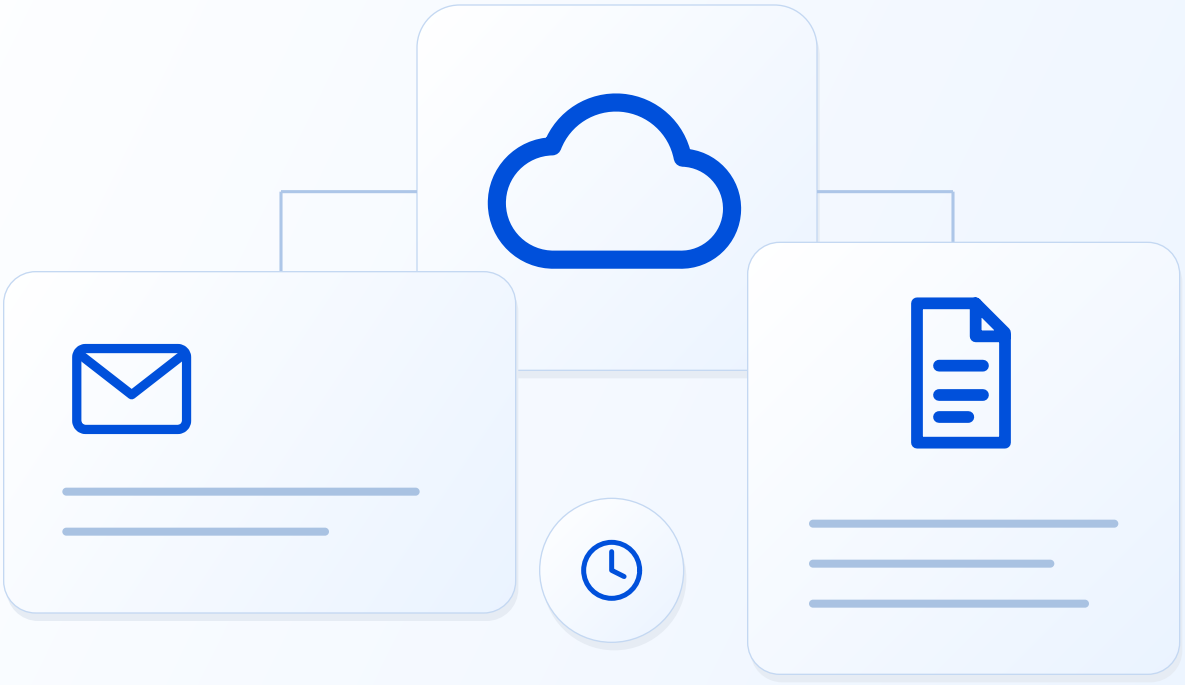
DFI FORENSICS

A GUIDE FOR LITIGATION LAWYERS

Email and cloud evidence

What lawyers need to preserve



NOVEMBER 2026

dfiforensics.ca

01 / EARLY PRESERVATION

Start before records expire

A client brings you an email approving a transaction. It links to a spreadsheet that has since changed. The sender has left, and IT is preparing to remove the account. The visible email is only one part of the evidence.

Begin with the factual question that will change the next decision: what was communicated, which version was available, what activity occurred, or whether the records support a chronology. Identify the sources capable of testing it.

Coordinate the first decisions

Confirm authority

Identify who controls each account or location and who can authorize preservation and collection. Credentials or an accessible link do not settle authority. Sources outside the client's control need a separate route.

Check what may disappear

Ask about departures, migrations, retention rules, licence changes and deletion dates. Confirm what records exist now and the earliest available date. Look for separately retained archives.

Verify implementation

Assign an owner, scope, due date and completion record to each action. A request sent to IT is not an implemented hold. Track pending locations, failed operations and exceptions.

