Cloud Evidence Is Not Just Files

Cloud evidence extends beyond files to include versions, logs, permissions, sharing links, deleted objects, configuration, and admin records. These seven layers often contain the critical evidence in a case, proving facts that files alone cannot. Understanding and collecting these layers is crucial for UK litigators.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/cloud-evidence-is-not-just-files

CLOUDEVIDENCEBEYONDFILES · A GUIDE FOR UK LAWYERS Cloud Evidence Is Not Just Files Versions, Logs, Permissions, Sharing Links, Deleted Objects and Admin Records: the Seven Layers Around Every Cloud Document COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the estate around the document 03 The seven layers, named 04 What each layer proves that files cannot 05 Scoping and request in g the layers, platform-neutrally 06 Collecting the layers: routes, fidelity, integrity 07 Correlation: turning layers into findings 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: INCLOUDPLATFORMSTHEFILEISONELAYEROFSEVEN, AND THEOTHERSIXAREUSUALLYTHECASE

§ 02 · FIRST PRINCIPLES The problem in plain English: the estate around the document

§ 03 · THEMAP The seven layers, named LAYER WHAT IT IS · WHERE THE BLOCK MET IT 1 · Versions / revisions Per-save series (SharePoint/OneDrive, guide 54-55) or per-edit streams (Google Docs, 3 · Permissions The computed possibility map with inheritance and group resolution: guide 55's discipline: 4 · Sharing links / external Link types, audiences, expiries, first-access events: guide 54's leak machinery: the 5 · Deletion / recycle records Staged bins, deletion metadata, restore events: guides 53-55's marches: the acts that 6 · Configuration / settings Retention rules, history toggles, sharing policies, version limits, with change dates: guides 7 · Admin / operations Role use, account lifecycle, hold/search/export operations: guides 51, 57 and 59's

§ 04 · THEPROOFS What each layer proves that files cannot

§ 05 · ASKINGPROPERLY Scoping and request in g the layers, platform-neutrally

§ 06 · GETTINGTHELAYERSOUT Collecting the layers: routes, fidelity, integrity

§ 07 · THE METHOD Correlation: turning layers into findings

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives LAYER EXTENDED

PLATFORM DEVICE COUNTERPARTS / BACKUP DELETED / (PRIMARY) SIDE RECIPIENTS LAYER RECOVERABLE SIEM / LOGS 1 · Versions Y: series via Shadow n/a As-shared Generational Pruning/trimming 2 · Events Y, window- Local Y: longer Their event layer Backup's Windows 3 · Now-state + n/a Change Membership Point-in-time Reconstructable 4 · Sharing States + use Browser/ Access The recipients States in Varies 5 · Deletions Recycle Mirror Deletion n/a Bracketing Acts outlive 6 · Settings Current + n/a Config- n/a Historic The conduct 7 · Y: the Admin Where n/a n/a Window-bound;

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEPRODUCTIONTHATWASTECHNICALLYCOMPLETE EXAMPLE2 · THELEAKWITHAFOUR - LAYERSIGNATURE EXAMPLE3 · THELAYERSTHATCLEAREDTHEESTATE

§ 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 · L AY ERSCHEDULECLAUSEFORTHEDISCLOSURE SPECIFIC AT ION

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

§ 13 · COMMON QUESTIONS Frequently asked questions Isn't this just metadata by another name? Which layers should a standard commercial dispute actually collect? The opponent says their platform "doesn't keep that". How do we test it? Can layers be fabricated or edited the way documents can? How does this model apply to platforms outside Microsoft and Google? What is the single highest-value habit this guide recommends?

§ 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

Isn't this just metadata by another name?

Broader and more organised: "metadata" usually means fields on files (layer zero's own properties); the layer model covers the platform's separate record systems: series, events, states, histories, operations: most of which are not on or in the file at all and are missed precisely because they are not. Naming seven layers gives requests, schedules and reports a fixed structure that "please include metadata" never achieved.

Which layers should a standard commercial dispute actually collect?

By default: layer 2 exported estate-wide in week one (it expires; it is cheap); layers 5-6 wherever deletion or "routine" is in issue; layer 1 as series for the documents the case turns on; layers 3-4 where access or audience is disputed; layer 7 where process or conduct is. The schedule scales with the issues: the discipline is deciding per population, on the record, rather than defaulting to zero.

The opponent says their platform "doesn't keep that". How do we test it?

Platform-neutral request first (§5's wording), then the documentation: every major platform's layer capabilities are publicly documented, and "doesn't keep" usually means "didn't look", "didn't license" or "let it expire": three different answers with three different consequences. Ask which, in terms; request the settings and operations layers that would show it; and remember that a lapsed window after a preservation letter is not a technical answer but a conduct one.

Can layers be fabricated or edited the way documents can?

Far less readily: platform-maintained series, events and operations records are not user-editable, which is much of their weight: the realistic vulnerabilities are at export (curation, scope) and interpretation: met by documented queries, retained self-describing exports, verification patterns and grain honesty. In practice the layers are where fabrication of documents goes to die, not a new place for it to live: Example 1's version series being the standing illustration.

How does this model apply to platforms outside Microsoft and Google?

Directly: it is the interview you conduct with any SaaS estate: does it version, does it log, how are permissions computed, what are the sharing mechanisms, what survives deletion and for how long, what settings histories exist, what does the admin layer record: seven questions that scope Dropbox, Slack, Salesforce or a bespoke system in an after no on. The SaaS guides ahead (112-114) are this interview, conducted platform by platform.

What is the single highest-value habit this guide recommends?

The week-one layer export: events and operations, full window, hashed and shelved, every cloud matter, before anyone knows whether they will matter: guide 57's instruction generalised to the whole estate. It is cheap, it is quick, it expires if skipped, and Examples 1-3 all rest on someone having done it: or on the other side having not. 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