NAS Evidence RAID Snapshots Shared Access Logs And Deleted Data

Network-Attached Storage, or NAS, devices are common in offices and homes, holding vast amounts of data. This guide explains their architecture, how evidence is acquired, and what records they keep, including accounts, logs, snapshots, and deleted files. It also covers common mistakes and technical limitations.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/nas-evidence-raid-snapshots-shared-access-logs-and-deleted-data

N AS EVIDENCE · A GUIDE FOR UK LAWYERS NAS Evidence: The Office Box That Holds Everything RAID, Snapshots, Shared Access, Logs and Deleted Data on Network- Attached Storage COMPUTER FORENSICS LAB

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

§ CONTENTS

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: TREATTHEAPPLIANCEASASMALLSERVERWITHBIGHABITS

§ 02 · FIRST PRINCIPLES The problem in plain English: the box nobody documented

§ 03 · THEARRAY RAID in plain English: why the disks are not the data

§ 04 · GETTINGITOUT Acquisition options: live, disks-out, or hybrid

§ 05 · WHATTHEBOXREMEMBERS What the appliance records: accounts, logs, snapshots, recycle folders

§ 06 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE NAS UNIT RELAY / REPLICA LOGS CLOUD US B / BACKUP BACKUP COUNTERPART DELETED / DEVICES RECOVERABLE

§ 07 · WHOSE H AND Attribution on a shared box

§ 08 · IN THE WILD Worked examples EXAMPLE1 · THERECYCLEBINNOBODYKNEWEXISTED EXAMPLE2 · THE DISK S IN THE WRONG ORDER EXAMPLE3 · THEBOXWASGONE; THEECOSYSTEMWASNOT

§ 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 · CLIENT HOLD IN G INSTRUCTION (SENDTO DAY)

§ 11 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The NAS evidence checklist Red flags When to involve a digital forensic expert 35 report that reads the appliance's own records properly (Example 1), or the review that prices an opponent's

§ 12 · COMMON QUESTIONS Frequently asked questions One of the disks has failed. Is the data gone? The NAS is password-protected and the person who set it up has left. Now what? Files were deleted from the NAS months ago. Recoverable? Can we prove who deleted them? The unit also records our CCTV. Anything special to do? Is a home NAS different from an office one?

§ 13 · 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

One of the disks has failed. Is the data gone?

Usually not: failure-tolerant RAID modes are designed to survive defined disk losses, and even the failed member often images part i all y in the laboratory. The dangerous moment is not the failure but the response: rebuilds and swaps on suspect hard w are can overwrite recoverable material. Power down on advice, touch nothing, and let imaging-then-virtual-reconstruction do the work: the route that preserves both the array and every option.

The NAS is password-protected and the person who set it up has left. Now what?

Hunt first: installers, IT suppliers, password managers, documentation, and the vendor account (which some time s enables recovery routes on managed units). In parallel, assess the ecosystem: sync mirrors and backups frequently contain the estate without the appliance's cooperation. Laboratory options on the unit itself depend on model and configuration (unencrypted volumes on extracted disks are readable regardless of the interface password; encrypted volumes need their keys): an examiner will tell you which case you have within a day of seeing the model.

Files were deleted from the NAS months ago. Recoverable?

Check, in order: the share's network recycle bin (deleted files often sit there for months); snapshot series (states bracketing the deletion, if pruning has not eaten them: hence the day-one suspension); backup generations (USB rotations and replicas reach furthest); and cloud-versioned copies where a sync or backup service was running. Classic carving inside the array is a last resort with modest odds on modern configurations. The honest answer is schedule-dependent: which is why this guide keeps sending the preservation email today.

Can we prove who deleted them?

Often to the account and end point, per the four links: recycle metadata and file-access logs (where enabled) name the NAS account and time; connection logs give the source address; the endpoint's own artefacts and, for remote access, relay and router records complete the triangulation. On boxes run on shared logins, the account link names a pool and the end point layer does the real work: the report should say exactly that, because over claim in g here is where NAS cases go to die in cross-examination.

The unit also records our CCTV. Anything special to do?

Move fastest on this of everything: surveillance retention is typically days to a few weeks and overwrite is continuous. Today: stop or reduce recording if the footage matters more than new coverage (a business decision to make explicitly), export the relevant date ranges through the surveillance app with times and camera identifiers, and preserve the app's logs. The dedicated CCTV guide later in this series covers format and timestamp handling; the NAS-specific point is simply that the deadline is the box's own timer.

Is a home NAS different from an office one?

Legally more than technically: the same vendors, arrays and artefacts, but personal ownership engages the consent, proportionality and privacy frameworks of this series'

personal-device guides, and household sharing complicates attribution further. Practically, home units are more often the replication partner or backup target of an office box (Example 3's second copy), which makes them disclosure-relevant through the ecosystem even when nobody thought of them as company systems: one more reason the §6 map belongs in every preservation notice. 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 14 of 16