COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

OneDrive Evidence

Sync, Versions, Deleted Files and Sharing: the Personal Drive That Is Never Only in One Place

OneDrive for Business is where an individual's working files actually live: the drafts, the exports, the "personal" folder that turns out to matter: and its defining forensic property is duplication by design: every account exists simultaneously in the cloud and as synced mirrors on the user's machines, each side keeping records the other cannot. Add default versioning on every file, a two-stage recycle system with generous windows, and sharing links whose history is itself evidence, and OneDrive becomes one of the richest per-custodian sources in the tenant. This guide covers both halves and their joins: cloud-side collection with versions and sharing states, device-side sync artefacts and what they betray, deletion and its stages, the leaver clock, and the exfiltration patterns: mass downloads, personal-account sync, link sharing: that OneDrive matters keep turning on.

⏱ Estimated reading time: 26 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. OneDrive analysis anchors much of its employment and IP casework: cloud-side collection with version and sharing history, device-side sync artefact examination, and the two-sided correlation that turns "he downloaded everything" from suspicion into a dated, itemised finding. Its eDiscovery arm, **e-discovery.uk**, processes OneDrive collections at disclosure scale.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | CLOUD & SYNC FORENSICS | EXFILTRATION ANALYSIS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: ONEDRIVE IS TWO SOURCES WEARING ONE NAME, AND THE CASE USUALLY LIVES IN THEIR DIFFERENCES

Every OneDrive account is a pair: the **cloud side** (the tenant-held store, with per-file version histories on by default, a two-stage recycle system reaching back roughly three months, sharing links and permission states as data, and the audit layer recording access, downloads, sharing and deletion events) and the **device side** (the sync client's mirror on each enrolled machine, plus the client's own logs and databases recording what synced, when, from which folders, to which accounts: including personal accounts signed into the same client). Each side preserves what the other loses: cloud deletion leaves the device mirror intact until the client processes it (and forever, if the machine is offline or the client disconnected); device wiping leaves the cloud store untouched; version histories survive local overwrites; local artefacts (guide 41's recents, shellbags, USB records) capture what was done with files after they left the cloud's sight. The evidential method is therefore inherently two-sided: collect the cloud store stratigraphically (current files, versions, both recycle stages, sharing states) via guide 52's chosen route, image the devices per guides 41-48, and **difference the halves**: divergence is chronology (what was deleted where, when), and the joins (an audit-logged download appearing in device artefacts minutes later; a sharing link created cloud-side opened in a personal browser session device-side) are how exfiltration is proven to the standard this series requires. The governing clocks: the recycle windows, the leaver deletion pipeline (a departed employee's OneDrive follows their account into the grace-period countdown: guide 51's trap, with files), and audit retention: all answer to the week-one playbook, which is why this guide, like the whole block, begins with holds.

- **Versioning is on by default and deep:** hundreds of versions per file are routine: the drafting history of every document in the account, waiting for guide 50's differencing.
- **The recycle system is generous but finite:** two stages, roughly 93 days combined: after which unheld deletion is real, and the device mirror or backup layer carries the answer.
- **Sharing is data, not anecdote:** who a file was shared with, by what kind of link, when, and whether anonymously: collectable states plus audit events: the leak inquiry's backbone.
- **The sync client keeps its own diary:** logs and databases naming synced accounts (corporate and personal), folder mappings and transfer activity: the device-side record that catches personal-account sync red-handed.
- **Departed custodians' drives die on schedule:** the leaver clock applies to files as to mail: suspension day one, or the backup/counterpart architecture later.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: one drive, two truths

Ask where someone's files are and OneDrive's honest answer is "everywhere they've signed in": the tenant's store, the office desktop's mirror, the home laptop's mirror, the phone's app cache: each copy governed by its own deletion rules and each machine adding its own commentary about what was opened, copied and moved. Parties habitually collect one copy and reason as if it were the account: the cloud store alone ("the files were gone") while the home laptop's mirror holds everything; the laptop alone ("nothing here") while the cloud's versions and recycle stages hold the story. The account is the ensemble, and the differences between its copies are not noise: they are the events.

