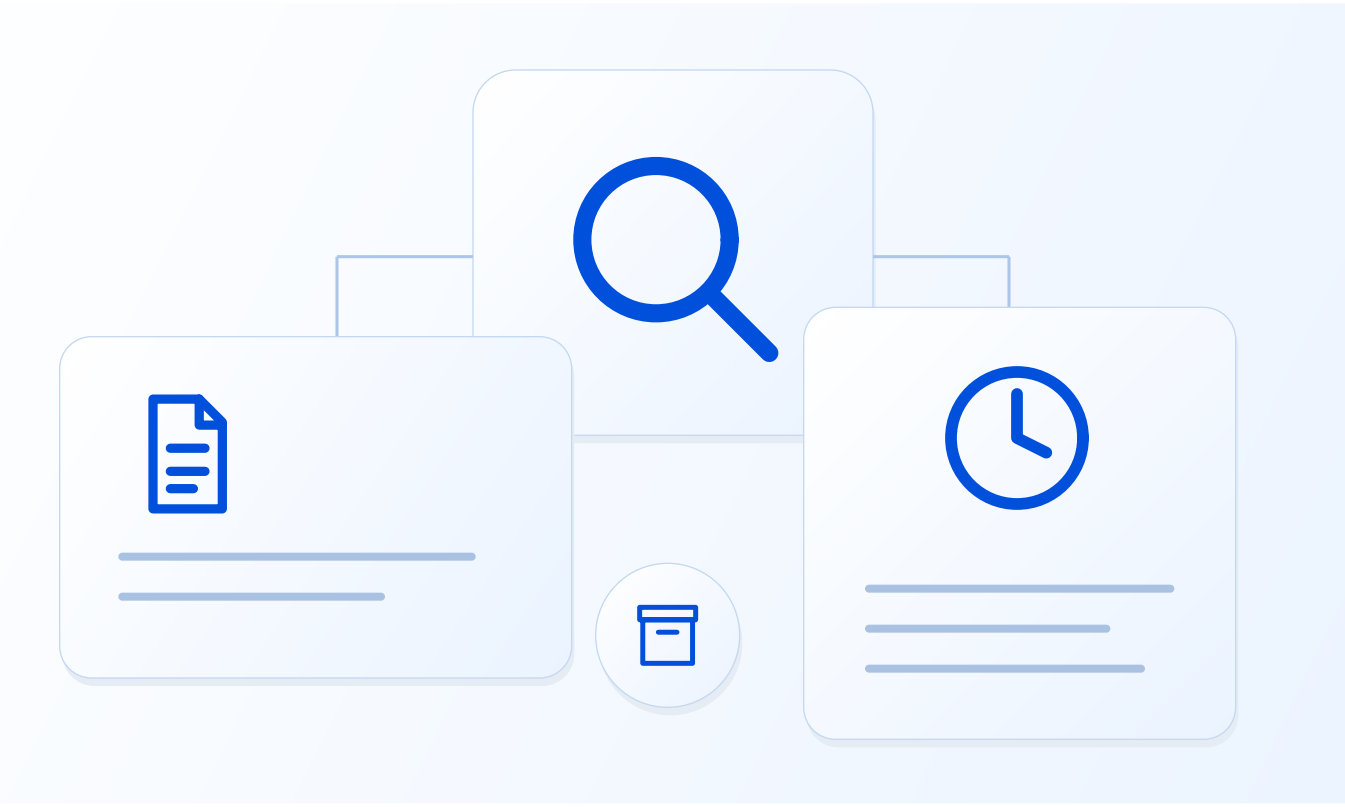
DFI FORENSICS

A GUIDE FOR LITIGATION LAWYERS

When digital evidence is disputed

Testing documents, dates and copies



NOVEMBER 2026

dfiforensics.ca

01 / DEFINE THE DISPUTE

Separate the questions before examining the file

A contract appears to have been created after the date on its face. Two copies of a project record contain different wording. A PDF's author field names someone who denies writing it. Each may justify investigation. None supplies the whole answer.

The useful starting point is the proposition that matters to the dispute: whether particular wording existed before an event, whether an exhibit matches a supplied source, or whether available records support the history described by a witness. A focused examination can help counsel distinguish a material inconsistency from an ordinary consequence of copying, exporting or editing.

Authenticity, integrity, authorship and truth overlap, but ask different things. A file can remain unchanged since collection while containing an inaccurate statement. A genuine copy can reproduce a document whose author is uncertain. Evidence that a document existed by a particular time does not necessarily establish when its wording was first composed.

Where the Canada Evidence Act applies, section 31.1 addresses authentication, while section 31.2 separately addresses the best evidence rule for electronic documents. Section 31.7 preserves other admissibility rules. The governing statute, proceeding and evidentiary issues must therefore be assessed by counsel; technical findings do not decide admissibility or weight. [1]

Define the proposed assertion before requesting an opinion. "Was this forged?" can hide several unresolved questions. "Does the available history support the presence of clause 8 in the document sent on 12 March?" gives the examiner a testable issue and counsel a more useful answer.

Make the proposition testable

Identify the wording, date, version or event in dispute before deciding which source or examination is needed.

General technical guidance for Canadian counsel, not legal advice. Technical findings do not determine admissibility or weight.

02 / FILES AND PROPERTIES

Know which version you are examining

The form of the record matters

A native file is the file in the format used by the relevant application, such as a Word document or spreadsheet. Depending on its format and history, it may preserve information beyond the visible pages. Microsoft identifies comments, tracked revisions, document properties and other hidden information in Office files. Their availability varies; a native file does not guarantee a complete editing history. [2]

An exported PDF is another record with its own properties and production history. A scanned PDF may primarily contain images of paper. A screenshot records a displayed view, potentially cropped or incomplete, rather than the underlying document's full structure. These forms can be useful, but they answer different questions.

Preserve the questioned item as received, even when a better source may exist. The screenshot or production PDF may itself be the disputed representation. Obtain the underlying file and comparison material where lawfully available, recording how each relates to the exhibit. Avoid calling the newest download "the original" without explaining its origin.

Treat metadata as contextual evidence

PDF metadata can include creation and modification dates, author information and application-specific fields. Adobe also documents functions for appending, replacing and deleting metadata. Those properties are useful observations, but their presence does not make them an independent certificate of the document's history. [3, 4]

Office properties likewise require care. Microsoft's Document Inspector can remove metadata and revision information. A missing author field may reflect an ordinary privacy workflow. An unexpected name should prompt questions about the file's origin and how it was prepared, rather than immediate attribution to that person. [2]

Examine the visible content alongside the internal records. A difference in wording matters differently from a difference in document properties. The report should explain which observation supports which inference, and what corroboration is missing. Software capability to change metadata establishes a limitation; it does not establish that someone changed the particular file dishonestly.

03 / DATES AND INTEGRITY

Test what a date or hash really establishes

A date printed inside a letter, a document's internal creation field, a file-system creation time and a cloud version timestamp describe different things. A timeline becomes misleading when these are presented as interchangeable "document dates."

Copying can create a new file-system creation time while retaining an earlier modification time. The behaviour depends on the file system, application and transfer method. NIST's forensic guidance specifically warns that some collection methods alter file times. A creation date later than a modification date can therefore have an ordinary explanation. [5]

Modification time also needs a defined source and meaning. It does not identify which words changed or who changed them. Microsoft documents differences in timestamp storage and resolution between file systems, and the ability to change Windows file times without changing file content. [6]

Before correlating events, establish time zones, display conversions, clock reliability and the available precision. Record both the source value and any normalization used. An apparent one-hour discrepancy may call for a time-zone explanation before it calls for an allegation. Where the underlying settings are unavailable, that uncertainty belongs in the conclusion.

Hashes test integrity, not every disputed fact

A cryptographic hash represents the bytes supplied to the hashing process. Comparing hashes is an important integrity check when collecting and handling evidence. The report should identify the algorithm, files compared and point at which values were recorded. NIST describes digest comparison as a means of verifying acquired data integrity. [5]

A matching file hash can support a finding that copies contain the same bytes. It does not establish who wrote the document, whether its statements are true, or whether it was accurate before collection. Conversely, different hashes establish a byte-level difference, not necessarily a substantive difference visible on the page. [8]

This distinction matters when two PDFs look alike. Analysis must identify whether the difference concerns text, images, metadata or another part of the file before counsel assigns significance to it.

04 / PROVENANCE AND SCOPE

Build the history from independent sources

Provenance is the account of where the material came from and how it reached the examiner. Identify the custodian, source device or account, collection method, relevant transfers and known transformations. A document detached from its email, folder or production context may lose useful evidence about its history.

Comparison sources might include an attachment in a preserved mailbox, an earlier project copy or a cloud version. Microsoft 365's version-history feature supports comparison of previous versions for files stored in OneDrive or SharePoint. Its availability should be confirmed in the actual account rather than assumed from the presence of a Word file. [7]

A comparison must also be independent enough to add information. Three copies downloaded from the same recent upload do not establish three separate historical occurrences. Counsel and examiner should ask what each source contributes and whether a missing interval prevents a reliable conclusion about when the disputed wording appeared.

Agree the next useful examination

Start with the contested proposition, significant dates and available sources. Counsel can identify authority, privilege and confidentiality constraints, and explain how the findings will be used. This allows the technical work to focus on the issue rather than expand into an unfocused search through unrelated information.

An initial file comparison may answer the immediate question. Alternatively, it may establish why a device acquisition, mailbox collection or cloud-history examination is needed. Agree the next stage against its likely evidentiary value and the consequences of missing information. Avoid promising that a particular tool will recover every version or identify an individual author.

A bounded answer can still be useful

Explain what was tested, what remains unresolved and which additional source could materially change the answer.

05 / AN ILLUSTRATIVE DISPUTE

Follow the evidence through the competing explanations

ILLUSTRATIVE SCENARIO / NOT A DFI CASE

Suppose a party produces a PDF agreement dated 3 April. The recipient's downloaded copy has a file-system creation date of 19 June. Counsel suspects that an exclusion clause was added after negotiations ended.

The June date alone cannot resolve that concern. It may record the download. The focused question is whether the exclusion appeared in material exchanged before the relevant deadline.

An examiner compares the produced PDF with an attachment obtained from an authorized, preserved mailbox and available earlier drafts. If the April attachment contains the same clause and has a matching hash, that supports byte-level continuity between those two copies. The reliability of the email chronology still requires assessment; the comparison does not establish assent to the clause.

If an independently preserved April attachment lacks the exclusion, the difference warrants investigation. Possible explanations include different drafts, an export from another version or a later substantive change. The examiner compares the sources and available chronology before attributing the change. If only a screenshot remains, the outcome may be limited to identifying visible differences and the further source needed to test them.

Read the finding against the question

The strongest conclusion is the one the available evidence can support. Byte-level continuity, a visible difference and a supported historical occurrence are different findings. Counsel should be able to trace the reported conclusion to the particular sources and comparisons behind it.

Where the record is incomplete, state the missing interval or source rather than replacing it with certainty. A report that explains an unresolved alternative can help counsel decide whether further collection is proportionate.

Do not alter the questioned item to improve it

Keep the file as received. Seek handling advice before opening, resaving or converting a source that may need examination.

06 / EXPERT HELP AND REFERENCES

Discuss the disputed record with DFI

DFI's metadata and evidence-authentication service examines questioned records through their sources, properties, chronology and available comparisons. The work can include relevant file-system records, version history and application or account records. Scope and deliverables are agreed before the examination. [8]

For counsel, the value is a clearer explanation of what the evidence supports, which alternatives remain plausible and where further collection could change the answer. Findings should distinguish observations from interpretation and make material limitations visible.

Arrange an initial evidence discussion

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

Contact DFI first to arrange secure evidence transfer.

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. This is general technical guidance, not legal advice. Verify applicable law, current product capabilities and the actual source environment for the matter.

[1] **Canada Evidence Act · Electronic documents provisions**
Sections 31.1, 31.2 and 31.7: authentication, best evidence and other rules where applicable.

[2] **Microsoft · Remove hidden data and personal information**
Office metadata, revisions, hidden content and removal limitations.

[3] **Adobe · Document properties and metadata overview**
PDF author, dates and application-specific properties.

[4] **Adobe · Edit document metadata**
Metadata can be appended, replaced or deleted; not a finding of alteration in a particular file.

[5] **NIST SP 800-86 · Forensic techniques, §§ 4.2.2–4.2.3**
2006 guidance cited for integrity, collection effects and clock limitations, not historical algorithm advice.

[6] **Microsoft · File Times**
Windows time behaviour, storage, resolution and setting file times.

[7] **Microsoft · View previous versions of Office files**
Described version-history feature requires OneDrive or SharePoint; actual retained history varies.

[8] **DFI Forensics · Metadata and evidence authentication**
Verified service scope, comparison sources and reporting limitations.