

OneDrive Evidence

OneDrive evidence is complex, involving cloud and device components. This guide details its anatomy, collection strategies, deletion recovery, exfiltration patterns, and common pitfalls, providing essential insights for UK legal professionals.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30. <https://e-discovery.uk/library/onedrive-evidence>

ONEDRIVE EVIDENCE · A GUIDE FOR UK LAWYERS One Drive Evidence Sync, Versions, Deleted Files and Sharing: the Personal Drive That Is Never Only in One Place COMPUTER FORENSICS LAB

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

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: one drive, two truths 03 Cloud-side anatomy: versions, recycle stages, sharing states 04 Device-side anatomy: the sync client's confessions 05 Collection: both halves, with the joins planned 06 Deletion, the leaver clock and recovery 07 Exfiltration patterns and how they prove 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: ONEDRIVEISTWOSOURCESWEARINGONENAME, AND THE CASE USUALLYLIVESINTHEIRDIFFERENCES

§ 02 · FIRST PRINCIPLES The problem in plain English: one drive, two truths

§ 03 · THE CLOUD HALF Cloud-side anatomy: versions, recycle stages, sharing states

§ 04 · THE DEVICE HALF Device-side anatomy: the sync client's confessions

§ 05 · GETTINGBOTH Collection: both halves, with the joins planned

§ 06 · GONE, GOING, KEPT Deletion, the leaver clock and recovery

§ 07 · THEPATTERNS Exfiltration patterns and how they prove

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE STORE + PART Y PERSONAL CLOUD THIRD- SHARED-OUT / LAYERS BACKUP ACCOUNTS SYNCED AUDIT / DELETED / DEVICES SIGN-IN RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEEMPTYDRIVEANDTHEDISCONNECTEDLAPTOP EXAMPLE2 · THE ANY ON E-LINKWITHATIMESTAMPEDAUDIENCE EXAMPLE3 · THEVERSIONHISTORYTHATAACQUITTEDTHEEDITOR

§ 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 · ONEDRIVELIMBFORTHECOLLECTIONSPECIFIC AT ION

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

§ 13 · COMMON QUESTIONS Frequently asked questions Files were deleted from One Drive six months ago, unheld. Gone? Can we tell if someone downloaded the whole drive before resigning? What does a sharing link actually prove? The custodian says the sync client "did things on its own". Plausible? How do One Drive and Share Point evidence differ? What single step most often decides One Drive matters?

§ 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

Files were deleted from One Drive six months ago, unheld. Gone?

From the cloud's own layers, yes: both recycle stages will have expired. The ensemble answer runs: any synced machine that disconnected or sat offline before processing the deletions (the time-capsule check comes first); third-party tenant backup sets; copies proliferated by sharing (recipients' drives and mailboxes); and the audit trail, if exported in time, proving what existed and when it went. Example 1 is the standard shape: cloud-clean, ensemble-rich.

Can we tell if someone downloaded the whole drive before resigning?

Usually, convergently: audit down load events (volume, cluster in g, folder coverage) plus device-side arrivals (the tree material is in g locally, hydration state flipping) plus onward traces (USB, uploads, personal sync). The report frames it against role baselines and canvasses the innocent twins: h and over packs and IT migrations produce similar shapes with different contexts: which is exactly the analysis that separates a finding from an accusation.

What does a sharing link actually prove?

Its records prove creation (account, time, link type, target item), configuration (anyone vs specified people, expiry, password) and access (events with timestamps and, for external access, source context): a mechanism- and-audience record. What they do not prove alone is the human intent behind creation: Example 2 needed the access pattern and the browser session to close that gap. Collect the states and events, then build the join: the link is the start of the proof, not its end.

The custodian says the sync client "did things on its own". Plausible?

Sometimes: clients do generate conflict copies, re-uploads after offline edits, and bulk activity on reconnection: shapes that can mimic deliberate action in the event stream. The client's own logs distinguish them: session context, error records, the difference between user-initiated and engine-initiated operations: which is one more reason the databases and logs are collected, and why event-stream conclusions are drawn with the client diary open beside them.

How do One Drive and Share Point evidence differ?

Mechanically little: One Drive is personal Share Point under the surface: versions, recycle stages and sharing behave alike. Evidentially much: One Drive is one custodian's world (attribution starts narrow), while Share Point is the shared estate (permissions and the pool come first, per guide 55 next). Files also migrate between them: a "personal" folder shared widely has become a library in practice: so scoping walks the actual sharing state, not the product name.

What single step most often decides One Drive matters?

The device census, run early and taken seriously: tenant device records plus client logs, every machine located and preserved. It finds the disconnected mirror (the account's time capsule), surfaces the personal-account sync, and defines the imaging plan the joins depend on. Cloud collection is the visible half of this source; the census is how the invisible half stops being

invisible. 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

Source: <https://e-discovery.uk/library/onedrive-evidence>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.