Can You Prove Who Deleted A File

Deletion is an act with actors, and platforms record it. This guide explores how to attribute file deletion to an account or person, covering cloud, server, and local deletion, deliberate erasure, and the wider evidence architecture. It details common mistakes, technical limitations, and when to involve a digital forensic expert.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/can-you-prove-who-deleted-a-file

DELETIONATTRIBUTION · A GUIDE FOR UK LAWYERS Can You Prove Who Deleted a File? Deletion Artefacts, Audit Trails and the Attribution of an Absence COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM FILE-SYSTEM JOURNAL ANALYSIS CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: DELETIONISRECORDEDBYTHEPLATFORM, THE FILE SYSTEM ANDTHEERASURETOOLITSELF: THERECORDNAMESANACCOUNTORPROFILE, THE CORROBORATIONNAMESTHEPERSON, ANDTHETIMINGAGAINSTTHEDUTYNAMESTHE CONSEQUENCE

§ 02 · FIRST PRINCIPLES The problem in plain English: deletion is an act, and acts have actors

§ 03 · CLOUDANDSERVERDELETION Cloud and server deletion: audit logs, recycle stages and admin actions

§ 04 · LOCALDELETION Local deletion: recycle bins, file-system journals and metadata residue

§ 05 · DELIBERATEERASURE Deliberate erasure: wiping tools, anti-forensics and their own artefacts

§ 06 · ATTRIBUTION Attribution: from account and profile to the person at the keyboard

§ 07 · DEPLOYMENT Deployment: spoliation, employment, fraud and the innocent explanation

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION DEVICE TOOL PLATFORM RECYCLE FILE-SYSTEM ESTATE AUDIT LOG STAGES STRUCTURES REDUNDANCY SESSION / ERASURE- LAYER ARTEFACTS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEPURGEAT23: 12ANDTHEACCOUNTTHATDIDIT EXAMPLE2 · THECLEANLAPTOPANDTHECLEANER ' SRECEIPT EXAMPLE3 · THEDELETIONTHATWASAPOLICY, ANDTHEALLEGATIONTHATWAS WITHDRAWN

§ 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 · INSTRUCTIONFORDELETION AT TRIBUTION

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

§ 13 · COMMON QUESTIONS Frequently asked questions If a file is gone, how can anyone know who deleted it? Does emptying the recycle bin remove the evidence of deletion? The laptop came back wiped. Is there anything to find? Can we prove it was the person and not just their account? Our client did delete the files, but before any dispute. Does that matter? What if the deletion was done by a retention policy or an administrator?

§ 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

If a file is gone, how can anyone know who deleted it?

Because deletion writes records the deleter does not see: the platform's audit event naming the account, the recycle bin's metadata naming the profile and time, the file system's journal recording the transaction (§3-§4): Example 1's purge sequence was reconstructed entirely from those. The content's absence and the act's record are separate things.

Does emptying the recycle bin remove the evidence of deletion?

It removes the item and, in time, the bin's metadata file: but the emptying is itself an audited or journaled event, the metadata file persists in unallocated space for a period, and the platform's second-stage store holds cloud items longer (§3-§4). Emptying the bin usually adds a second attributed event rather than removing the first.

The laptop came back wiped. Is there anything to find?

Often the most important thing: the wiping tool's installation and execution records, its settings, the overwrite pattern and the change journal it did not target (§5, Example 2): deliberate erasure after a duty arose is stronger evidence than the erased files would have been. The device is imaged first and the tool's receipt read second.

Can we prove it was the person and not just their account?

To the extent the corroboration allows: session and device from sign-in records, presence from badges or calendar, their own messages about it, and the exclusion of alternatives (shared login, unattended desk, sync, policy) (§6): the report grades the attribution accordingly. "Account X on device Y at 23:12" is a finding; the name follows when the lattice supports it.

Our client did delete the files, but before any dispute. Does that matter?

Enormously: deletion before the preservation duty arose is retention or housekeeping, and the attribution record proves the timing (§7, guide 95 §6): Example 3's policy deletions eleven months before contemplation defeated the allegation with costs. Establish the date from the record; it is the whole difference between a gap and spoliation.

What if the deletion was done by a retention policy or an administrator?

Then the audit event says so: system identities, policy execution records and admin actions are distinguishable from user deletions by event type and acting account (§3), and the policy's configuration history dates its origin. Attribution to a policy is a finding that exonerates the individual: and, if the policy ran after a hold should have suspended it, a preservation failure of a different kind. cflab. u k · e-disc ove r y. u k