Who Accessed Or Downloaded A Confidential Document

Understanding who accessed or downloaded a confidential document involves examining access trails across cloud platforms, file servers, and endpoints. This guide details what each record proves, retention policies, attribution methods, and common pitfalls for UK legal professionals.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/who-accessed-or-downloaded-a-confidential-document

DOCUMENT ACCESS EVIDENCE · A GUIDE FOR UK LAWYERS Who Accessed or Downloaded a Confidential Document Reading Access Trails Across Cloud Platforms, File Servers and Endpoints COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES ACCESS-LOG ANALYSIS

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: access is logged, and logs are not names 03 Cloud platforms: what Share Point, One Drive, Google Drive and SaaS record 04 File servers, DMS and end point s: the on-premises and local record 05 What each record proves: view, open, d own load, sync, print and share 06 Retention, licensing and the clocks that decide survival 07 From account to person: attribution and deployment 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: FILEACCESSISRECORDEDATTHEPLATFORM, THE SERVER AND THE END POINT, EACHNAMINGANACCOUNTRATHERTHANAPERSONANDEACHONITS OWNRETENTIONCLOCK: EXPORTTHELOGSFIRST, READWHATEACHEVENTACTUALLY MEANS, THENJOINACCOUNTTOPERSONWITHINDEPENDENTCORROBORATION

§ 02 · FIRST PRINCIPLES The problem in plain English: access is logged, and logs are not names

§ 03 · THECLOUDRECORD Cloud platforms: what Share Point, One Drive, Google Drive and SaaS record

§ 04 · THEON - PREMISESANDLOCALRECORD File servers, DMS and end point s: the on-premises and local record

§ 05 · WHATEACHEVENTPROVES What each record proves: view, open, d own load, sync, print and share

§ 06 · THECLOCKS Retention, licensing and the clocks that decide survival

§ 07 · FROMACCOUNTTOPERSON From account to person: attribution and deployment 99

§ 6's clocks), and leak inquiries where the access population narrows the candidates: the finding drafted to

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION SESSION COPY + PLATFORM END POINT PHYSICAL DELETED/ AUDIT LOG ARTEFACTS LAYER EXPIRED SIGN-IN / DOWNSTREAM LAYER RECIPIENT

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEBOARDPAPERANDTHEFORTY - ONEACCOUNTS EXAMPLE2 · THESERVERTHATWASNEVERLISTENING EXAMPLE3 · THE ACCESS THAT WAS AP REVIEW, ANDTHEDISCIPLINARYTHATWAS 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 · AC CESS - RECORDPRESER VAT I ON AND DISCLOSURE REQUEST

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

§ 13 · COMMON QUESTIONS Frequently asked questions Can we find out who opened a document on Share Point? How long do access logs last? The file server has no access logs. Is the trail cold? The log says my client's account accessed the record. Is that the end of it? Can access to a document be proved after it was deleted? Someone photographed the screen. Can that be traced?

§ 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

Can we find out who opened a document on Share Point?

Usually, within the audit retention window: the unified audit log records access, d own load, share and related events with the acting account, client and IP (§3): Example 1's forty-one accounts came from one search. The account is then joined to a person through §7's lattice, and the event type read for what it proves (§5): a preview is not a read.

How long do access logs last?

Months by default on the major platforms, longer with premium licensing or retention policies, days on busy on- premises servers, and anything from days to indefinite on SaaS systems (§6): the tenant's actual configuration is the first fact, and export is the first act. Logs allowed to expire after proceedings are contemplated are a preservation failure.

The file server has no access logs. Is the trail cold?

The server's trail never existed if audit in g was off (Example 2), but the endpoint's did: shortcut files, recent-file lists, sync databases and browser artefacts on the device that opened the file prove local access independently (§4, §8). Sequester the device before it is reissued; the trail is on it.

The log says my client's account accessed the record. Is that the end of it?

No: the event's semantics may be a preview or a search render (Example 3), the d own load may be a sync client's, and the account may have been used by someone else: the defensive lattice of §7 tests each. Access allegations built on a single log line without semantics, baseline or corroboration are the ones that fail at the hearing.

Can access to a document be proved after it was deleted?

Access events are recorded independently of the item's survival, so the audit log holds the history of a deleted document for its retention period; end point artefacts likewise persist (§8). The document's content may need guide 95 or 102's recovery; its access history is a separate, often longer-lived record.

Someone photographed the screen. Can that be traced?

Not from the platform: a camera leaves no access event beyond the open itself. The investigation narrows the population to accounts that had the document displayed at the relevant time (§5's open events), joins sessions to devices and rooms (§7), and examines the downstream image for screen artefacts, reflections and the platform's on-screen watermarks where deployed: bounded honestly, and some time s sufficient. 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 15 of 17