week, the copied environment: are argued on the hypervisor floor, and parties that only ever look inside guests never see them.

§ 0 3 · ANATOMY

The anatomy of a VM: disks, snapshots, memory, configuration

- **Virtual disks** (VMDK for VMware, VHD/VHDX for Hyper-V, VDI for VirtualBox, QCOW2 for KVM): the machine's storage as files; mounted read-only in the laboratory they are the disk image, with every guest artefact inside. Thin-provisioned disks grow with use, and their growth history is itself informative.
- **Snapshot/checkpoint files:** a snapshot freezes the disk state and diverts subsequent writes to delta files; the chain of deltas encodes the machine's states at each snapshot moment, each reconstructable. Snapshot metadata records names, timestamps and (in managed environments) the creating account: administrators name snapshots candidly ("before clean-up", "pre-audit"), and those names become exhibits.
- **Memory files:** suspended VMs and memory-inclusive snapshots write the guest's RAM to disk: passwords, keys, open documents and running processes, preserved involuntarily: guide 33's volatile evidence, captured by the platform itself.
- **Configuration files:** the VM's hardware story: attached disks (including ones since removed), network connections, USB passthrough history on desktop products, and names and paths that survive in host records after deletion.
- **Guest time versus host time:** VMs take time from hosts but can drift or be deliberately skewed: and a guest booted from an old snapshot lives in the past until synchronised. Timestamp arguments from inside VMs are made with the virtualisation layer's clock behaviour established, or not at all: this series' clock discipline, one floor up.

§ 0 4 · ACQUISITION

Acquiring virtual machines defensibly

- **The standard route:** hypervisor snapshot at the acquisition moment (freezing a consistent state), forensic copy of the virtual disk files (all members of the snapshot chain, not just the base disk), hashes computed on the datastore side and verified on receipt, exports of the VM's configuration and snapshot metadata alongside: the whole exercise logged in the protocol's terms, with no downtime for the guest.
- **Include the memory where it matters:** for live-state questions (running malware, logged-in sessions, encryption keys), a memory-inclusive snapshot or suspend captures RAM as part of the same operation: decided in the plan, per guide 33.
- **Whole-chain discipline:** copying only the current disk collapses the history; the acquisition manifest lists every disk, delta and memory file, because the chain is the evidence of the past states and of the snapshot activity itself.
- **Scale by the campaign rules:** tens of VMs are collected like any estate: guide 36's protocol, guide 37's targeting (which guests, which chains), guide 40's coordination where hypervisors span sites: with the hypervisor administrators in the supporting, supervised role this series always assigns to IT.
- **Desktop VMs are seized with their hosts:** a VirtualBox machine on a laptop is files inside a guide 41/42 image; the host's acquisition captures it, and the host's artefacts frame it (when run, from where, with what devices attached).

§ 0 5 · TIME TRAVEL

Historical states: snapshot chains, backups and rollback

- **Snapshot chains recover moments:** each snapshot in a chain is a bootable past: the laboratory reconstructs the machine as at each point, mounts or runs it isolated, and differences states to chronicle change: guide 43's differencing, applied to whole computers.
- **VM-aware backups recover eras:** enterprise backup platforms (Veeam and peers) catalogue whole-VM restore points on nightly and weekly schedules reaching months or years: the deep archive from which deleted guests and pre-dispute states return. The catalogue itself is evidence: what was backed up, when jobs changed, which VM quietly left the schedule.
- **Rollback and its shadow:** reverting to a snapshot rewinds the guest: files, logs and all: as if the interval never happened inside the machine. The shadow falls outside: hypervisor task logs record the revert (account, time, snapshot reverted to); snapshot metadata shows creation and deletion patterns; external records (email flows, other systems' logs, backups taken during the erased interval) preserve what the guest no longer knows. A rollback after a preservation duty is spoliation with a timestamped confession one floor up.
- **Running the past, safely:** historical states are operated only in isolated laboratory networks, from copies, with the method recorded: the demonstrative power of "here is the system as it stood that morning, working" is considerable in court, and the safety rules keep it admissible.

