



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Document Management Systems in Disclosure

iManage, NetDocuments and the Version History That Decides Professional Disputes

Law firms, accountants, agencies and in-house teams keep their working documents in a DMS: iManage, NetDocuments, SharePoint dressed as one, or a legacy equivalent: and when the dispute is about the work itself (the drafting error, the missed clause, the advice that changed between versions), the DMS is the primary witness. Every saved version numbered and dated, every open and edit logged against a user, every email filed to the matter workspace: a professional-negligence chronology waiting to be extracted properly, or spoiled by a collection that flattens versions into final PDFs. This guide covers DMS anatomy for litigators, version and access histories, matter-centric collection, privilege complications when the DMS belongs to a firm, and the audit layers that show who looked at what and when.

© Estimated reading time: 25 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. DMS collections feature across its professional-negligence, partnership and departing-fee-earner casework: version-preserving extraction from iManage and NetDocuments, access-history analysis, and matter-workspace collections that keep the drafting record intact. Its eDiscovery arm, **e-discovery.uk**, hosts DMS estates with versions reviewable side by side.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

DMS & VERSION FORENSICS

ACCESS-HISTORY ANALYSIS

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the drafting record as witness
- 03 DMS anatomy: workspaces, profiles, versions and filed email
- 04 Histories: versions, access logs and activity trails
- 05 Collection: extracting matters without flattening them
- 06 Privilege and third-party complications
- 07 Departing fee earners and DMS exfiltration
- 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

Executive summary

THE HEADLINE POINT: THE DMS KEEPS EVERY VERSION AND LOGS EVERY TOUCH: COLLECT IT SO BOTH SURVIVE

A DMS records two things litigation prizes: **the drafting record** (numbered, dated versions of every document, showing exactly how the advice, contract or report evolved and who saved each step) and **the access record** (who opened, edited, printed, emailed or exported what, when). Professional-negligence, partnership and departing-fee-earner disputes are decided in these layers: the clause present in version 6 and absent in version 7; the file opened by the departing partner forty times in his last week. The craft is preserving both: collection must be version-complete and history-complete (a folder of final PDFs is spoliation by export), privilege must be handled matter by matter where the DMS belongs to a firm, and the audit trails: retention-bound: must be frozen before they rotate.

- **Versions are the evidence:** the drafting sequence, not the final document, answers how the error happened: collected complete with metadata.
- **Access logs answer who and when:** opens, edits, prints and exports per user: the conduct layer, retention-bound and frozen early.
- **Matter-centric collection:** the workspace (documents, versions, filed email, notes) is the natural unit: extracted whole, not cherry-picked.
- **Flattened productions are challengeable:** final-version-only exports destroy the record the dispute needs: refuse and demand natively.
- **Firm-held DMS raises privilege mechanics:** other clients' matters, the firm's own advice: scoped and filtered per the intermediary model.

The problem in plain English: the drafting record as witness

When the claim is that the professional got it wrong, the question is nearly always historical: what did the draft say at each stage, who changed it, what did they know when they changed it, and who reviewed the change? Memory answers unreliably and self-servingly; the DMS answers precisely: version 4 saved by the trainee at 18:22, version 5 by the partner at 09:10 with the limitation clause deleted, the client email attaching version 5 filed at 09:31. The system was built for knowledge management; it functions as a deposition of the drafting process.

The equal and opposite hazard: this record is fragile in collection. Export routines default to latest versions; migrations shed history; audit trails rotate on configurable windows. The party who requests "the documents" receives finals and loses the case's chronology; the party who requests versions, profiles and activity logs by name: this guide's §11: receives the witness intact.

DMS anatomy: workspaces, profiles, versions and filed email

- **Matter workspaces:** the organising unit: documents, folders, filed email and notes grouped per matter or client: the natural collection scope, and the container security answers "who could see".
- **Document profiles:** the metadata card: author, operator, dates, matter and client codes, document type, custom fields: searchable structure the file system never had, and the profile history is itself evidence.
- **Versions:** numbered saves with per-version author, date and comments: the drafting record: including check-in/check-out data showing who held the document locked and for how long.
- **Filed email:** messages filed to matters from Outlook with their metadata: often the most complete matter correspondence set available, and collected as part of the workspace.
- **Links, related documents and compares:** attachments-as-links, related-document references, and saved comparison documents (the redline someone ran between versions 6 and 7 is frequently the best exhibit in the case).

Histories: versions, access logs and activity trails

- **Version history:** the per-document ladder: number, author, date-time, comment, size: read as a chronology, with gaps (deleted versions) visible in the numbering.
- **Document activity logs:** opens, edits, prints, copies, emails and exports per user with timestamps: platform- and configuration-dependent in depth and retention: the access record frozen and exported in week one.
- **Security and ACL history:** who was granted or denied access to workspaces and documents, and when it changed: the "ethical wall raised late" evidence in conflicts disputes.
- **Search and browse trails:** where logged, what users searched for and which results they opened: powerful in exfiltration matters (the departing partner searching "top clients billing" is its own exhibit).
- **Admin trails:** deletions, profile edits, security changes and export jobs by administrators: read for mid-dispute acts per this series' standing trail-integrity rule.

Collection: extracting matters without flattening them

- **Version-complete export:** every version as a distinct file with its metadata, or database-level acquisition preserving the ladder: named explicitly in the collection specification, because default exports flatten.
- **Profile and history capture:** metadata, version tables and activity logs exported alongside content: the histories are first-class evidence, not system exhaust.
- **Workspace-scoped collection:** the matter as the unit: documents, filed email, notes: with cross-matter duplicates handled by hashing downstream, not by pre-filtering that guesses at relevance.
- **Reproducibility bundle:** per guide 71 §5: what was queried, when, counts and hashes: DMS collections verified like any structured extraction.
- **Review with versions intact:** hosting that renders version ladders and compares side by side: through **e-discovery.uk**, the drafting sequence reviewable as a sequence.

Privilege and third-party complications

- **The client's matter in the firm's system:** in negligence claims the former client is generally entitled to their matter file: the workspace collection scoped to their matters, with the firm's separate self-advice (post-dispute internal counsel workspaces) identified and treated distinctly.
- **Other clients everywhere:** the DMS holds every client: collections scoped hard to the relevant matters, and any broader forensic work (activity analysis across the system) run by an independent examiner under protocol so other clients' material never reaches the parties: guide 68's intermediary model, DMS edition.
- **Joint and common-interest wrinkles:** shared workspaces, co-advised matters, secondees' access: the privilege map drawn before extraction, not litigated after.
- **Privilege in versions:** earlier drafts may embed advice later removed: version-level privilege review is real work, planned into the protocol.
- **Regulatory and SRA overlays:** confidentiality duties survive the dispute: handling, undertakings and destruction terms written into every DMS protocol.

Departing fee earners and DMS exfiltration

- **The pre-departure signature:** access spikes on client and precedent material outside the leaver's live matters, bulk opens, print runs and exports in the notice period: read from activity logs against the departure chronology, per guide 73 §5's method.
- **Export and email-out events:** documents emailed to personal accounts (guide 69's trail), exported to local drives, or synced offline: each logged where configuration permits, each correlated with device artefacts per guide 41.
- **Precedents and know-how:** the firm's drafting bank as taken property: access patterns on precedent workspaces are the team-move case's quiet second front.
- **Search trails as intent:** §4's browse evidence: what the leaver went looking for, before taking it.
- **The fair reading:** fee earners legitimately access much; the finding is pattern against baseline: volume, breadth beyond live matters, timing against notice: stated to its rung, per the standing fairness rule.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the DMS is the hub of a wider drafting estate. The record also lives in: local copies and offline sync caches on fee earners' devices (echo copies with their own timestamps); the email estate carrying drafts as attachments (each a frozen version with transmission context: guides 53, 69); document comparison outputs saved or emailed; backups and archived matters holding what migrations shed; the client's own copies of everything sent (the counterpart layer that verifies the firm's production); co-adviser and counsel systems in multi-firm matters; and print/cost-recovery logs dating hard-copy runs. When the DMS history is incomplete: rotated logs, migrated matters: the attachments trail and the client's inbox rebuild the version chronology from outside.

