COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Damaged Computers and Data Recovery

Physically Broken Devices, the Recovery That Is Possible, and the Damage That Is a Clue

The device arrives broken. It was dropped, it was in a fire, it went through the wash, it was run over, it "died", or it was hit with a hammer the day the letter of claim arrived. A damaged computer or phone raises two questions at once. The first is technical: how much of the data can be recovered from a device that will not power on, and by what means, from a simple board repair to the removal of the storage chip itself and the reading of its raw contents in a cleanroom. The second is forensic: is this damage accidental, or is it the physical cousin of the wiping and encryption of earlier guides, a deliberate attempt to destroy evidence that leaves its own tell-tale signs. The two questions interact, because the pattern and timing of damage can be as evidential as the data recovered from the wreckage. This guide sets out for UK lawyers what data recovery from damaged devices can and cannot achieve, how it is done defensibly, and how accidental damage is distinguished from deliberate destruction.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Damaged-device recovery is recurring laboratory work: forensic recovery from computers and phones that will not power on, chip-level extraction where the board has failed, and the assessment of whether damage is accidental or a deliberate attempt to destroy evidence: with recovery conducted to preserve integrity and reported under CPR Part 35 and CrimPR Part 19, including where the damage pattern is itself the evidence.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | DAMAGED-DEVICE RECOVERY | CHIP-LEVEL EXTRACTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: A BROKEN DEVICE IS RARELY AN EMPTY ONE: MUCH DATA SURVIVES PHYSICAL DAMAGE AND CAN BE RECOVERED BY TECHNIQUES FROM BOARD REPAIR TO CHIP-LEVEL EXTRACTION, AND THE PATTERN AND TIMING OF THE DAMAGE OFTEN TELL THEIR OWN STORY ABOUT WHETHER IT WAS ACCIDENT OR A DELIBERATE ATTEMPT TO DESTROY EVIDENCE

Broken is not empty (§2, §3): most physical damage disables the device's ability to run, not the storage's ability to hold data: a laptop that will not power on, a phone with a smashed screen or a soaked board, a drive that clicks, usually still contains its data, because the damage is to the machine around the storage, not to the recorded bits themselves: the honest exceptions being genuine destruction of the storage medium and secure erasure. **The techniques (§4):** a ladder from the simple to the heroic: repairing or replacing failed components to make the device readable, transplanting the storage into working hardware, reading the storage chip directly (chip-off) where the board is dead, and cleanroom recovery of mechanical hard drives with physical platter damage: each more invasive and costly, chosen by what the damage requires and the matter justifies. **Defensible recovery (§5):** the recovery conducted to preserve integrity and the recovered data hashed and documented, the interaction with encryption understood (a physically recovered but still-encrypted volume needs the key of guides 117 to 118), and the honest limit stated where the medium itself is destroyed. **Accident or design (§6):** the forensic question running alongside the technical one: the pattern of damage (targeted versus general), its timing against the dispute (guide 110 §7), the inconsistency of an account with the physical evidence, and the tell-tale signs of deliberate destruction: read so that damage claimed as accidental can be tested. **Deployment (§7):** recovery for ordinary evidential purposes, the spoliation case where destruction was deliberate (guides 95, 110), the insurance and product contexts where the cause of damage is itself the issue, and the estate's redundancy (guides 95, 117 §6) that frequently holds the data whether or not the wreckage yields it.

- **Broken is not empty:** most damage disables the device, not the data, which usually survives and can be recovered.
- **A ladder of techniques:** board repair, storage transplant, chip-off, cleanroom, each more invasive as the damage demands.
- **Recovery preserves integrity:** recovered data is hashed and documented, and encryption still needs its key.
- **Damage can be evidence:** the pattern and timing distinguish accident from deliberate destruction.
- **The estate holds copies:** the wreckage is rarely the only source; backups and syncs often carry the case.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: broken does not mean empty

When a device is dropped, soaked or refuses to switch on, the natural assumption, shared by clients and often by opponents, is that its data is gone. That assumption is usually wrong, and understanding why is the key to the whole subject. A computer or phone is two things bolted together: the machine that runs, the screen, the board, the power system, the processor, and the storage that holds the data, the drive or the memory chips. Most physical damage breaks the first and leaves the second intact. A laptop with a fried power board will not turn on, but its storage still holds every file. A phone with a shattered screen and a soaked circuit board is dead to its owner, but its memory chips have retained their contents. A hard drive that clicks has a mechanical fault, but its platters still carry the recorded data.