This guide's discipline is to treat every OneDrive question as a two-sided question from the first scoping call: which machines synced this account, where is each, what does the cloud hold at each layer: and to plan the correlation explicitly, because the joins are where mere presence becomes proof.

§ 0 3 · THE CLOUD HALF

Cloud-side anatomy: versions, recycle stages, sharing states

- **Current files with true metadata:** the store's files carry created/modified times and modifying-account attribution the platform maintains: collected with structure intact via the route guide 52 selects, with export mechanics that keep those properties.
- **Version histories per file:** default-on, per-save generations with author and timestamp: guide 50's finest-grain layer, collectable as series and differenced into drafting chronologies; version deletion and history trimming are audit-visible acts.
- **Two-stage recycle:** stage one (user recycle bin) then stage two (site-collection recycle) with a combined window around 93 days: deleted files enumerable with deletion dates and deleting accounts through the window: the deletion chronology's cloud source.
- **Sharing and permission states:** per-item shares (people, groups, link types including anyone-links, expiries, passwords) as collectable data, plus creation and access events in audit: the difference between "he must have leaked it" and "an anyone-link was created at 17:12 and first accessed from outside at 17:31".
- **Holds convert windows to permanence:** a held OneDrive preserves deletions and prior versions past every window: guide 53's hold logic, applied to files: and the hold's placement date is again the governing fact.

§ 0 4 · THE DEVICE HALF

Device-side anatomy: the sync client's confessions

- **The mirror itself:** the synced folder tree as last processed: which, on a disconnected or offline machine, is the account as at disconnection: the pre-purge snapshot that survives cloud-side clean-ups, and guide 53's OST logic for files.
- **Client logs and databases:** the sync engine's own records: accounts configured (business and personal, side by side), folder mappings, sync sessions and errors: the artefact that proves a personal OneDrive was signed in on the corporate laptop, with dates.
- **Files-on-demand states:** modern clients keep placeholders until content is opened; the local hydration state (which files were actually downloaded to disk) is itself usage evidence: a fully hydrated confidential folder on a personal device reads differently from placeholders.
- **The surrounding artefact record:** everything in guides 41-48 applies to the mirror's contents: recents and shellbags for what was opened, USB records for what moved onward, wiping traces for what was cleaned: the after-the-cloud story only the device tells.
- **Imaging over copying, as ever:** the client's databases, logs and the guide 50 shadow-copy layer ride only with full images: guide 32's method question, answered the same way here.

§ 0 5 · GETTING BOTH

Collection: both halves, with the joins planned

- **Cloud-side:** stratigraphic scope (current + versions + both recycle stages + sharing states), route per guide 52, export mechanics preserving attribution and structure, manifests and hashes: the standing disciplines, applied to the drive.
- **Device-side:** the machine census first (which devices synced this account: answerable from tenant device records and the client's own logs), then imaging per logistics, prioritised by the census and the matter.
- **The audit export beside both:** file access, download, sharing and deletion events for the account across the period (guide 57): the event stream the joins are built on: secured in week one regardless of collection timing.
- **Joins instructed, not hoped for:** the instruction names the correlations wanted: downloads to device arrivals, link creations to browser sessions, deletion events to mirror divergence: because two competent halves left unjoined is this source's signature failure (guide 51 §7).
- **Personal accounts flagged early:** where client logs show personal-account sync, the legal route to that account (guide 69 ahead: preservation requests, orders, undertakings) starts immediately: its own clocks are running too.

§ 0 6 · GONE, GOING, KEPT

Deletion, the leaver clock and recovery

- **The layer walk for files:** recycle stage one → stage two → window expiry: with holds suspending the whole march: every "the files were deleted" begins with which stage, what date, held or not: guide 53's four facts, translated.
- **Restore points cut both ways:** the platform's mass-restore capability (rolling a drive back after ransomware or mass deletion) can recover recent estates wholesale: and a restore performed mid-dispute rewrites the current state, which is why tenant operations stay inside the protocol's log.
- **The leaver pipeline:** account deletion queues the OneDrive for removal after the grace period (retention policies and holds can preserve content beyond it): the suspension instruction, the day the custodian list exists, decides whether this paragraph is administrative or archaeological.
- **After the windows:** the architecture: device mirrors (especially disconnected machines), third-party tenant backups, shared-out counterpart copies, and the audit trail of the deletion itself: the recovery plan, and frequently sufficient.