EVIDENCE	DMS (NATIVE)	DEVICE / SYNC CACHES	EMAIL ESTATE	BACKUPS / ARCHIVES	CLIENT & CO-ADVISER COPIES	DELETED / RECOVERABLE
Versions	Y: the ladder	Offline copies	Attached drafts, dated	Pre-migration ladders	As-sent versions	Ladder gaps rebuilt from echoes
Access / activity	Y: retention-bound	Open/edit artefacts	Send events	Log archives sometimes	n/a	Frozen early or lost
Filed correspondence	Y: matter-filed	OST/PST caches	Y: the source	Y	Their mailboxes	Multi-copy, resilient
Deletions	Admin trails, version gaps	Cache survivals	Attachment copies	Pre-deletion states	Their intact set	The act datable; content from echoes
Exfiltration events	Export/email logs	Guide 41's artefacts	Personal-account trail	n/a	Recipient side	Chain per guides 41/69

Fallback strategy in one line: when the DMS record thins, the attachments trail and the client's copies rebuild the versions, and the device layer rebuilds the conduct.

Worked examples

EXAMPLE 1 · THE CLAUSE THAT VANISHED BETWEEN VERSIONS

A negligence claim alleged a firm deleted a critical indemnity cap from a supply agreement without advising the client. The version ladder answered in four rows: the cap present through version 8; version 9, saved by the supervising partner at 21:47 the night before completion with the comment "client changes per call", cap absent; no attendance note of any call; and the activity log showing the client partner never opened version 9 before it was sent. The client's own inbox: the counterpart layer: held version 8 as last received, version 9 arriving only as the execution copy. The firm's case that the client instructed the deletion did not survive its own system's chronology.

EXAMPLE 2 · THE PARTNER WHO READ NINETY FILES IN A WEEK

A two-partner team resigned for a rival. The DMS activity export, frozen the same day, showed one partner's final fortnight: ninety-one client workspaces opened against a baseline of a dozen; the billing-report precedent opened six times; forty-two documents emailed to an address one letter off his firm account (the personal-Gmail trail of guide 69); and search logs including "panel appointment letters" and "fee agreements 2024". Device forensics matched twenty-two of the emailed documents' hashes on his home laptop. The springboard injunction was granted on the pattern-against-baseline analysis, with the judgment adopting the fortnight table verbatim.

EXAMPLE 3 · THE FLATTENED PRODUCTION, UNFLATTENED

In a partnership valuation dispute, one side produced "the complete drafting file": 240 final PDFs, no versions, no metadata. The §11 challenge forced a native re-collection: the version ladders showed the disputed goodwill schedule had existed in eleven versions, with the contested figure appearing only in version 11: created three weeks after the valuation date it bore, by the producing party's own login, the earlier versions all carrying the higher figure. The flattening had not been neutral: it had removed precisely the ladder that dated the change. Costs of the re-collection followed the flattener, and the figure reverted to version 10's.

Common mistakes and technical limitations

Common mistakes

- **Finals-only requests and productions:** Example 3's flattening: the record's chronology destroyed by export default.
- **Activity logs left to rotate:** the conduct layer's retention window spent on correspondence.
- **Filed email forgotten:** the matter's correspondence collected from mailboxes alone, the DMS's curated set ignored (or vice versa: one without the other).
- **Cross-client spillover:** broad forensic sweeps run without the intermediary protocol: other clients' privilege breached in the name of diligence.
- **Comparison documents missed:** the saved redlines: the case's best exhibits: unrequested.
- **Migration boundaries unmapped:** "no history before 2022" treated as suspicious or final instead of traced to the migration and its archives.
- **Baseline-free conduct claims:** access volumes pleaded without the leaver's normal pattern: the fairness gap opponents drive through.

