Forensic Collection From Corporate File Servers

Forensic collection from corporate file servers presents unique challenges compared to device imaging. This guide explores how servers record permissions, audit trails, and metadata, and discusses the attribution problem on shared systems. It provides a playbook for collection, common mistakes, and questions to ask.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/forensic-collection-from-corporate-file-servers

FILE SERVER EVIDENCE · A GUIDE FOR UK LAWYERS Forensic Collection from Corporate File Servers Shared Drives, Permissions, Snapshots, Deleted Files and the Attribution Problem COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES SERVER & LIVE-SYSTEM ACQUISITION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: everyone's drive, no one's machine 03 How server collection differs from device imaging 04 What the server records: permissions, audit and metadata 05 Snapshots, previous versions and deleted files 06 Attribution on shared systems 07 The collection playbook 08 Worked examples 09 Common mistakes and technical limitations 10 Questions to ask · Suggested wording 11 Checklist and red flags · When to involve a digital forensic expert 12 Frequently asked questions 13 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: COLLECTTHEFILES, THEHISTORYANDTHECONTEXT, ORTHE COLLECTIONANSWERSNOTHING

§ 02 · FIRST PRINCIPLES The problem in plain English: everyone's drive, no one's machine

§ 03 · THEDIFFERENCESTHATMATTER How server collection differs from device imaging

§ 04 · WHATTHESERVERKNOWS What the server records: permissions, audit and metadata

§ 05 · THEHISTORYLAYER Snapshots, previous versions and deleted files

§ 06 · WHOSE H AND Attribution on shared systems

§ 07 · THEPLAYBOOK The collection playbook

§ 08 · IN THE WILD Worked examples EXAMPLE1 · THEVANISHEDCONTRACTSFOLDER, REBUILTFROMSNAPSHOTS EXAMPLE2 · " MODIFIEDBY " ANDTHEMIGRATIONTHATFOOLEDEVERYONE EXAMPLE3 · THEPRICINGFOLDERFORTYPEOPLECOULDREAD

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

§ 10 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · DAY- ON E PRESERVATION EMAIL TO IT (A DA PTANDSEND TO DAY) SUGGESTED WORDING · INSTRUCTION FOR A SERVER EXAM IN AT I ON

§ 11 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The file-server evidence checklist Red flags When to involve a digital forensic expert 35. Against an opponent, the same literacy runs in reverse: their server-based schedule of sins is tested against

§ 12 · COMMON QUESTIONS Frequently asked questions Can we just have IT export the relevant folders to save cost? The files we need were deleted from the share months ago. Are they gone? Can the server tell us who read a document, not just who changed it? The share lives in SharePoint/OneDrive now. Does this guide still apply? How disruptive is server collection to the business?

§ 13 · REFERENCE Glossary Sources and authoritative references 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides 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

Can we just have IT export the relevant folders to save cost?

IT can assist; the export must still be forensic: metadata-preserving tooling, hashing, manifests, logging, under an examiner-written method with supervision and sampling (the hybrid conditions this series keeps insisting on). The drag-and-drop alternative rewrites timestamps across the very documents in dispute and converts a defensible collection into a witness-statement apology. The cost difference between the two is small; the evidential difference is the whole case's metadata.

The files we need were deleted from the share months ago. Are they gone?

Ask the history layer, quickly: snapshots reach days to weeks; previous-versions data similar; backup generations months to years, until recycling eats the relevant generation. The §10 suspension email is there for e the first act, today; the second is establishing which states bracket the deletion; recovery then usually follows. What rarely helps on servers is carving: enterprise storage abstractions bury released space: so the schedule conversation is the recovery conversation.

Can the server tell us who read a document, not just who changed it?

Only if read-auditing was configured for that tree during the period, which is the exception rather than the rule (read events are voluminous and often left off). Where it was on, the log answers directly; where it was off, "who read it" is rebuilt from the reader's side: end point recency artefacts, application traces, and (for remote access) VPN and authentication correlation: per guide 41. The audit-configuration export tells you which world you are in before anyone promises the client an answer.

Our opponent says their server "only keeps thirty days of logs" so nothing can be shown. Is that the end of it?

It is the beginning of three questions: what did the thirty-day window overlap (rotation schedules preserved from your first preservation letter onward: late suspension is itself a disclosure issue); what do snapshots and backups hold (log files are files: earlier generations often contain earlier log states); and what do the end point s and adjacent systems record (authentication servers, VPNs, the implicated workstations). Short retention narrows one source; it does not answer for the estate, and a Part 35 review of what should exist else where usually reframes the correspondence.

The share lives in SharePoint/OneDrive now. Does this guide still apply?

The three-layer thinking applies exactly; the machinery differs: cloud platforms keep their own version histories, recycle stages, audit logs and permission models, generally richer and longer-retained than on-premises defaults, collected through platform mechanisms rather than snapshots. The dedicated Microsoft 365 and cloud guides in this series carry the specifics; the transferable instruction is unchanged: name content, history and context in every preservation notice, which ever world hosts the share.

How disruptive is server collection to the business?

With snapshots, negligible: the freeze is instant and collection proceeds from the frozen copy

while production runs on. Live share collection is scheduled into quiet windows and throttled; full imaging, where genuinely needed, is negotiated like any guide 39 disruption. The honest cost is administrative at ten t i on (IT time for snapshots, exports and questions) rather than d own time: which is one more reason the cooperative, planned collection beats the improvised one on every axis this series measures. 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 17