

RAID NAS And Server Recovery

This guide for UK lawyers addresses the complexities of recovering data from RAID arrays, Network Attached Storage, and servers. It covers reconstruction methods, handling failed systems, preserving live storage, and avoiding common pitfalls to ensure evidence integrity.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
<https://e-discovery.uk/library/raid-nas-and-server-recovery>

ARRAY & SERVER RECOVERY · A GUIDE FOR UK LAWYERS RAID, NAS and Server
Recovery Reconstructing Arrays, Network Storage and Servers Without Losing the Evidence
COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
NAS & VIRTUALISATION RECOVERY CPR PART 35 EXPERT REPORT S FULL
CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the data is not on any one disk 03 How RAID, NAS and servers store data 04 Reconstructing an array: geometry, parity and forensic imaging 05 Failed and degraded arrays: recovery from partial sets 06 Preserving live server storage: snapshots, shares and proportionality 07 Deployment: disclosure, spoliation and the mishandled rebuild 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 only when the array's geometry is correctly reconstructed, and the commonest way to lose it is a well-meant

§ 02 · FIRST PRINCIPLES The problem in plain English: the data is not on any one disk

§ 03 · HOWITSTORESDATA How RAID, NAS and servers store data MEMBERS GEOMETRY
ARRAY FILE SYSTEM EVIDENCE

§ 04 · RECONSTRUCTION Reconstructing an array: geometry, parity and forensic imaging

§ 05 · FAILEDANDDEGRADEDARRAYS Failed and degraded arrays: recovery from partial sets

§ 06 · PRESERVINGLIVESERVERSTORAGE Preserving live server storage: snapshots, shares and proportionality

§ 07 · DEPLOYMENT Deployment: disclosure, spoliation and the mishandled rebuild

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE ARRAY
/ (SYNCED/ COUNTERPARTS THE END POINT S SERVER CACHED) BACKUPS & CLOUD
DELETED / REPLICAS PLATFORMS RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·
THEHELPFULREBUILDTHATNEARLYLOSTTHECASE EXAMPLE2 ·

THENASINTHECUPBOARDANDTHEBACKUPTHATSAVEDIT EXAMPLE3 ·
THEVIRTUALISEDSEVERANDTHELAYEREDRECONSTRUCTION

§ 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 · INSTRUCTIONFORANARRAY / SERVER RECOVERY

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

§ 13 · COMMON QUESTIONS Frequently asked questions Can you just image one disk from the
server? A disk failed and IT put in a new one and rebuilt the array. Is the evidence gone? The
array has lost two disks. Can it be recovered? Do we have to shut the business server down to
preserve it? The whole array is huge. Do we really need to image all of it? Is a reconstructed
array admissible as evidence?

§ 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

Can you just image one disk from the server?

Not use full y, on a striped or parity RAID: a single member holds only interleaved fragments, every file sliced through, and reads as gibberish (§2). The array must be reassembled from forensic images of every member, using the solved geometry (§4). The exception is a mirror (RAID 1), where one member is a readable whole, but even then the array metadata matters for currency.

A disk failed and IT put in a new one and rebuilt the array. Is the evidence gone?

Possibly, and this is the single most damaging thing that can happen (§5, Example 1): a rebuild recalculates and overwrites stripes. Caught early, enough original stripes may survive on forensic images of the members to reconstruct; run to completion, the overwritten data is gone. Stop any rebuild at once, image every member including the failed and replacement disks, and recover on the copies.

The array has lost two disks. Can it be recovered?

It depends on the parity: a single-parity array (RAID 5) survives one failure, not two, so two losses put it beyond reconstruction from the survivors alone (§5). A double-parity array (RAID 6) survives two. Where the array is beyond parity, partial recovery of what the survivors cover is attempted, and the estate, backups, replicas, end point s, carries the rest (Example 2, §8).

Do we have to shut the business server down to preserve it?

Usually not: live server storage is preserved by snapshots and live forensic acquisition that capture the relevant data while the system keeps running (§6), and by targeted, documented collection of the relevant shares rather than wholesale imaging. Downtime is reserved for where the array itself must be imaged member by member, which is planned to minimise disruption.

The whole array is huge. Do we really need to image all of it?

Often not: where it is the documents that matter, targeted collection of the relevant shares, home directories and mailboxes is the proportionate route (§6, guide 20). Full member-by-member reconstruction is reserved for where the array itself is in issue, its deleted data, its structure, or where the file system must be rebuilt. The method is sized to what the dispute actually needs.

Is a reconstructed array admissible as evidence?

Yes, when done properly: the members are imaged and hashed, the reconstruction is validated and its geometry and method documented so it can be explained and reproduced by another examiner (§4). A reconstructed logical volume is as sound as any other image; what must be avoided is the undocumented black-box reassembly that cannot be explained, and the rebuild-in-place that alters the original. 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

Source: <https://e-discovery.uk/library/raid-nas-and-server-recovery>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.