§ 0 7 · THE PATTERNS

Exfiltration patterns and how they prove

- **Mass download:** audit's download events in volume and cluster (the folder tree pulled in one evening), matched to device-side arrivals and onward USB or upload traces: dated, itemised, and framed against role-normal usage before adjectives are chosen.
- **Personal-account sync:** the client's dual-account records plus transfer activity: corporate files appearing in the personal mirror: with the personal account then pursued legally: the pattern guide 46's Example 1 sketched, proven from the sync layer.
- **Link sharing outward:** anyone-links and external shares created on sensitive items, with creation and first-access events: the leak mechanism that leaves the cleanest trail of all, because both halves of it are platform-recorded.
- **The pre-departure pattern:** hydration of dormant folders, downloads outside role norms, link creation, then deletion: the sequence read as a whole across audit, versions and device artefacts: and its innocent twins (role change, handover preparation, IT migration) canvassed per the CPR 35 duty before anything is pleaded.
- **Defence symmetry, as always:** the same records establishing role-consistent access, IT-initiated transfers, or an accusation's timeline that the audit stream contradicts: the layers exonerate with the same mechanics.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the OneDrive in isolation. The account's evidence spans: the cloud store and its layers; every synced device (mirrors, client logs, surrounding artefacts); mobile apps (cached files and access records); the audit and sign-in layers; third-party tenant backups (point-in-time drives across months); shared-item counterparts (every shared file exists in recipients' visibility, and copies proliferate); SharePoint (where "OneDrive" folders are shared libraries in disguise, guide 55's territory); personal cloud accounts reached by sync or upload (guide 69); and USB and external media where files moved onward (guides 47-48). When the account's own layers have expired: the disconnected mirror, the backup product and the shared-out copies are the recovery plan, and the audit export taken in week one frames what existed.

EVIDENCE	CLOUD STORE + LAYERS	SYNCED DEVICES	AUDIT / SIGN-IN	THIRD-PARTY BACKUP	SHARED-OUT / PERSONAL ACCOUNTS	DELETED / RECOVERABLE
Files (content)	Y + versions + recycle	Mirrors: as last synced	n/a	Y where deployed	Recipient copies: Y	Windows + hold governed
Drafting history	Y: version series	Shadow copies of mirror	Edit events	Generational states	As-shared generations	Guide 50 layers
Deletion chronology	Recycle stages: dated	Mirror divergence	Y: deletion events	Bracketing sets	n/a	The march is enumerable
Sharing / leak route	Sharing states	Browser + client artefacts	Y: creation + access events	Point-in-time states	The destination itself	Varies
Onward movement	n/a	Y: USB, uploads, recents	Download events	n/a	Arrival records	Guides 47-48

Fallback strategy in one line: when the cloud has forgotten, find the machine that stopped syncing: the disconnected mirror is this source's time capsule: then the backup product, then the recipients of every share.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE EMPTY DRIVE AND THE DISCONNECTED LAPTOP

A departing consultant's OneDrive was inspected a month after he left: near-empty, recycle stages barren, "nothing to see". The audit export said otherwise: eleven hundred deletion events across two evenings in his notice period: but the window had passed and the content seemed gone. The census found the time capsule: his old laptop, swapped out mid-notice for a replacement and sitting in IT's returns cupboard, its sync client disconnected the day of the swap. Its mirror held the account as at that date: the full drive, pre-purge: and its artefact record held the rest: the folder tree copied to a USB device (serial preserved for guide 47 treatment) the evening before the swap. The cloud had been cleaned; the ensemble had not.