This is why data recovery from damaged devices is so often successful: the recovery engineer's task is usually not to un-destroy data but to get past the broken machinery to the storage that was never damaged, whether by repairing the machine, moving the storage to working hardware, or reading the storage directly. There are genuine exceptions, a burned or physically shattered chip, a securely wiped drive, platters ground away, where the data really is gone, and the honest engineer says so. But the default expectation should be that a broken device still holds its data, and the second question, whether the damage was an accident or a deliberate attempt to destroy that data, is often as important as the recovery itself. This guide takes both questions together.

§ 0 3 · TYPES OF DAMAGE

Types of damage and what each does to the data

- **Power and board failure:** a device that will not power on because of a failed power system, board component or connector: the commonest presentation, and usually the most recoverable, because the storage is untouched and only the path to it is broken: fixed by repair, transplant or direct chip reading.
- **Liquid damage:** a device dropped in water or drink: the immediate risk is corrosion of the board over time, which is why a wet device should be powered off and sent for recovery promptly rather than dried and switched on: the storage chips usually survive and are read directly if the board has corroded.
- **Impact and crushing:** a dropped, run-over or struck device: the screen and board may shatter while the storage chip survives intact, or, in severe cases, the chip itself cracks: the outcome established by inspection, because impact damage is variable and often leaves the storage readable.
- **Fire and heat:** a device in a fire: heat destroys components progressively, and while a badly burned storage chip may be beyond recovery, chips are often better protected than the surrounding board and survive fires that destroy the device: the recovery attempted, not assumed lost.
- **Mechanical hard-drive failure:** the clicking or seized traditional hard drive: a mechanical fault (heads, motor, bearings) with the platters and their data usually intact, recovered in a cleanroom by repairing or transplanting the mechanism, distinct from actual platter surface damage, which is the harder case.

§ 0 4 · THE RECOVERY TECHNIQUES

The recovery techniques: from board repair to chip-off

- **Board and component repair:** repairing or replacing the failed part, a power component, a connector, a controller, to make the device or drive readable again, then imaging it normally: the least invasive route, sufficient where the storage is intact and only the machine failed.
- **Storage transplant:** removing the storage (a drive, or a removable module) and reading it in known-good hardware, bypassing the damaged device entirely: straightforward where the storage is a discrete, transferable component.
- **Chip-off extraction:** where the board is dead and the storage is soldered memory, removing the memory chip itself and reading its raw contents on a specialist reader, then reconstructing the file system from the raw data: an invasive, skilled technique for devices whose board cannot be revived, and often the only route for a badly damaged phone.
- **Cleanroom recovery:** for mechanical hard drives with internal faults, opening the drive in a contamination-controlled cleanroom to repair or transplant the head assembly or motor and read the platters: the specialist recovery for the clicking or seized drive, defeated only by actual platter surface destruction.
- **The escalating ladder:** the techniques applied in order of invasiveness and cost, the simplest that will work chosen first, and the more heroic reserved for what the matter justifies and the damage requires: with the interaction with encryption (a recovered volume may still be encrypted) and the honest limit (a destroyed medium) governing what any technique can deliver (§5).

§ 0 5 · RECOVERING DEFENSIBLY

Recovering defensibly: integrity, encryption and honest limits

- **Integrity through the recovery:** the recovery conducted so that the recovered data's integrity is preserved and demonstrable, the recovered image hashed, and the recovery method and any repairs documented (guides 2, 3): so that data pulled from a broken device is as sound and admissible as data imaged from a working one.
- **Recovery is not examination:** the recovery engineer's job is to retrieve the data intact; the forensic examination then proceeds on the recovered image by the ordinary methods: the two stages distinct, with the recovery documented as the provenance of the image the examination relies on.
- **The encryption interaction:** physically recovering the storage does not decrypt it: a chip-off of an encrypted phone yields encrypted data that still needs the key (guides 117 to 118), so the recovery and the access problems are separate and both must be solved: a point often missed when a recovery is commissioned in isolation.
- **The honest limit:** where the storage medium itself is genuinely destroyed, a burned or shattered chip, ground-away platters, a securely wiped drive, the data is gone, and the engineer states this plainly rather than raising false hope (guide 100's honest-limits discipline, guide 117 §3).
- **One attempt, done right:** damaged-media recovery is often a one-shot exercise, a failed amateur attempt (drying and powering on a wet phone, running data-recovery software on a failing drive) can destroy what a proper recovery would have retrieved: the device sent to a specialist unaltered, not tinkered with first (guide 108's do-not-switch-it-on principle, for damaged media).

§ 0 6 · ACCIDENTAL OR DELIBERATE

Accidental or deliberate: reading the damage as evidence

- **The pattern of damage:** general damage consistent with an accident (a phone dropped, a laptop knocked off a desk) versus targeted damage aimed at the storage (a drive removed and struck, a chip deliberately destroyed, a device disassembled and its storage singled out): the pattern often distinguishing misfortune from method (guide 110 §4's overwrite-pattern logic, for physical destruction).
- **The timing:** damage dated, or reported, against the dispute, the device "died" the day the hold notice arrived, the laptop was "dropped" the week before disclosure: the timing against the duty (guides 95 §6, 110 §7) supplying the same suspicion physical destruction shares with wiping.
- **The account against the evidence:** the claimed cause of damage tested against the physical reality, a device said to have been in a house fire showing impact rather than heat damage, a "water-damaged" phone with a cleanly cracked chip: the inconsistency between story and wreckage a classic tell (guide 109's world-test logic, for hardware).
- **The convenient loss:** the device that is damaged and then also lost or disposed of, or the storage removed before the device is handed over: the destruction compounded by the disappearance (guide 95 Example 2), read together.
- **The recovery that contradicts the claim:** where recovery succeeds despite a claim the device was destroyed, or reveals a wipe run before the physical damage (the destroyer who wiped and then smashed), the recovered evidence contradicting the account of loss: the damage and the data together telling the story.

§ 0 7 · DEPLOYMENT

Deployment: spoliation, insurance and the estate around the wreckage

- **Ordinary recovery for evidence:** the common case, a genuinely accidentally damaged device holding relevant material, recovered and examined normally, the damage an obstacle overcome rather than an issue in itself: most damaged-device instructions are simply this.
- **Spoliation where destruction was deliberate:** where the §6 analysis shows targeted, timed, account-inconsistent damage, the deliberate-destruction case with its adverse-inference, strike-out and contempt consequences (guides 95 §7, 110 §7): physical destruction of evidence treated as gravely as its digital cousins.
- **Insurance and product contexts:** matters where the cause of damage is itself the dispute, an insurance claim turning on whether damage was accidental, a product-liability claim on whether a device failed or was misused: the damage analysis of §6 as the substantive evidence, not merely a recovery obstacle.
- **The estate around the wreckage:** the recovery pursued alongside, not instead of, the estate reach-around, the backups, syncs, server-side platforms and counterpart copies (guides 95, 117 §6) that frequently hold the same data whether or not the wreckage yields it, so a failed recovery does not mean lost evidence.
- **Proportionality of heroic recovery:** the cost of chip-off and cleanroom recovery weighed against what the estate already holds and what the device uniquely contains, the heroic recovery justified where the device holds unique, central evidence and disproportionate where a backup holds the same material (guide 20's balance).

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a damaged device is one node, and the data on it is usually reflected across a redundant estate that no accident or hammer can reach. The device holds the local and deleted material, recoverable from the wreckage by the §4 ladder. But the cloud backups made before the damage, the synced copies on other devices, the server-side mailbox, drives and SaaS, and the counterparties' copies hold the same data untouched by the physical harm. The discipline is to pursue the recovery and the estate reach-around together: the estate frequently delivers the evidence quickly and cheaply while the recovery is attempted, so a difficult or failed recovery does not mean a lost case. And the physical evidence adds a layer the estate cannot: the damage pattern, timing and account-consistency that reveal whether the destruction was deliberate, read alongside the digital anti-forensic record (guide 110) where a device was both wiped and smashed. When the wreckage yields nothing, the estate carries the case and the damage becomes spoliation evidence; when it yields data, that data corroborates or contradicts the account of the loss.

QUESTION	DAMAGED DEVICE	CLOUD BACKUP	SYNCED / COUNTERPART COPIES	SERVER-SIDE PLATFORMS	PHYSICAL EVIDENCE LAYER	DELETED / LOCAL-ONLY
Documents	Recoverable from storage	Y: pre-damage backup	Y: shared copies	Y: drives, SaaS	n/a	Local-only files
Messages	Recoverable from chips	Y: pre-damage backup	Y: counterparts	Y: mailbox, chat	n/a	Local caches
Local-only / deleted	Y: from recovered image	Sometimes	n/a	Version history	n/a	Y: once recovered
Was it accident or design	Y: damage pattern	n/a	n/a	n/a	Y: pattern, timing, account	Wipe before smash
When it was damaged	Last-use artefacts	Last-sync bracket	Last contact	Sign-in bracket	Reported vs actual	n/a

Fallback strategy in one line: pursue the recovery and the estate reach-around together so a hard recovery is not a lost case; and read the damage pattern, timing and account as evidence of whether the destruction was accident or design.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE LAPTOP THAT WOULD NOT POWER ON AND HELD EVERYTHING

A key custodian's laptop, holding the documents central to a commercial dispute, would not switch on, and the client feared the evidence lost. The §3 assessment identified the fault as a failed power board, not storage damage, the commonest and most recoverable presentation. The §4 recovery was routine: the storage, an intact solid-state drive, was transplanted into known-good hardware and imaged forensically, hashed and documented (§5), and every file was present. The device that looked dead to its owner had held its data intact the entire time, because the damage was to the machine, not the storage. The §5 discipline mattered, the client was advised not to send it to a high-street repair shop that might have attempted a board fix and inadvertently altered the drive, but to a forensic recovery that preserved integrity. Broken did not mean empty; it meant the path to the data was blocked, and the recovery cleared it.

EXAMPLE 2 · THE HOUSE FIRE THAT WAS REALLY A HAMMER

A respondent to a fraud claim reported that the laptop holding the relevant accounts had been destroyed in a house fire, and produced a burned device. The §6 damage analysis contradicted the account: the pattern of damage was mechanical, not thermal, the casing was shattered and the internal board cracked in a way consistent with heavy impact, and there was none of the progressive heat damage, melted plastics, scorch gradients, a genuine fire produces. The storage chip, though the board was destroyed, was intact, and a §4 chip-off recovered its contents, which included the accounts the respondent had said were lost, and, tellingly, a §6 finding that a wiping tool had been run over the accounts folder two days before the "fire" (guide 110). The damage was staged, the recovery succeeded, and the account of the fire, tested against the physical and digital evidence together, collapsed. The wreckage and the data told one story; the respondent had told another.