§ 0 6 · ONE FLOOR UP

The hypervisor's own record: lifecycle, logs and attribution

- **Management logs are the lifecycle ledger:** vCenter/ESXi, Hyper-V and desktop products log VM operations: create, power, snapshot, revert, clone, export, migrate, delete: with timestamps and, in managed environments, the administrator account: the who-did-what-to-the-machine record no guest can hold.
- **Inventory and datastore records:** registered VMs past and present, orphaned files, datastore browsing history and storage events corroborate the ledger and expose the unregistered and the removed.
- **Attribution runs the familiar chain:** operation → admin account → session/endpoint → person: with the usual small-estate hazard of shared root passwords, answered the usual way (endpoint correlation, per guides 41 and 43).
- **Preserve this floor explicitly:** management logs rotate like all logs; the day-one email (guide 43's, extended) names hypervisor and backup-platform logs, snapshot retention and catalogue data: the sentence that keeps the lifecycle ledger alive.

§ 0 7 · THE CONCEALED AND THE DESTROYED

Hidden and deleted VMs

- **The concealed-VM pattern:** a second operating environment inside an innocent-looking machine: VirtualBox on the accountant's laptop running the parallel books; a VM inside an encrypted container (this series' fraud example); a cloud-hosted guest reached from a clean corporate desktop. Host artefacts betray it: hypervisor software in execution records, VM files (or container files of telling size and entropy), configuration remnants naming machines and disks, and USB/network traces of the guest's activity.
- **Deleted guests, recovered:** deletion removes datastore files, which persist as recoverable data until overwritten (large-file carving on datastores succeeds respectably), while inventory records, logs and configuration remnants prove the machine existed, its name, size and lifetime. Backup catalogues and replication targets then supply the machine itself, whole, from before its death.
- **Existence findings carry weight alone:** proving a VM named "Trading-2" was created in March, snapshotted weekly, exported to a portable drive in September and deleted the day after the audit letter is a case narrative before any interior is examined: the hypervisor floor doing what it does.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the VM in isolation. Its evidence exists across an ecosystem: the hypervisor hosts and their datastores; the management layer (vCenter/System Center and its database of events); VM-aware backup platforms and their catalogues; replication and disaster-recovery targets holding synchronised copies at other sites; exported OVA/OVF archives and clones on portable media; the storage array beneath the datastores (with its own snapshots, per guide 43); identity providers authenticating the administrators; the guests' own external footprints (email through mail systems, transactions in other databases, traffic in network logs): which survive rollback: and, for desktop virtualisation, the host machine's full guide 41/42 artefact record. When the primary source is unavailable: the VM deleted, the chain pruned, the datastore reallocated: these paths are the recovery plan.

EVIDENCE	VM / CHAIN	BACKUP CATALOGUE	REPLICA / EXPORT	HYPERVISOR LOGS	GUEST'S EXTERNAL FOOTPRINT	DELETED / RECOVERABLE
Guest contents (files, artefacts)	Y	Y (restore points)	Y where taken	n/a	Partially (mail, DBs elsewhere)	Datastore carving: varies
Historical states	Snapshot chain	Y (deep reach)	Point-in-time copies	Metadata only	Corroborates intervals	Pruned chains: sometimes in backups
Lifecycle events (create/revert/delete)	Chain metadata	Job history	Sync logs	Y (the ledger)	n/a	Log rotation limits
Rolled-back activity	Erased in guest	Y if job ran in interval	Y if synced in interval	Revert event: Y	Y (external systems kept it)	Varies
Admin attribution	n/a	Y (job operators)	n/a	Y (accounts, sessions)	n/a	Varies

Fallback strategy in one line: when the guest cannot speak, argue from the ledger and the copies: hypervisor and backup-platform records prove the lifecycle, restore points and replicas resurrect the machine, and the guest's external footprint reconstructs the interval a rollback tried to erase.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE ROLLED-BACK WEEK

An operations director, accused of altering stock records, produced the inventory server's logs showing nothing unusual: genuinely nothing, because the guest had been reverted. The hypervisor floor told the fuller story: a snapshot named "temp" created on the 3rd at 22:14 under his admin account, a revert to it on the 9th at 23:02, and the snapshot deleted minutes later: bracketing exactly the week the discrepancies arose. The erased interval was then rebuilt from outside the guest: the nightly backup of the 6th (a restore point inside the vanished week) contained the database mid-alteration, and the ERP's own application logs on a different server recorded his sessions. The guest's clean logs, far from exonerating, became the centrepiece: a machine with a week missing, and a ledger one floor up explaining precisely who removed it.