Technical limitations

- **Log depth and retention are configured:** what was recorded, and for how long, is an implementation fact established first.
- **Version ladders start at filing:** pre-DMS drafting (local files, email rounds) predates the ladder: the echoes of §8 fill backwards.
- **Login is not hand:** shared logins and secretarial saves need the attribution ladder: the version's author field names the credential.
- **Cloud DMS mediates access:** SaaS platforms constrain database-level work: provider export and API routes govern, audited per deployment.
- **Deleted-version recovery is layer-bound:** admin trails date the act; content returns from backups and echoes or not at all: promised never, per the standing rule.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which platform and version, what activity logging is on, and what are its retention windows: frozen today?
- Which matters and workspaces carry the dispute: and where are the migration archives for anything older?
- For leaver cases: is the activity export run, and are the suspect's credentials revoked?

Ask your opponent

- Please produce the relevant matter workspaces natively and version-complete: all versions of each document with profile metadata, version comments, filed email and saved comparisons: not final versions alone.
- Please produce the document activity logs (opens, edits, prints, emails, exports) and security/ACL history for the workspaces and period, stating the logging configuration and retention applicable.
- Please confirm whether any versions or documents have been deleted and produce the administrative trails recording any such acts.

Ask your eDiscovery / forensic provider

- Does the collection preserve the ladders and histories: and what does the reproducibility bundle show?
- What does the version chronology say about the disputed drafting: and what do the echoes add?
- For conduct claims: what is the baseline, and does the pattern clear it?

SUGGESTED WORDING · DMS LIMB FOR THE PRESERVATION LETTER

"Your client must immediately preserve all document management system data relating to the issues, including: (a) the relevant matter workspaces in full: all documents with all versions, profile metadata, version comments, filed email, notes and saved comparison documents: none of which may be deleted, re-profiled or migrated; (b) all document activity logs, access histories and security or permission records for those workspaces, whose rotation or purge must be suspended and which should be exported forthwith where retention cannot be extended; (c) all administrative and audit trails; and (d) all backups and archived matters covering the period. Any export for disclosure must be version-complete and metadata-preserving; production of final versions alone will not be accepted as compliance."

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

The DMS checklist

- ☐ Platform, logging configuration and retention windows established day one
- ☐ Activity logs exported before rotation; admin trails reviewed
- ☐ Workspaces collected version-complete with profiles and filed email
- ☐ Saved comparisons and related documents included
- ☐ Privilege map drawn; intermediary protocol for any cross-client work
- ☐ Migration archives located for pre-migration history
- ☐ Conduct analyses run against per-user baselines
- ☐ Echo layers joined: attachments trail, client copies, device caches
- ☐ Flattened opposing productions challenged per §11
- ☐ Reproducibility bundle retained for every extraction

Red flags

- Version gaps in the numbering around the disputed change.
- Late-night saves with comments no attendance note supports: Example 1's 21:47.
- Access spikes beyond live matters in notice periods: Example 2's ninety-one.
- Finals-only productions resisting native re-collection: Example 3.
- Documents bearing dates their version ladders contradict.
- ACL changes walling off workspaces after the dispute arose.
- Export or email-out events to near-miss personal addresses.

When to involve a digital forensic expert

At preservation, where logging retention sets the clock; at collection, where version-complete extraction and the reproducibility bundle are craft; at analysis, where ladders become drafting chronologies, activity becomes baselined conduct findings, and echoes rebuild what the system shed (Examples 1-3's machinery); and at reporting under CPR Part 35 with configurations and rungs stated. Through **e-discovery.uk**, DMS estates are hosted with ladders and compares reviewable in sequence beside the correspondence per guide 70.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is a former client entitled to the firm's DMS versions, or only the final file?

In negligence litigation, the drafting record for the client's matters is squarely disclosable: versions, profiles and activity are documents within the firm's control bearing directly on the pleaded work: and finals-only production meets Example 3's challenge. The firm's separate post-dispute self-advice is its own privileged stream, identified and carved out rather than used to fog the matter file.

Can the DMS prove who actually made a disputed edit?

To the credential, yes: version author, check-out records and activity logs name the login and time: and the hand behind it runs the standard ladder: secretarial-save practices, shared logins and delegation established from the firm's working patterns, device artefacts where it matters. Version comments and the surrounding email round usually complete the attribution the author field starts.

The firm migrated DMS three years ago and history "starts" there. Suspicious?

Usually structural: migrations commonly carry latest versions and shed ladders: the finding is the boundary's date against the migration records, then the rebuild: pre-migration backups and archives, the attachments trail (every emailed draft is a dated version), and the client's own set. Suspicion attaches only where the boundary's timing or selectivity tracks the dispute rather than the project plan.

What can be proved about a fee earner who "just looked" at files before leaving?

Access alone proves access: the finding becomes conduct through pattern against baseline (volume, breadth beyond live matters, timing), pairing with output events (prints, exports, emails out), and the downstream chain on devices and personal accounts per guides 41 and 69: Example 2's construction. Looking is lawful; the fortnight table is what tribunals act on.

Our opponent's DMS is cloud-hosted. Does that change anything?

Route, not obligation: SaaS platforms constrain database-level acquisition, so collection runs on the platform's export and API facilities: capability audited per deployment, the version-complete and history-complete requirements unchanged, and provider retention (activity-log windows especially) making the early freeze more urgent, not less.

Are saved document comparisons really that important?

Repeatedly decisive: a saved or emailed redline is a contemporaneous statement of exactly what changed between versions, made by the parties themselves, with a date: it collapses "nobody noticed the deletion" defences (someone ran the compare) and anchors drafting chronologies without expert reconstruction. They are requested by name in every DMS matter for that reason.

§ 1 4 · REFERENCE

Glossary

ACL history

The record of workspace and document permission changes.

Activity log

Per-document opens, edits, prints, emails and exports by user.

Check-out

The exclusive-edit lock; its records show who held a document when.

Filed email

Correspondence saved to the matter workspace with metadata.

Flattening

Export that discards versions and metadata; the challengeable production.

Matter workspace

The per-matter container; the natural collection unit.

Profile

The document's metadata card: authorship, codes, dates, custom fields.

Saved comparison

A stored redline between versions; frequently the key exhibit.

Version ladder

The numbered sequence of saves; the drafting record.

Version comment

The per-save annotation; contemporaneous and quotable.

Sources and authoritative references

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

- cflab.uk, digital forensics services (DMS forensics, version-chronology analysis, activity baselining, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation, Phase 03 · Collection and Phase 05 · Review (log-window preservation; version-complete extraction; ladders in review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection · e-discovery.uk/edrm/review
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Platform documentation: iManage: imanager.com · NetDocuments: netdocuments.com
- PD 57AD, CPR Part 31 and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- SRA Standards and Regulations: sra.org.uk · ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about DMS evidence as at August 2026. Platform capabilities, logging depth and retention behaviour vary by product, version and configuration; verify the current position for the system in the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

DMS instructions at the laboratory run this guide's sequence: logging configuration and retention established in the first call; activity exports frozen before rotation; workspaces collected version-complete with profiles, filed email and saved comparisons; privilege protected by scoping and the intermediary protocol where the system holds other clients; and analysis delivering the version chronologies, baselined conduct findings and echo-layer rebuilds of Examples 1-3, reported under CPR Part 35. Flattened opposing productions are met with the §11 challenge and re-collection support. Through **e-discovery.uk**, the ladders sit reviewable in sequence beside the correspondence. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a leaver's activity log rotates monthly, its export is today's work.



I N S T R U C T T H E L A B

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