DFI FORENSICS

A GUIDE FOR LITIGATION LAWYERS

Court-ordered digital evidence collection

Counsel's planning guide



NOVEMBER 2026

dfiforensics.ca

01 / AUTHORITY BEFORE ACCESS

Translate the order into separate permissions

A collection team arrives to preserve a former executive's laptop. The computer also connects to a family account, a shared company drive and a cloud service administered abroad. Counsel expects a copy by afternoon. The order permits preservation, but access for review is subject to a further protocol.

Those distinctions determine what the team can do. Early technical input helps counsel identify ambiguous wording, unavailable access and operational constraints before they become disputes during execution.

This guide concerns planning and technical execution. It is not legal advice or a model order. Counsel must determine the governing law, authority and procedural safeguards for the particular proceeding. Collection does not guarantee admissibility.

Read the permissions and limits together

Read the issued order, incorporated schedules, amendments and applicable protocol together. Distinguish permission to enter premises, identify sources, take possession, preserve copies, search content, conduct analysis and release results. A direction covering one stage may leave another restricted.

The instructions should identify custodians, devices, accounts, locations, relevant periods and permitted methods. Resolve whether "email" includes archives, attachments and linked documents, and whether deleted material or historical versions are within scope. Record boundaries that remain undecided.

Have counsel resolve material ambiguity before the affected step. A client's possession of credentials does not establish authority to use every account they unlock. Neither urgency nor technical convenience expands the order.

An Anton Piller order requires particular care. In Celanese Canada Inc. v. Murray Demolition Corp., the Supreme Court emphasized a carefully drawn order, privilege safeguards, independent supervision and restraint in execution. Those safeguards concern an exceptional remedy and should not be presented as the identical requirements for every collection order. [1]

02 / ROLES AND SOURCES

Make the mandate and access route explicit

Identify who instructs the examiner, who pays, who receives communications and who can resolve operational questions. If the examiner is jointly retained or appointed to a neutral role, establish how instructions and material communications reach the parties. One party's request should not quietly change that mandate.

An examiner retained by one party should also work within the authorized scope and distinguish technical observations from advocacy. Payment by a party does not make unsupported conclusions acceptable; appointment as a neutral does not confer authority to decide legal disputes.

Where an independent supervising solicitor is required, distinguish that legal supervisory role from the examiner's technical responsibilities. Specify the escalation route for privilege claims, unexpected sources, access refusal and competing instructions. The technician should not have to decide whose interpretation of the order prevails at the doorway.

Identify sources, access and locations precisely

Match each proposed collection to a specific source and lawful access route. Record device identifiers, account addresses, tenant or organization identifiers, physical locations and the person who controls access. Distinguish a local synchronized folder from the cloud account it reflects.

Ask what practical cooperation is needed: an administrator, an account holder for authentication, a service provider, building access or a scheduled maintenance window. Assess encryption and collection feasibility without promising that a device can be unlocked or that every deleted item can be recovered.

Identify third-party systems and foreign storage or administration early. Counsel should address any jurisdictional, privacy or provider-process issues before access or transfer. A logged-in session reaching an additional account is a reason to check scope, not an invitation to explore it.

03 / METHOD AND SAFEGUARDS

Collect proportionately and protect restricted material

Ask the examiner to explain the coverage, limitations, cost and disruption of feasible methods. A targeted export, logical acquisition and full forensic image preserve different material. The broadest technically available method may collect substantial unrelated information.

Where authorized and technically suitable, staged collection can preserve the sources at risk while deferring wider examination. If broader acquisition is necessary to preserve relevant material, establish the legal basis and access restrictions before collecting it.

British Columbia's Supreme Court Civil Rules expressly link proportionality to the amount involved, importance of the issues and complexity of the proceeding. Counsel should apply the governing jurisdiction's rules rather than treating a technical preference as the legal standard. [2]

Privacy analysis also remains necessary. PIPEDA's paragraph 7(3)(c) addresses disclosure required by qualifying orders and court rules. It is not general permission to search any accessible system, and applicable provincial legislation must also be considered. [3]

Design privilege protection before collection

Specify how potentially privileged material will be identified, segregated and withheld from unauthorized review. Address mixed personal and business accounts, legal-advice folders and documents whose status is disputed. Search terms may assist screening but should not be treated as a complete privilege determination.

Define who performs the legal review, what the examiner may inspect for technical purposes and how disputes are resolved. Where the order permits preservation pending a decision, use the prescribed restricted-access or sealing process. Do not assume that creating a separate folder supplies an adequate access barrier.

Celanese illustrates why post-collection handling matters: preservation does not itself authorize opposing counsel to review privileged material. Controls must remain effective after the team leaves the premises. [1]

04 / EXECUTION AND TRACEABILITY

Plan for the live environment and document what happens

Confirm the permitted attendance time, authorized participants, expected duration, equipment, storage capacity and secure transport arrangements. Identify business-critical systems and agree who can approve any interruption within the order's limits.

Avoid improvised shutdowns, disconnections or account changes. NIST's forensic guidance explains that volatile information can disappear when a system powers down, while live collection can itself change information. The examiner should assess that trade-off and document the method selected. NIST is technical guidance, not Canadian legal authority. [4]

Plan for incomplete access and unexpected delay. If a source cannot be collected within the permitted window, record its status and seek direction through the agreed process. A failed password, an unavailable administrator or a storage error does not authorize a workaround outside scope. Site safety and any resistance should be handled through the lawful process, never improvised self-help.

Leave a record another person can follow

The execution record should connect the authority to the material actually obtained. Preserve the operative instructions and record attendance, source identifiers, relevant times and time zones, methods, tool versions, settings and transfers. Distinguish material collected directly from material supplied by someone else.

Record errors, unavailable sources, interrupted operations, retries and approved changes when they happen. Explain how each exception affects coverage. "No responsive items exported" should not conceal an inaccessible location or an unsupported file type.

Use appropriate integrity verification and retain the results. A matching cryptographic hash supports a comparison of the specified data; it does not establish who authored a document or prove that every relevant source was collected.

Keep the preserved material separate from working copies. Document who accessed it and which copies were created or released. DFI's evidence-handling approach expressly distinguishes preservation, review and disclosure, with access and retention arrangements agreed for the matter. [7]

05 / HANDOFF AND RESTRICTED ACCESS

Release only what the authority permits

Determine whether the required output is a preserved collection, an execution report, an affidavit, a selected production or an expert opinion. These require different instructions and work. A collection report should explain what was done, departures from the plan and unresolved limitations without implying an examination that never occurred.

Release only the authorized material to the authorized recipients through the agreed channel. Record delivery and receipt, and confirm what remains restricted. Return, retention and destruction should follow the order and applicable preservation obligations, with counsel resolving any conflict before action.

Where the Canada Evidence Act applies, section 31.1 addresses authentication and section 31.2 addresses the electronic-document best-evidence rule. Section 31.7 preserves other admissibility rules. A documented collection helps explain the evidence; it does not settle every legal objection. [5]

Preserve first, review when authorized

ILLUSTRATIVE SCENARIO / NOT A DFI CASE

An order permits an examiner to image a departing director's identified laptop and collect a defined company mailbox. The copies must remain restricted pending privilege review.

During collection, the laptop displays a synchronized personal drive. The team records the issue and follows the protocol for any local material captured by the permitted image, without using the session to collect the separate cloud account. It escalates the scope question. A mailbox export fails partway through; the examiner records the failure, completes an authorized retry and explains the resulting coverage.

The applicant asks for immediate access to the preserved image. The examiner follows the release restriction and refers the request through the agreed route. Counsel receives an execution report, an inventory and the outstanding issues, while the preserved content remains protected until access is authorized.

06 / EXPERT HELP AND REFERENCES

Plan a court-ordered collection with DFI

DFI works with counsel to plan and carry out court-ordered digital evidence collection within the order's scope and agreed instructions. Technical input can help turn legal boundaries into a feasible collection and make limitations visible before they affect the next decision. [6]

Bring the order or proposed protocol, known sources and timing constraints to an initial discussion. Contact DFI before sending the documents so an appropriate transfer method can be agreed.

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] **Celanese Canada Inc. v. Murray Demolition Corp., 2006 SCC 36**
Especially paras. 1–4: Anton Piller safeguards, privilege, supervision and restraint.

[2] **BC Supreme Court Civil Rules · Rule 1-3**
BC civil proportionality factors; not a national procedural rule.

[3] **PIPEDA · Section 7**
Paragraph 7(3)(c): disclosure required by qualifying orders or court rules.

[4] **NIST SP 800-86 · Forensic techniques, §§ 3.1 and 5.2.1**
2006 technical guidance on volatility and live collection, not Canadian legal authority.

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

[6] **DFI Forensics · Court-ordered evidence preservation**
Current service scope and agreed instructions.

[7] **DFI Forensics · Evidence handling and quality controls**
Scope, traceability, access, delivery and retention arrangements.

[8] **DFI Forensics · Contact**
Contact details, secure-transfer instructions and inquiry limitations.