EXAMPLE 3 · THE GENUINELY DESTROYED DRIVE AND THE ESTATE THAT SAVED THE CASE

A drive central to a dispute had suffered genuine platter surface damage, the heads had crashed and scored the platters, and the §5 honest assessment was that the affected regions were physically destroyed and unrecoverable, a real limit, stated plainly rather than pursued with false hope through ever-more-expensive attempts. But the §8 estate carried the case: the drive's data had been backed up to the organisation's server two days before the failure, and the synced copies and server-side mailbox held the correspondence, so the material the destroyed drive would have yielded existed, untouched, elsewhere. The §7 proportionality analysis stopped the futile pursuit of the ruined platters and directed effort to the backup that held the same data cheaply and completely. The lesson is §8's: the wreckage is rarely the only source, and the honest limit on one node is not the end of the case when the estate is redundant.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Assuming broken means empty:** a recoverable device written off as lost, the data abandoned when a transplant or chip-off would have retrieved it (Example 1).
- **Amateur recovery attempts:** a wet phone dried and powered on, a failing drive run through recovery software, a device sent to a high-street shop, destroying what a proper recovery would have saved (§5).
- **Damage taken at face value:** a claimed accidental cause accepted without the §6 pattern, timing and account analysis that would have exposed staged destruction (Example 2).
- **Recovery commissioned without the encryption plan:** a chip-off delivering encrypted data with no plan to obtain the key (guides 117 to 118), the recovery half-finished.
- **The estate ignored:** heroic, expensive recovery pursued while a backup held the same data cheaply (Example 3).
- **Heroic recovery pursued past proportionality:** ruined platters chased with ever-costlier attempts when the honest limit had been reached (§5, §7).
- **Recovery and forensic examination confused:** a recovery engineer treated as the forensic examiner, or the recovery's provenance undocumented so the recovered image's integrity is challengeable.
- **The convenient loss unremarked:** a damaged-then-disposed device or a removed drive accepted without the spoliation inference it invites (§6).

Technical limitations

- **Some destruction is genuine:** burned or shattered chips, ground-away platters and securely wiped drives are beyond recovery: the honest limit, stated, not wished away (§5, Example 3).
- **Recovery does not decrypt:** physically recovered encrypted storage still needs its key; the recovery and access problems are separate (§5).
- **Chip-off is invasive and skilled:** it risks the chip if done poorly and requires specialist capability; it is a considered step, not a default.
- **One attempt often:** a failed first attempt can foreclose a successful one; the device is sent unaltered to a specialist the first time.
- **Damage analysis has limits:** the pattern and timing are strong evidence but not always conclusive; the finding is graded honestly and corroborated with the digital record (guide 110).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- How, when and where was the device damaged, and who has handled it since, so the account can be tested against the physical evidence?
- What backups, syncs and server-side copies of the device's data exist, so recovery and the estate are pursued together?
- Has anyone attempted repair, drying or recovery already, which may have altered the device?

Ask your opponent

- Please preserve the damaged device unaltered and do not attempt repair, recovery or disposal, and confirm the circumstances, date and cause of the damage and the identity of everyone who has handled the device since.
- Please confirm whether the device has been examined, repaired or subjected to any recovery attempt, and permit forensic recovery and examination by an agreed or independent examiner, including analysis of the cause and pattern of damage.
- Please identify all backups, synchronised copies and server-side data holding the same material as the damaged device.

Ask your eDiscovery / forensic provider

- What is the likely fault, and which recovery technique does it call for at what cost?
- Is the damage consistent with the claimed accidental cause, or does its pattern and timing suggest deliberate destruction?
- Does the estate already hold the same data, so heroic recovery may be unnecessary?

SUGGESTED WORDING · INSTRUCTION FOR A DAMAGED-DEVICE RECOVERY AND DAMAGE ANALYSIS

> "We instruct you to recover and examine the damaged device(s) identified at Schedule 1, and to assess the cause of the damage. Please: (1) assess the nature of the damage and the likely fault, and advise on the appropriate recovery technique (board repair, storage transplant, chip-off or cleanroom recovery) and its prospects and cost, before proceeding; (2) recover the data preserving integrity, hashing the recovered image and documenting the recovery method and any repairs as its provenance; (3) where the recovered storage is encrypted, advise on obtaining the key separately, and where the medium is genuinely destroyed, state that limit honestly; (4) analyse the pattern, extent and, so far as possible, the timing of the damage, and assess whether it is consistent with the claimed cause or indicative of deliberate destruction, having regard to any evidence of prior wiping; and (5) identify the material available from backups, synchronised copies and server-side platforms, so recovery is pursued proportionately alongside the wider estate. Do not power on, dry, repair or otherwise alter the device before forensic recovery."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The damaged-device checklist

