Virtual Machines As Evidence

Virtual machines present unique challenges and opportunities as evidence in UK litigation. This guide explains their anatomy, defensible acquisition, and the recovery of historical states from snapshots and backups. It also covers hypervisor logs, hidden or deleted VMs, and common mistakes, providing practical questions and a checklist for practitioners.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/virtual-machines-as-evidence

VIRTUALMACHINEEVIDENCE · A GUIDE FOR UK LAWYERS Virtual Machines as Evidence VMware, Hyper-V, Snapshots, Virtual Disks and the Recovery of Historical States COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: APERFECTCOPYISONEFILEOPERATIONAWAY, AND SO IS A PERFECTDISAPPEARANCE

§ 02 · FIRST PRINCIPLES The problem in plain English: the computer that is a file

§ 03 · ANATOMY The anatomy of a VM: disks, snapshots, memory, configuration

§ 04 · ACQUISITION Acquiring virtual machines defensibly

§ 05 · TIMETRAVEL Historical states: snapshot chains, backups and rollback

§ 06 · ONEFLOORUP The hypervisor's own record: lifecycle, logs and attribution

§ 07 · THECONCEALEDANDTHEDESTROYED Hidden and deleted VMs

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE EXTERNAL VM / BACKUP REPLICA / HYPERVISOR DELETED / CHAIN CATALOGUE EXPORT LOGS RECOVERABLE GUEST'S FOOTPRINT

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEROLLED - BACKWEEK EXAMPLE2 · THECOMPANYONAPORTABLEDRIVE EXAMPLE3 · THEDELETEDGUESTANDTHEBACKUPCATALOGUE

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTIONFORAVMEXAMIN AT ION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The VM evidence checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Is a copied VM as good as imaging the original server? Someone reverted the machine to an old snapshot. Is the interval gone? A VM was deleted before we could act. What are the odds? Can we make the other side disclose hypervisor logs and backup catalogues? The disputed VM runs in Azure/AWS, not on our opponent's own servers. Does the approach change? We suspect an employee ran a hidden VM on their laptop. What should we ask for?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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 d own time: 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. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 15 of 18

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 p or table), 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 exam in at i on you would already be instructing. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 16 of 18