Short retention windows deserve early attention

Microsoft currently lists seven-day audit and sign-in retention for Entra ID Free, and 30 days for P1 and P2. Longer retention requires other arrangements. These identity records are distinct from the Microsoft 365 Unified Audit Log, whose retention depends on licensing, activity and policy. Verify the actual environment. [4,5]

Do not assume a licence upgrade reconstructs expired history. Distinguish "no event found" from "no records available for that period" and "this event was not recorded." Avoid improvised retention changes that could affect other matters.

General technical guidance, not legal advice. Counsel determines preservation obligations, lawful authority, proportionality, privacy, privilege and procedural requirements. Technical collection does not decide admissibility.

02 / SOURCE MAPPING

Map the evidence beyond the inbox

An email address is a starting point, not a complete source list. Record stable identifiers alongside names, the organization or tenant controlling each source, and the person who can explain its configuration.

Mailboxes and archives

Identify individual and shared mailboxes, aliases, delegates, archives and relevant local copies. Preserve surrounding conversations and message–attachment relationships.

Cloud locations

Map drives, shared sites, collaboration spaces, external sharing locations and backups. Record file identifiers, owners and relevant versions, not only folder names.

Activity records

Consider message handling, access, sharing, deletion and administrative activity where available. Establish whether logging covered the event and whether the period remains accessible.

Identity and access

Identify account IDs, delegated permissions and relevant sign-in, application or session context. Ask who else or what automated process could use an account.

A content hold is not a universal freeze

Microsoft eDiscovery holds apply to specified content locations. Audit and identity records have separate retention arrangements. Confirm content, activity and identity sources independently rather than relying on the statement “Microsoft 365 is on hold.” [3–5]

Google Vault coverage is also service-specific. A Drive file linked in Gmail is not included merely because the Gmail message is retained, held or searched. Establish the relevant Drive location and preservation action separately. [6]

Keep verified facts separate from leads

For every source, record what was checked, by whom and when. Mark unknown locations or coverage as unknown.

03 / CONTENT AND CONTEXT

Preserve the message and the linked version

Keep the message as received, with available headers, attachments and source context. Screenshots and PDFs can explain what a witness saw, but may omit details needed to test transmission, threading or attachment relationships.

Retain those representations too, with an explanation of how they were made. Before asking a client to forward "all relevant emails," agree the format and its limits. Forwarding creates another communication and can change the context presented for review.

Read message fields for what they mean

The email format standard distinguishes the origination date from actual transport time. A Message-ID can assist correlation; it is not a guarantee of authenticity or authorship. Compare available source records rather than treating a displayed sender name or date as conclusive. [7]

Where available and authorized, consider both sender and recipient copies. Keep detached attachments traceable to their source messages and preserve relevant surrounding exchanges.

Follow the link to the object and the time

A cloud link may open a document that changed after the email was sent. Identify the linked object, owner, sharing location and relevant time. Decide whether the question concerns the version shared, a version accessible at a later event, or the version now produced.

Request available version history and relevant sharing context. Ask how the collection method handles cloud attachments, versions and comments. A readable export may not contain all the history available in the service. Microsoft treats cloud attachments as a specific eDiscovery feature. [3]

Do not substitute today's file for yesterday's

If a historical version is unavailable, record the limit and seek comparison sources such as a sent attachment or independent retained copy.

A mailbox hold and a linked-file preservation step may cover different sources. Check both. [3,6]

04 / COLLECTION INSTRUCTIONS

Give the collection a clear boundary

A useful brief identifies the question, custodians, accounts, locations, dates, authority, urgency and intended deliverable. State unresolved decisions and agree how unexpected sources, sensitive material and scope changes will be handled.

Separate preservation from review. Urgent retention risk may justify preserving a broader set before the initial examination is settled. Counsel should decide the appropriate scope and safeguards.

Request a collection record that can be explained

- Who collected the records, when, using which access and method.
- Source identifiers, date ranges, original time zones, search terms and filters.
- Export settings, completion reports, item counts, failed items and significant errors.
- Treatment of attachments, linked files, versions and excluded locations.
- An inventory of received files, integrity checks and subsequent transfers.