- ☐ Device preserved unaltered; no drying, repair or recovery attempted first
- ☐ Nature of damage and likely fault assessed before recovery
- ☐ Recovery technique matched to the damage and the matter
- ☐ Recovered data hashed; recovery method documented as provenance
- ☐ Encryption plan in place where recovered storage is encrypted
- ☐ Honest limit stated where the medium is genuinely destroyed
- ☐ Damage pattern, extent and timing analysed for cause
- ☐ Claimed cause tested against the physical and digital evidence
- ☐ Estate mapped for the same data held elsewhere
- ☐ Heroic recovery weighed against proportionality and the estate

Red flags

- A device that "died" or was "dropped" just as the dispute crystallised: Example 2's timing.
- Damage inconsistent with the claimed cause: the "fire" that is impact.
- A device damaged and then also lost, disposed of, or its storage removed.
- Evidence of wiping preceding the physical damage.
- An amateur repair or recovery attempted before forensic recovery.
- A recovered drive that is encrypted with no key plan.
- A damaged device treated as the only source while backups exist.

When to involve a digital forensic expert

Before the device is touched, because a well-meant repair or a drying-and-powering-on can destroy what a proper recovery would have saved (Example 1, §5); at assessment, where the fault is diagnosed and the right recovery technique and its cost are advised before proceeding; at recovery, where the data is retrieved preserving integrity and the encryption and honest-limit questions are resolved; at damage analysis, where the pattern, extent and timing are read to test whether the damage was accident or deliberate destruction (Example 2); and at deployment, where the recovered evidence and the damage finding are reported under CPR Part 35 or CrimPR Part 19, alongside the estate that often holds the same data (Example 3). Through **cflab.uk** and **e-discovery.uk**, damaged-device work combines forensic recovery with damage analysis and the estate reach-around: because broken rarely means empty, the wreckage is seldom the only source, and the way a device was broken is often as telling as what it held.

§ 13 · COMMON QUESTIONS

Frequently asked questions

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 hardware 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 examination 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.

§ 14 · REFERENCE

Glossary

Chip-off
Removing a memory chip to read its raw contents directly.

Cleanroom
A contamination-controlled space for opening hard drives.

Storage transplant
Moving storage into working hardware to read it.

Board repair
Fixing failed components to make a device readable.

Platter
The disk inside a hard drive that holds the data.

Head crash
A drive fault where heads contact and damage the platters.

Provenance
The documented history establishing recovered data's origin.

Damage pattern
The distribution of harm, revealing accident or intent.

Recovery
Retrieving data from a failed or damaged device.

Honest limit
The point beyond which data is genuinely unrecoverable.

Sources and authoritative references

The damaged-device disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (damaged-device recovery, chip-off and cleanroom recovery, damage analysis, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (recovery of damaged sources and estate reach-around as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (integrity and method in recovery): gov.uk, FSR Code · ISO/IEC 27037 (identification, collection and preservation, including damaged media): iso.org, 27037
- NIST SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics (chip-off and physical extraction): csrc.nist.gov, SP 800-101
- PD 57AD (preservation and spoliation) and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Damaged-device work at the laboratory starts from the premise that broken rarely means empty: most physical damage disables the machine and leaves the storage intact, so the first step is a careful assessment of the fault and the right recovery technique, board repair, storage transplant, chip-off or cleanroom recovery, chosen for what the damage requires and the matter justifies (Example 1). Recovery is conducted to preserve integrity, the recovered image hashed and the method documented as its provenance, with the encryption question resolved separately where recovered storage is still encrypted, and the honest limit stated plainly where a medium is genuinely destroyed (Example 3). Alongside the recovery, the laboratory reads the damage itself, its pattern, extent and timing, testing a claimed accidental cause against the physical and digital evidence and exposing staged destruction where the story and the wreckage do not match (Example 2). And the estate reach-around runs in parallel, so a difficult or failed recovery is not a lost case when backups and server-side copies hold the same data. Devices are never powered on, dried or repaired before forensic recovery. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a device has arrived broken, the first instruction is the same as for every fragile source: do not switch it on, do not tinker, send it in as it is.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace