What Evidence Can Be Recovered From A Windows Computer (1)

Windows computers retain a significant amount of data beyond what users intentionally create. This guide details the types of digital evidence recoverable from these systems, such as deleted files, login activity, program execution traces, and internet browsing history, which can be crucial in legal investigations.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/what-evidence-can-be-recovered-from-a-windows-computer-1

WINDOWS FORENSICS · A GUIDE FOR UK LAWYERS What Evidence Can Be Recovered from a Windows Computer? Deleted Files, USB History, Logins, Browsing, Execution Traces and the Timeline They Build COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM 35 and CrimPR Part 19. Its e Discovery arm, e-discovery.uk, integrates device-level findings into disclosure-scale COURT-EXPERIENCED EXPERT WITNESSES

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the machine remembers 03 Deleted files and where they hide 04 USB devices and external media history 05 Logins, accounts and who was at the keyboard 06 Files opened, folders browsed: the recency artefacts 07 Programs run: the execution artefacts 08 Browsing, search in g and the online record 09 Event logs and the system's own diary 10 Building the timeline: from artefacts to narrative 11 Worked examples 12 Common mistakes and technical limitations 13 Questions to ask · Suggested wording 14 Checklist and red flags · When to involve a digital forensic expert 15 Frequently asked questions 16 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: WINDOWSRECORDSFARMORETHANUSERSCREATE

§ 02 · FIRST PRINCIPLES The problem in plain English: the machine remembers

§ 03 · WHATDELETIONLEAVES Deleted files and where they hide

§ 04 · THEPLUG - INRECORD USB devices and external media history

§ 05 · WHOWASSIGNEDIN Logins, accounts and who was at the keyboard

§ 06 · WHATWASOPENED Files opened, folders browsed: the recency artefacts

§ 07 · WHATWASRUN Programs run: the execution artefacts

§ 08 · THEONLINERECORD Browsing, search in g and the online record

§ 09 · THE SYSTEM ' SDIARY Event logs and the system's own diary

§ 10 · ASSEMBLY Building the timeline: from artefacts to narrative

§ 11 · IN THE WILD Worked examples EXAMPLE1 · THELEAVER,

THESTICKANDTHEFIFTEENMINUTES EXAMPLE2 · THEDELETIONTHATPROVEDMORETHANTHEDOCUMENTSWOULDHAVE EXAMPLE3 · THESHAREDOFFICECOMPUTERANDTHEACCOUNTTHATWASNOTHIM

§ 12 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 13 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTION FOR A WINDOWS EXAM IN AT I ON

§ 14 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The Windows evidence checklist Red flags When to involve a digital forensic expert 35 / CrimPR Part 19 report that presents convergence a court can act on. Defensively, instruct an examiner

§ 15 · COMMON QUESTIONS Frequently asked questions Can deleted files really be recovered, and for how long? Can the computer prove who was using it, rather than which account? If someone used a wiping tool, is the evidence gone? The laptop has been used for months since the events. Is exam in at i on point less? Does any of this work on a Mac, or on cloud-stored files? What does a Windows exam in at i on cost and how long does it take?

§ 16 · REFERENCE Glossary SRUM 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 deleted files really be recovered, and for how long?

Often, and it depends: on drive type (hard drives hold released content until overwritten, months or years; SSDs erase it in background housekeeping, days or less), on activity since, and on the parallel routes: Recycle Bin remnants, shadow copies, temporary and cached duplicates, backups. Two honest constants: the metadata layer (that files existed, and when they were deleted) survives far longer than content; and every week of delay closes doors. Instruct early and let the examiner report which doors this particular machine still has open.

Can the computer prove who was using it, rather than which account?

Not alone, and no honest expert claims it can: the machine proves account sessions. The human layer is built around them: authentication type and credential exclusivity, corroborating records (badges, VPN, CCTV, phones), and in-session behaviour (whose webmail, whose files, whose patterns): usually to a comfortable civil standard, some time s beyond. What decides cases is doing that layer explicitly: Example 3 is what happens when a party skips it, and §5 is the discipline that survives cross-examination.

If someone used a wiping tool, is the evidence gone?

The targeted content may be; the event rarely is. Wiping tools appear in execution artefacts (Prefetch, User Assist, Amcache) with run times, their acquisition often sits in the browser record, mass deletions leave file- system and journal traces, and configuration changes are logged. Post-duty destruction then does its own damage: adverse inferences, strike-out exposure, and Example 2's outcome: courts treat proven spoliation, provably timed, as loudly as the missing documents would have spoken.

The laptop has been used for months since the events. Is exam in at i on point less?

No: it re-weights toward the durable layers. Registry device history, LNK and shellbag records, execution artefacts, and event-log reach often survive routine use for long periods; deleted-content recovery and short- horizon artefacts suffer most. The exam in at i on scopes to what the elapsed time left, and the report states horizons honestly: months of use narrows the window, it does not board it up.

Does any of this work on a Mac, or on cloud-stored files?

The philosophy transfers, the artefacts differ: macOS keeps its own equivalents (covered in the next guide in this series), and files living in cloud tenancies leave their substantive record server-side, where platform audit logs and versions do the work (the cloud guides that follow). The Windows machine remains evidentially rich even in cloud-centric estates: sync clients, local caches and the artefact families above record the local half of every story: but complete answers usually mean collecting both halves.

What does a Windows exam in at i on cost and how long does it take?

Scoped work on defined questions (a leaver's last month, a USB window, an attribution dispute) is typically days of examiner time on a fixed estimate, after imaging; full-timeline work on multi-year questions scales with the ambition. The economical route is the instruction wording in §13: precise questions, graded findings, stated limits: which buys conclusions

rather than tooling output, and usually answers in one report what open-ended "look at everything" instructions answer in three. 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 17 of 20

Source: https://e-discovery.uk/library/what-evidence-can-be-recovered-from-a-windows-computer-1. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.