EXAMPLE 2 · THE ANYONE-LINK WITH A TIMESTAMPED AUDIENCE

A confidential pricing model reached a competitor; suspicion fell on a commercial manager with drive access. The sharing analysis replaced suspicion with a sequence: an anyone-link created on the model at 17:12 on the Thursday (audit event, her account), first external access at 17:31 from a non-corporate address, six further accesses over the weekend, the link deleted Monday 08:04. Her defence: link created for a legitimate agency review: collapsed against the access pattern (the agency's addresses were known and absent) and her browser history's webmail session at 17:14. The device half and the cloud half had each recorded their portion; together they were a timeline no explanation survived.

EXAMPLE 3 · THE VERSION HISTORY THAT ACQUITTED THE EDITOR

A finance analyst was accused of doctoring a forecast after board sign-off: the file's modified date fell squarely in the accusation's window and her account was the modifier. The version series told a longer story: forty-one versions across three months, the disputed figures stable through the sign-off version, then a change in version 39: authored not by her but by her director's account, four days before the modification attributed to her: whose own version 40 was a formatting save. The audit stream corroborated: his session, his edit event, her subsequent open-and-save. The accusation had read the last touch as the only touch; the history read the sequence. She was cleared in a week; the enquiry moved one office up.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **One-half collection:** cloud without devices or devices without cloud: Example 1's case, lost either way alone.
- **The census skipped:** synced machines never enumerated; the disconnected mirror never found.
- **Versions uncollected:** current-state exports in a drafting-history dispute: Example 3's acquittal, forfeited.
- **Sharing states ignored:** leak inquiries run on interviews while the link records sit unread.
- **Last-touch attribution:** the modified-by field read as the whole story: Example 3's near-miss.
- **Leaver drives deleted on schedule:** the suspension email unsent, again.
- **Joins left to review:** correlation nobody instructed, discovered missing at report stage.
- **Mid-dispute restores and tidy-ups:** tenant operations outside the protocol rewriting the evidence's current state.

Technical limitations

- **Windows expire:** unheld recycle stages and audit retention are finite: the architecture paths are the recourse, and week one the prevention.
- **Version series are save-grained:** per-save states, not keystrokes; co-authoring interleaves per guide 50's caution: claims sized to the grain.
- **Files-on-demand thins mirrors:** placeholder-heavy mirrors hold less content than they appear to; hydration state is read before the mirror is promised as a capsule.
- **Audit granularity is licence- and event-dependent:** guide 57's caveats govern; download and access claims match the events actually logged.
- **Attribution remains layered:** account events plus device correlation plus the human layer: the platform names accounts, and this series' standing discipline names people.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which devices have synced this account: tenant device list and client records: and where is each machine now?
- Hold status and date for the OneDrive; recycle window; leaver pipeline position if departed?
- What sharing was legitimate for this custodian's role: the baseline the patterns are read against?

Ask your opponent

- Please confirm hold status and placement date for [custodian]'s OneDrive, and that collection included version histories, both recycle stages and sharing/permission states.
- Please identify all devices that have synchronised the account in [period], their current whereabouts, and preserve each pending imaging.
- Please produce the audit events for the account (access, download, sharing, deletion) for [period], and particulars of any restore or mass operation performed since [date].

Ask your eDiscovery / forensic provider

- What does the two-sided plan look like here: census, imaging priority, cloud scope, and the joins to build?
- What do the version series and sharing states show for the documents in issue?
- Where the windows have run: which architecture paths are live, and in what order?

SUGGESTED WORDING · ONEDRIVE LIMB FOR THE COLLECTION SPECIFICATION

> "For each custodian at Schedule A: (a) the OneDrive shall be collected including current content with folder structure, complete version histories, both recycle-bin stages with deletion metadata, and sharing and permission states as structured data; (b) the unified audit log events for the account (access, download, sharing, deletion, restore) for [period] shall be exported and preserved; (c) all devices that have synchronised the account shall be identified from tenant and client records, preserved, and forensically imaged, the sync client's databases and logs being within scope; and (d) the report shall correlate cloud-side events with device-side artefacts for the matters at Schedule B, stating hold status and window facts per account and the innocent explanations canvassed."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The OneDrive checklist

