Damaged Computers And Data Recovery

Physically broken devices rarely mean empty ones. Much data survives damage and can be recovered using techniques from board repair to chip-level extraction. The pattern and timing of damage often indicate whether it was accidental or a deliberate attempt to destroy evidence, providing crucial insights for UK litigators and investigators.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/damaged-computers-and-data-recovery

DAMAGEDMEDIA · A GUIDE FOR UK LAWYERS Damaged Computers and Data Recovery Physically Broken Devices, the Recovery That Is Possible, and the Damage That Is a Clue COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES DAMAGED-DEVICE RECOVERY CHIP-LEVEL EXTRACTION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: broken does not mean empty 03 Types of damage and what each does to the data 04 The recovery techniques: from board repair to chip-off 05 Recovering defensibly: integrity, encryption and honest limits 06 Accidental or deliberate: reading the damage as evidence 07 Deployment: spoliation, insurance and the estate around the wreckage 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: ABROKENDEVICEISRARELYANEMPTYONE: MUCH DATA SURVIVESPHYSICALDAMAGEANDCANBERECOVEREDBYTECHNIQUESFROMBOARD REPAIRTOCHIP - LEVEL EXTRACTION, ANDTHEPATTERNANDTIMINGOFTHEDAMAGE OFTENTELLTHEIROWNSTORYABOUTWHETHERITWASACCIDENTORADELIBERATE ATTEMPTTODESTROYEVIDENCE

§ 02 · FIRST PRINCIPLES The problem in plain English: broken does not mean empty

§ 03 · TYPESOFDAMAGE Types of damage and what each does to the data

§ 04 · THERECOVERYTECHNIQUES The recovery techniques: from board repair to chip-off

§ 05 · RECOVERINGDEFENSIBLY Recovering defensibly: integrity, encryption and honest limits

§ 06 · ACCIDENTALORDELIBERATE Accidental or deliberate: reading the damage as evidence

§ 07 · DEPLOYMENT Deployment: spoliation, insurance and the estate around the wreckage

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION

COUNTERPART EVIDENCE LOCAL- DAMAGED CLOUD SERVER-SIDE DEVICE BACKUP PLATFORM S SYNCED / PHYSICAL DELETED / COPIES LAYER ONLY

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THELAPTOPTHATWOULDNOTPOWERONANDHELDEVERYTHING EXAMPLE2 · THEHOUSEFIRETHATWASREALLYAHAMMER EXAMPLE3 · THEGENUINELYDESTROYEDDRIVEANDTHEESTATETHATSAVEDTHECASE

§ 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 DA M AG EANA LY SIS

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The damaged-device checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions The laptop will not turn on. Is the data gone? The phone was smashed or soaked. Can anything be recovered? How can you tell if a device was broken deliberately? Does recovering a damaged drive also decrypt it? Is recovered data admissible, given the device was broken? The drive is genuinely destroyed. Is the case lost?

§ 14 · REFERENCE Glossary Sources and authoritative references 35 and CrimPR Part 19 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

The laptop will not turn on. Is the data gone?

Almost never, if the fault is power or board failure, which is the commonest presentation (§3): the storage is untouched and only the path to it is broken, so the drive is transplanted into working hard w are or read directly and the data recovered intact (§4, Example 1). Broken usually means the machine failed, not the storage. Send it for forensic recovery unaltered, do not let a repair shop tinker with it first.

The phone was smashed or soaked. Can anything be recovered?

Often yes: the screen and board may be destroyed while the memory chips survive, and where the board is dead the chips are removed and read directly (chip-off, §4). A wet phone should be powered off and sent promptly, drying and switching it on risks corrosion and can destroy what a proper recovery would retrieve (§5). The honest exceptions are a genuinely burned or shattered chip, where the data is gone.

How can you tell if a device was broken deliberately?

From the pattern, the timing and the account (§6): general damage suggests an accident, targeted damage to the storage suggests method; damage dated against the dispute is suspicious; and a claimed cause that the physical evidence contradicts, a "fire" that is really impact (Example 2), is a classic tell. Where a device was wiped before being smashed, the digital and physical evidence together tell the story (guide 110).

Does recovering a damaged drive also decrypt it?

No: physically recovering the storage and decrypting it are separate problems (§5). A chip-off of an encrypted phone yields encrypted data that still needs the key (guides 117 to 118), so a recovery commissioned without an encryption plan is only half done. Plan both from the start: recover the storage, then obtain the key by the recovery-key or compulsion routes.

Is recovered data admissible, given the device was broken?

Yes, when the recovery preserves integrity: the recovered image is hashed and the recovery method and any repairs documented as its provenance (§5), so data pulled from a broken device is as sound and admissible as an image of a working one. The recovery and the forensic exam in at i on are distinct stages, and the documented recovery answers any challenge to how the data was obtained.

The drive is genuinely destroyed. Is the case lost?

Usually not: the wreckage is rarely the only source (§8, Example 3). Backups made before the damage, synced copies, server-side mailbox and SaaS data, and counterparts' copies frequently hold the same material untouched, so a genuinely unrecoverable drive does not mean lost evidence. And a deliberately destroyed device becomes spoliation evidence in its own right (§6, §7): the destruction itself part of the case. 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