Keep received exports separate from working copies. Search results are not automatically a complete account history. Ask how indexing limits, failed items and filters were checked before relying on a negative result.

Set privacy and privilege arrangements before review

Specify who may access collected material, where it will be stored and how privileged, personal or out-of-scope material will be segregated or escalated. Consider provider, subprocessor and storage-location issues that counsel needs to address.

Confirm secure transfer, access controls and the treatment of working copies. Keep the instructions actually given and agreed changes. A collection is not privileged simply because counsel requested it; the legal basis needs its own assessment.

Do not send passwords or confidential evidence through an ordinary website inquiry. Arrange the evidence-transfer route first.

05 / INTERPRETATION AND DELIVERY

Explain what the records actually support

An activity record may associate an operation with an account, application or session. The named account holder may not have been the person acting. Delegation, shared access, automation and compromised credentials can change the interpretation.

Preserve underlying exported records and ask which fields support an interpretation. Microsoft audit records can include application context, user-agent information and other event details. A simplified chart should not replace those records. [8]

Separate sending, delivery, access and human reading. A record supporting one does not necessarily establish the others. Keep original timestamps and offsets while presenting a chronology in a stated time zone. Explain unresolved clock or display issues.

A focused example

ILLUSTRATIVE SCENARIO / NOT A DFI CASE

A supplier says the client approved a revised price schedule. The client produces an email with a cloud link and denies seeing the revision.

A proportionate first stage preserves the messages and headers, identifies the file, secures available versions around the approval date, and captures relevant activity records before expiry. It also identifies accounts and delegates with access.

Test whether the revision existed when the link was sent, whether the recipient could access it, and what the records actually show. Delivery alone does not establish reading.

Match the deliverable to the decision

A preserved collection, indexed messages, focused chronology, technical comparison and formal expert report serve different purposes. Agree the output before work begins and connect material findings to their source records.

Distinguish sources collected from sources examined, observations from interpretation, and supported conclusions from unresolved alternatives. Show missing accounts, incomplete periods and unavailable versions. Define what further evidence would change the next decision.

06 / EXPERT HELP AND REFERENCES

Discuss the evidence your matter needs

DFI can help identify relevant sources, preserve authorized mailbox and cloud material, and examine the available records against counsel's question. Agreed work may include scoped collections, selected messages and attachments, activity analysis and a chronology where the evidence supports one. [1]

Bring the issue, dates, known accounts, existing holds or exports and any approaching deletion or reporting deadline. An early scoped discussion can help identify useful work and avoidable evidence gaps.

Arrange an initial evidence discussion

dfiforensics.ca/contact · 778-742-5621 · info@dfiforensics.ca

Contact DFI first to arrange secure evidence transfer. [2]

An inquiry does not establish an engagement or guarantee a response time. Do not include passwords or confidential evidence with the initial inquiry.

Sources and technical notes

Primary sources checked 9 November 2026. Capabilities, licences and retention rules change. Verify the current documentation and actual configuration. These references do not establish a universal legal standard.

[1] DFI Forensics · Email and cloud evidence
Service scope, evidence sources and possible deliverables.

[2] DFI Forensics · Contact
Contact details and secure-transfer guidance.

[3] Microsoft · eDiscovery features and components
Content-location holds and cloud attachments.

[4] Microsoft · Audit log retention policies
Licensing, policies and audit retention.

[5] Microsoft · Entra data retention
Identity-report retention and separation from the Unified Audit Log.

[6] Google · Vault supported services and data types
Service coverage and Drive files linked from Gmail.

[7] RFC Editor · RFC 5322 §§3.6.1 and 3.6.4
Origination-date and message-identification fields.

[8] Microsoft · Detailed audit-log activity properties
Event fields, application context and user-agent information.