

PRACTICAL GUIDANCE FOR LEGAL MATTERS

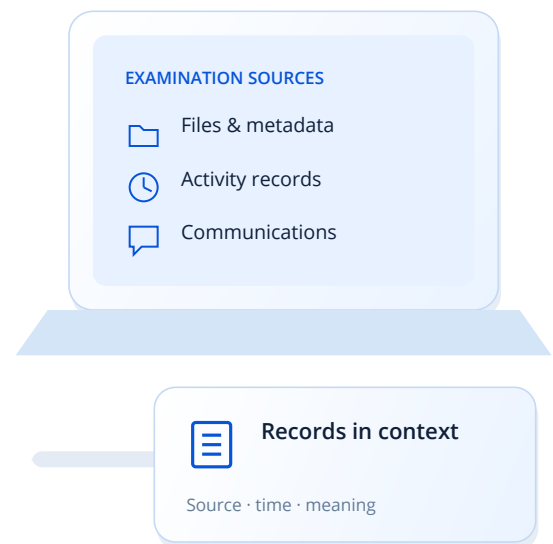
Computer evidence for litigation

Forensic acquisition and analysis
for facts that need to be established.

Computers retain traces of files, communications and activity. We help you identify the relevant sources, preserve the available data and explain what it supports in the context of your matter.

WHEN A COMPUTER EXAMINATION CAN HELP

- ✓ **Employee departures and data theft**
Investigate access to business files, USB use and traces of copying or sharing.
- ✓ **Commercial and workplace disputes**
Examine documents, communications and activity relevant to events or competing accounts.
- ✓ **Fraud and suspected compromise**
Assess available account and system activity, suspicious files and evidence of unauthorized use.



Windows PCs, laptops, servers,
MacBooks and Surface devices.
The method is matched to the system.

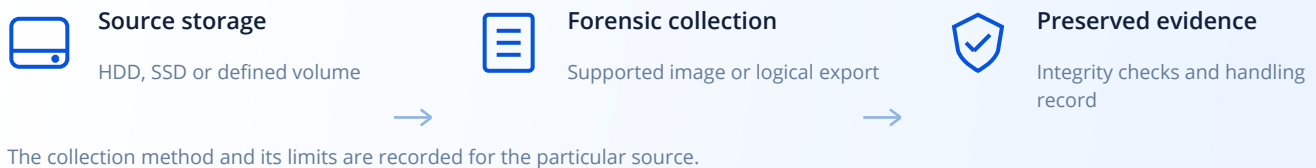
The legal need guides the examination

You may need to test a factual account, address a legal issue in your matter, or obtain a reliable set of records. We advise on the sources and scope before collection, then provide independent findings and supporting material suited to that purpose.

01 / ACQUISITION AND PRESERVATION

Preserve the source. Examine a verified copy.

A forensic image captures the readable data in the selected storage source. A physical image can include allocated and unallocated areas of an accessible hard drive or SSD; a logical collection captures selected files or accessible records.



We document the device and authority, select the collection method, preserve the output and analyze controlled working copies. Where appropriate, hardware or software write protection helps prevent changes to source storage during acquisition.

- | | |
|--|---|
|  Offline imaging | Where supported, readable storage is imaged without running the installed operating system. A verified image allows examination of the collected data while preserving the original source. |
|  Live or targeted collection | An unlocked or running system may be the best route to accessible decrypted data or volatile information. Live collection changes the system; we document the relevant actions and limitations. |
|  Servers and virtual systems | RAID, virtual disks, active databases and business uptime can require coordinated collection. We define the disks, volumes, snapshots and logs in scope; a snapshot alone is not automatically a complete evidence acquisition. |

What verification establishes

A cryptographic hash is a digital fingerprint of collected bytes. Comparing hashes helps detect changes to that copy. It supports integrity, but does not prove that every relevant source was collected, that a record is true or who performed an action.

An encrypted image may preserve data without making it readable. Access to the necessary keys is a separate issue.

02 / DEVICES AND ACCESS

One method does not fit every computer.

We assess the model, storage design, operating system, encryption and current power state before choosing tools. Credentials or recovery material may be important, but should be shared only through an agreed secure route.

 **Windows PCs and laptops** Internal hard drives (HDDs) and solid-state drives (SSDs) may be removable or integrated. BitLocker and device encryption can protect the data even after storage is removed. A password, recovery key or authorized access to an unlocked system may affect the available collection route.

 **Apple MacBooks** Intel Macs without T2, T2-equipped Intel Macs and Apple silicon Macs require different acquisition planning. On T2 and Apple silicon Macs, internal-storage protection is tied to secure hardware. Removing or copying storage does not necessarily yield readable data; access, FileVault and tool support must be assessed.

 **Microsoft Surface Pro** Surface Pro models differ in storage access and processor architecture. Pro 9, for example, has Intel and Arm variants and removable SSDs. Encryption still matters; acquisition tools and their drivers must support the particular model and architecture.

 **Servers and shared systems** A file on one computer may have relevant counterparts on a server, virtual machine, backup or cloud service. We coordinate scope with you and collection logistics with the system administrator, rather than assuming one device contains the full history.



Access is assessed, not assumed

Encryption, damaged storage and unsupported hardware can limit or prevent collection. SSD TRIM and other storage processes can make deleted data unavailable. We explain these constraints before promising an approach or recovery.

Have clients and custodians avoid resets, reinstalls and recovery software. Seek device-specific guidance before power changes or disconnection.

Sources: [Apple encryption](#) · [Surface Pro 9](#) · [Windows Arm](#) · [BitLocker](#) · Reviewed 24 October 2026.

03 / ARTIFACTS AND TIMELINES

Connect records to the events that matter.

An artifact is a record left by an operating system or application. Several artifacts considered together can help explain a sequence of activity more reliably than a single timestamp or file viewed alone.

ILLUSTRATIVE CORRELATION, NOT A CASE FINDING



File activity

Metadata and file-system traces



USB connection

Device and connection records



Document use

Recent-item and application traces



Sharing activity

Browser, sync or transfer records



Files and documents

Names, content, available metadata, file-system journals and recent-file references may help establish creation, modification or use. Different timestamps describe different events.



USB and external storage

Connection traces may identify a device and relevant times. Correlation with file and application records may support an assessment of transfer activity; connection alone does not prove copying.



Communications and online activity

Available email, browser history, downloads and records from WhatsApp, WeChat and other messaging apps can add context. Coverage depends on the application, local storage, retention and access.



Accounts and system activity

Login, security and application logs may help reconstruct activity or investigate suspected compromise. Logging may be incomplete, overwritten or outside the collected source.

A timeline needs interpretation

We account for time zones, clock differences and how each artifact was generated. An account association does not by itself identify the person at the keyboard. Absence of an artifact is not proof an event never occurred.

Sources: [Microsoft file times](#) · [Windows object-access auditing](#) · Reviewed 24 October 2026.

Evidence lawyers and litigants can use.

We explain what the records show, what they do not resolve and how our findings relate to the agreed purpose. The work may answer a factual question or simply produce a verified set of relevant records for disclosure or court.

	Clear findings	Plain-language explanations of the sources, methods, observations and limitations. Interpretation remains independent and grounded in the evidence.
	Organized supporting records	Relevant files, communications, metadata and artifacts, with source references and useful context retained. Export formats are agreed to fit the matter.
	Focused timelines	A sequence of relevant events supported by identified records, with time-zone treatment, gaps and alternative explanations addressed where material.
	Expert consultation	Advice to counsel and litigants on the digital evidence. Additional analysis, formal expert reports or testimony can be scoped as the matter develops.

Before collection

- ✓ Identify the devices, users, relevant dates and the facts your matter needs to establish.
- ✓ Define collection authority, privilege handling and scope restrictions for the matter.
- ✓ Arrange preservation instructions for clients and custodians before systems are altered.

Reliability throughout

Documented acquisition, integrity checks, handling records and clear explanations support the reliability and admissibility of digital evidence. The court determines admissibility in the particular proceeding.

Discuss the evidence your matter needs

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

General information, not legal advice. Device support and access are assessed for each engagement. Technical sources are linked within this guide and documented in the editable source package.