- ☐ Hold placed day one; leaver pipeline suspended; window facts documented
- ☐ Device census run from tenant and client records; machines preserved
- ☐ Cloud collection stratigraphic: content, versions, both recycle stages, sharing states
- ☐ Audit events exported for the full period in week one
- ☐ Devices imaged, not copied; client databases and logs in scope
- ☐ Joins instructed by name: downloads↔arrivals, links↔sessions, deletions↔divergence
- ☐ Version series differenced for the documents in issue; last-touch attribution refused
- ☐ Personal-account indications escalated to the guide 69 route immediately
- ☐ Patterns framed against role baselines; innocent twins canvassed on the record
- ☐ No tenant restores or tidy-ups outside the protocol's log

Red flags

- An "empty" drive with a deletion-heavy audit stream.
- A sync'd machine nobody can produce.
- Anyone-links on sensitive items with external first-access events.
- A personal account in the client's configuration.
- Version histories trimmed or absent on the disputed documents.
- A mass restore performed after proceedings intimated.
- Accusations resting on the modified-by field alone.

When to involve a digital forensic expert

At the census, where finding every synced machine: including Example 1's cupboard laptop: is the step that decides what can be proven; at collection, for the stratigraphic cloud scope and the imaging discipline the client databases require; at correlation, where the joins are built to report standard; and in every exfiltration and authenticity matter, where the version, sharing and audit layers carry the finding and the innocent-explanation duty carries the credibility. Both directions are standing work: Examples 2 and 3 are the same machinery pointed opposite ways: reported under CPR Part 35 with windows, grains and limits stated, and processed through **e-discovery.uk** so review sees the drive's story, not its noise.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Files were deleted from OneDrive 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 download events (volume, clustering, folder coverage) plus device-side arrivals (the tree materialising locally, hydration state flipping) plus onward traces (USB, uploads, personal sync). The report frames it against role baselines and canvasses the innocent twins: handover 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 OneDrive and SharePoint evidence differ?

Mechanically little: OneDrive is personal SharePoint under the surface: versions, recycle stages and sharing behave alike. Evidentially much: OneDrive is one custodian's world (attribution starts narrow), while SharePoint 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 OneDrive 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.

§ 14 · REFERENCE

Glossary

Anyone-link
A share link usable without sign-in; the leak mechanism with the cleanest trail.

Census (device)
The enumeration of every machine that synced the account; this source's first step.

Conflict copy
Client-generated duplicate from divergent edits; engine activity, not user intent.

Files-on-demand
Placeholder mode; hydration state records what was actually downloaded.

Hydration
A placeholder becoming local content; usage evidence in itself.

Mirror
The synced local folder tree; disconnected, the account's time capsule.

Restore (drive)
Platform mass-rollback; recovery tool and, mid-dispute, state-rewriter.

Sharing state
Per-item share and link configuration as collectable data.

Two-stage recycle
User then site-collection bins; the bounded march guide 53 walks for mail.

Version series
Default per-save generations; the drafting history layer.

Sources and authoritative references

The account disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (OneDrive and sync forensics, exfiltration analysis, version and sharing examination, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (two-sided cloud-and-device collection at disclosure scale): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft documentation: OneDrive retention and deletion: learn.microsoft.com, retention and deletion · learn.microsoft.com, Purview eDiscovery
- PD 57AD and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- ICO, UK GDPR guidance: ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

OneDrive matters run two-sided at the laboratory by default: the device census from tenant and client records; stratigraphic cloud collection by the guide 52 route with versions, recycle stages and sharing states; imaging that keeps the client's diary; audit exports in week one; and the joins: downloads to arrivals, links to sessions, deletions to divergence: built to report standard with role baselines and innocent explanations on the record. Examples 1-3 are the practice's recurring shapes: the cupboard laptop, the timestamped link, the acquitting version series. Reporting is CPR Part 35 throughout; personal-account discoveries route straight into the legal-preservation track; and through **e-discovery.uk** the collected ensemble is processed so review sees the story. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a leaver's drive or a returned laptop is in a pipeline somewhere, the suspension call comes first.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace