Citrix VDI And Remote Desktop Where The Evidence Actually Resides (2)

Understanding where digital evidence resides in Citrix, VDI, and Remote Desktop environments is crucial for UK litigators. This guide details the architectures, persistent versus non-persistent systems, and the actual locations of user data, connection records, and other relevant information, helping practitioners avoid common pitfalls.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/citrix-vdi-and-remote-desktop-where-the-evidence-actually-resides-2

VDI & REMOTEDESKTOPEVIDENCE · A GUIDE FOR UK LAWYERS Citrix, VDI and Remote Desktop: Where the Evidence Actually Resides Session Hosts, Golden Images, Profile Stores and the Endpoint That Holds Almost Nothing COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM VDI & SESSION-HOST COLLECTION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: imaging the window 03 The architectures in plain English: RDS, Citrix, VDI 04 Persistent versus non-persistent: the question that decides everything 05 Where the user's world actually lives: profiles and redirection 06 The connection record: brokers, gateways and session logs 07 What the end point does keep 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: FOLLOWTHESESSION, NOTTHESCREEN

§ 02 · FIRST PRINCIPLES The problem in plain English: imaging the window

§ 03 · THEESTATES The architectures in plain English: RDS, Citrix, VDI

§ 04 · THEDECIDINGQUESTION Persistent versus non-persistent: the question that decides everything

§ 05 · THEUSER ' SREALHARDDRIVE Where the user's world actually lives: profiles and redirection

§ 06 · THELOGBOOK The connection record: brokers, gateways and session logs

§ 07 · THETHINTRACE What the end point does keep

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE GATEWAY END POINT DESKTOP / PROFILE IDENTIT Y DELETED / HOST STORE PROVIDER RECOVERABLE BROKER / LOGS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEEMPTYLAPTOPANDTHEFULLPROFILECONTAINER EXAMPLE2 · THE02: 00SESSIONSANDTHEBORROWEDCREDENTIALS EXAMPLE3 · THENIGHTLYREVERTANDTHEEIGHT - HOURWINDOW

§ 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

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The VDI / remote desktop checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions The employee only ever used a company laptop. Why isn't imaging it enough? The desktop rebuilds itself every night. Has the evidence been destroyed? Can these environments show us exactly what the user saw on screen? How do we prove which person was behind a session, rather than which account? Work happened through published apps, not a desktop. What changes? Our opponent runs Citrix and says session data "is not retained". How do we test that?

§ 14 · REFERENCE Glossary VDI 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

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 end point 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 request in g 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, end point 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