External Storage Devices As Evidence

External storage devices are crucial evidence sources in UK litigation, revealing copied files, timestamps, and deleted data. This guide details their examination, from intake and imaging to attribution and common pitfalls. It assists practitioners in understanding what these devices disclose and how to interpret their contents.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/external-storage-devices-as-evidence

EXTERNALSTORAGEEVIDENCE · A GUIDE FOR UK LAWYERS External Storage Devices as Evidence What Memory Sticks, External Drives and Cards Reveal: Copied Files, Timestamps, Deleted Data and Attribution COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the object in the evidence bag 03 Getting the device examined: intake, imaging, integrity 04 What the live file system tells you 05 Timestamps on external media: reading the copy story 06 Deleted data: recycle folders, unallocated space and the SSD problem 07 Whose device, whose hand: attribution on p or table media 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: THEDEVICEISDIRECTEVIDENCE; TREATITLIKETHEEXHIBITIT

§ 02 · FIRST PRINCIPLES The problem in plain English: the object in the evidence bag

§ 03 · INTAKE Getting the device examined: intake, imaging, integrity

§ 04 · WHAT IS THERE What the live file system tells you

§ 05 · WHENITGOTTHERE Timestamps on external media: reading the copy story

§ 06 · WHAT WAS THERE Deleted data: recycle folders, unallocated space and the SSD problem

§ 07 · WHOSE H AND Whose device, whose hand: attribution on p or table media

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE THE DEVICE SERVER S / SOURCE CORPORATE ONWARD DELETED / MACHINE(S) TOOLING DEVICES RECOVERABLE SOURCE CLOUD

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THETWO - CLOCKSIGNATUREANDTHEINJUNCTIONDATE EXAMPLE2 · THESNAPPEDSTICK, RECOVERED EXAMPLE3 · THEDRIVETHATCLEAREDHER

§ 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 · INSTRUCTION FOR DEVICE EXAM IN AT I ON

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The external media checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions We have the stick. Do we still need the computers? The files were deleted from the stick before it was handed over. Gone? Can you tell which computer the files came from? The device belongs to the company but lived on a shared desk. Is attribution hopeless? What about memory cards from cameras, dashcams and phones? Our opponent simply has not produced the drive we know exists. What now?

§ 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

We have the stick. Do we still need the computers?

For a strong case, yes: the device supplies content and arrival times; the machines supply connection records, sessions and access artefacts: and the welds between them are what attribution stands on. A device alone proves what it holds and roughly when it arrived; paired with even one source machine it proves the corridor the files travelled and whose session the transfer sat inside. Ask for both in the same order wherever possible.

The files were deleted from the stick before it was handed over. Gone?

Frequently not: removable-media deletion is shallow (index dropped, content resident until overwritten), and sticks see little post-deletion writing in the ordinary course. Expect file-system remnant recovery first (names, dates, content) and carving behind it: unless the device is a TRIM-active SSD, where the honest answer arrives only after imaging. Reformatting changes little: prior volumes and content routinely survive quick formats, and the reformat's own date joins the chronology.

Can you tell which computer the files came from?

Often, by convergence: source-side modified times and embedded metadata carrying the origin environment; host droppings typing the platforms the device met; and, decisively, the machine-side interlock: the source computer's own records of this device's serial, connected in a session, with the very files accessed in the window the device says they arrived. Any single strand indicates; the convergence identifies: and the report will use exactly those verbs.

The device belongs to the company but lived on a shared desk. Is attribution hopeless?

No: it is shared-asset work, per Example 3: map the users whose sessions the device appears in across the machine fleet, read the content's internal ownership signals, and time the disputed transfer against the session record. Shared possession widens the starting pool and the interlock narrows it: some time s to one, some time s to two-with-submissions: and a report that shows that narrowing honestly out per form s one that never admitted the pool existed.

What about memory cards from cameras, dashcams and phones?

Same laboratory treatment, distinct habits: DCIM structures and device-written metadata (camera model, some time s GPS in the images themselves) make provenance unusually rich; FAT semantics govern times; deletion recovery is typically generous; and the card frequently outlives and contradicts the device it served ("the dashcam footage was overwritten" meets the card's unallocated space). Treat cards as first-class exhibits, not accessories: they decide cases about incidents, journeys and timelines with some regularity.

Our opponent simply has not produced the drive we know exists. What now?

Run the fallback line: machine-side records prove the device's existence, serial, and every connection (guide 47); corporate tooling and server audit prove access and pattern; onward copies are pursued where the content travelled. Then put the absence itself to work: specific disclosure and delivery-up applications, questions about disposal with dates, and the adverse-inference submission that a produced device would have answered. Non- production of a pocketable exhibit is rarely neutral, and courts are readier than opponents expect to say