EXAMPLE 2 · THE COMPANY ON A PORTABLE DRIVE

A departing MD was suspected of taking "the business" with him: nothing appeared in mailbox or file-transfer evidence. The hypervisor logs supplied the mechanism: an export of the finance and CRM guests to OVA archives on a Saturday, under his credentials, followed by datastore browsing to an attached USB volume: the whole company's working systems, portable, in two files. His home laptop (delivered up on that evidence) carried VirtualBox in its execution artefacts and both machines registered in its VM inventory, run repeatedly in the following month; the guests' interiors, examined, showed customer exports created post-departure. The claim was proven not from documents but from machines as objects: copied, carried and run, each step logged by a layer he had not considered.

EXAMPLE 3 · THE DELETED GUEST AND THE BACKUP CATALOGUE

In a joint-venture dispute, the respondent maintained a disputed pricing tool "never existed as a system: it was a spreadsheet". The datastore's orphaned files said otherwise: configuration remnants naming a VM "PriceEngine", carved fragments of its virtual disk, and inventory records of its registration and deletion: the deletion dated three days after the letter before action. The backup platform's catalogue then produced the machine entire: weekly restore points across two years, the latest from the week before deletion, restored and booted in isolation to demonstrate the tool running: its interface, its rules, its authorship metadata. The "spreadsheet" account was abandoned at the CMC; the costs of the concealment attempt were not.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Guest-only thinking:** examining interiors while the lifecycle ledger, snapshot metadata and catalogues go uncollected: the floor where Examples 1-3 were all won.
- **Partial-chain acquisition:** the current disk copied, the deltas and memory files left: history collapsed at the moment of collection.
- **Schedules unsuspended:** snapshot auto-pruning and backup recycling eating past states through the correspondence phase: guide 43's email, unsent one floor up.
- **Timestamps argued without the clock layer:** guest drift, skew and snapshot-boot time travel unexamined.
- **Powering on evidence casually:** booting the actual acquired VM (not an isolated copy) and writing today into the exhibit.
- **Host artefacts ignored in desktop cases:** the concealed VM's existence provable from the laptop, missed because only "documents" were sought.
- **Attribution from shared root:** the hypervisor's one password, everyone's alibi: endpoint correlation skipped.

Technical limitations

- **Chains prune by design:** production estates keep few snapshots; long history lives in backups or nowhere: the reach question is asked of the catalogue, early.
- **Datastore recovery is probabilistic:** deleted-VM carving competes with busy storage reallocation; existence findings (logs, remnants) outlast content recovery.
- **Encrypted guests gate interiors:** a BitLocker'd or FileVault'd guest inside a VM needs its keys like any machine (guide 33); the lifecycle ledger remains readable regardless.
- **Cloud VMs shift the floor:** IaaS guests (Azure/AWS) put the hypervisor layer in the provider's hands: platform logs, disk snapshots and APIs replace datastore access, per this series' cloud guides; the two-floor thinking transfers intact.
- **Rollback detection needs the outside:** where hypervisor logs are gone and no external footprint exists, an expertly executed revert can be genuinely silent: the honest limitation, stated when it applies.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which systems in issue are virtual, on what platform, and who administers it? (The two-floor map, drawn first.)
- What snapshot policies, backup platform and retention apply to the relevant guests: and who can suspend pruning today?
- For desktop concerns: is virtualisation software present on the individual's machines, and do we have their images?

Ask your opponent

- Please preserve, for [named VMs/hosts]: all virtual disk and snapshot files including deltas and memory files; hypervisor and management logs; backup catalogues and restore points; and replication or exported copies: suspending all pruning, recycling and rotation meanwhile.
- Please provide the lifecycle history of [VM]: creation, snapshots, reverts, clones, exports, migrations and deletion, with dates and operating accounts.
- If any VM relevant to the issues has been deleted, reverted or exported since [date], please give particulars: when, by whom, and on whose instruction.

Ask your eDiscovery / forensic provider

- What is the acquisition plan per guest: chain scope, memory inclusion, hash regime, and hypervisor exports?
- How far back do the catalogue and chains actually reach for our questions?
- If we need to demonstrate a historical state, what is the isolated-operation method and its record?

SUGGESTED WORDING · INSTRUCTION FOR A VM EXAMINATION

> "Please acquire from [hypervisor/host] the virtual machines listed in Schedule A, including in each case the complete virtual disk and snapshot chain, memory and suspend files, and configuration files, hashed and manifested; export and preserve the hypervisor and management logs, snapshot metadata and backup catalogue entries relating to those machines; and report on: (1) the lifecycle of each machine (creation, snapshot, revert, clone, export, migration, deletion events, with operating accounts and endpoint correlation so far as available); (2) the guest-level findings within [issues], applying the artefact and attribution disciplines of the relevant operating system; (3) any indications of rollback, deletion or export affecting the period [dates], with reconstruction from backup restore points, replicas and external footprints as required; and (4) clock behaviour at both hypervisor and guest level as it affects any timestamp relied on. Historical states are to be operated only as isolated copies, with the method recorded."

§ 12 · QUICK CONTROL

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

The VM evidence checklist

- ☐ Virtual estate mapped: platforms, hosts, administrators, the guests in issue
- ☐ Day-one preservation extended one floor up: chains, memory files, management logs, catalogues, replicas; schedules suspended
- ☐ Acquisition whole-chain, hashed, manifested; memory captured where live state matters
- ☐ Hypervisor exhibits exported: lifecycle logs, snapshot metadata, inventory, datastore records
- ☐ Guest examination run to the OS guides' disciplines on mounted copies
- ☐ Historical states reconstructed from chains and restore points; differencing applied; operation isolated and recorded
- ☐ Rollback and deletion checked from the ledger and the outside footprint
- ☐ Desktop hosts examined for concealed-VM indicators where relevant
- ☐ Clock behaviour established before timestamp argument
- ☐ Attribution four-linked; shared-root realities faced with endpoint correlation

Red flags

- A guest's logs suspiciously clean across the disputed interval.
- Snapshots named "temp", "before fix" or "old" created and deleted around key dates.
- A VM exported or cloned to portable media near a departure.
- A machine deleted days after a letter before action.
- Backup jobs quietly dropping a guest from the schedule.
- An opponent offering the current VM but silent on chains, catalogues and logs.
- Virtualisation software on a suspect laptop with no innocent explanation.

When to involve a digital forensic expert

At mapping, to draw the two floors and extend day-one preservation to the layer that actually holds the lifecycle; at acquisition, where whole-chain, memory and hypervisor-export discipline decides what exists to examine; at analysis, for the ledger reading, historical-state reconstruction and rollback detection that guests cannot provide about themselves; and at presentation, where an isolated, recorded demonstration of a past state (Example 3's booted machine) is among the most persuasive exhibits digital evidence offers: all under CPR Part 35, limitations stated. Against opponents, the same two-floor review prices guest-only disclosure at its true value: the current machine without its chains, catalogue and logs is a photograph offered in place of the film.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is a copied VM as good as imaging the original server?

For the guest's contents, yes: the virtual disk is the disk, and a hash-verified copy of the full chain is a complete, examinable image acquired without downtime: often better in practice, because snapshot consistency beats imaging a live physical machine. What the copy alone lacks is the management context: which is why acquisition always pairs the chain with the hypervisor's exports, and why "we gave you the VM" is only half an answer to a proper request.

Someone reverted the machine to an old snapshot. Is the interval gone?

Inside the guest, yes; in the estate, usually not. The revert itself is logged one floor up with account and time; backups and replicas taken during the interval preserve the machine mid-period; and the guest's external footprint (mail flows, database writes on other systems, network logs) records what it did while the erased week was live. Example 1 is the pattern: a rollback converts "what happened" into "who erased it and what do the outside records show": frequently a better case than the original.

A VM was deleted before we could act. What are the odds?

Split the question: existence and lifecycle are usually provable regardless (inventory, logs, configuration remnants, catalogue entries survive deletion); content recovery depends on the backup reach (whole restore points are the jackpot, and enterprise estates usually have them) and, failing that, on datastore carving against ongoing reallocation: genuinely time-sensitive. Hence the standing sequence: preservation letter naming catalogues and replicas today, carving assessment this week, and the lifecycle findings meanwhile doing the adverse-inference work.

Can we make the other side disclose hypervisor logs and backup catalogues?

They are documents like any others: within disclosure duties where relevant, and squarely relevant wherever lifecycle events (deletion, rollback, export) are in issue. The practical route is the §11 request: preservation first (rotation is the enemy), then the lifecycle history of named machines with operating accounts, then the catalogue entries: framed so that silence or gaps are themselves informative. Courts grasp the photograph-versus-film point quickly once it is explained; PD 57AD's cooperation machinery does the rest.

The disputed VM runs in Azure/AWS, not on our opponent's own servers. Does the approach change?

The floors persist; the access routes change. The guest is acquired via platform disk-snapshot and export mechanisms; the "hypervisor floor" becomes the provider's control-plane logs (who created, resized, snapshotted, deleted, from which principal), retained on platform schedules that reward early preservation; and catalogues become the platform's backup and replication services. This series' cloud guides carry the mechanics; the strategic instruction transfers verbatim: never accept the machine without its ledger.

We suspect an employee ran a hidden VM on their laptop. What should we ask for?

The laptop's forensic image, examined for the host-side pattern: virtualisation software in execution artefacts (installed or portable), VM files and inventories, large high-entropy container files, and USB/network traces consistent with guest activity: plus any encrypted-volume keys through the guide 33 routes. The finding often available even where the VM is encrypted or deleted is that a concealed environment existed and when it ran: which reframes the whole dispute, and which host artefacts yield to exactly the guide 41/42 examination you would already be instructing.

§ 14 · REFERENCE

Glossary

Chain (snapshot chain)
Base disk plus delta files encoding the machine's states at each snapshot.

Checkpoint
Hyper-V's term for a snapshot.

Datastore
Hypervisor storage holding VM files; the ground where deleted guests are carved.

Delta file
Post-snapshot writes diverted to a new file; history's building block.

Guest / host
The VM and the machine (or hypervisor) running it; two artefact floors.

Lifecycle ledger
Management-layer logs of create/snapshot/revert/clone/export/delete events with accounts.

Memory file
Guest RAM written to disk on suspend or memory-inclusive snapshot.

OVA/OVF export
A portable packaged copy of a VM; the Example 2 mechanism.

Restore point
A whole-VM state in a backup catalogue; the deep archive.

Rollback / revert
Returning a guest to a snapshot, erasing the interval inside it.

Virtual disk
The machine's storage as a file (VMDK, VHDX, VDI, QCOW2); mountable as an image.

Sources and authoritative references

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

- cflab.uk, digital forensics services (hypervisor-level acquisition, snapshot-chain and deleted-VM recovery, concealed-environment findings, 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 (virtual estates preserved and collected at disclosure scale): 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: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Virtualised estates are examined on both floors at the laboratory: whole-chain, memory-inclusive acquisition from hypervisors without downtime; lifecycle-ledger analysis with four-link attribution; historical-state reconstruction from chains and backup catalogues, differenced and, where the matter warrants, operated in isolation for demonstration; deleted-guest recovery from datastores, replicas and restore points; and concealed-VM findings from host artefacts in fraud and exfiltration matters: reported under CPR Part 35 with limitations stated. The day-one preservation letter for a virtual estate (chains, memory files, management logs, catalogues, replicas) can be settled with an examiner today. Through **e-discovery.uk**, VM-derived collections flow into disclosure-scale processing beside every other source. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

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