The Cloud of Evidence

A Forensic Guide to Preserving Digital Truth: Master the protocols for collecting volatile cloud data to build a defensible and legally admissible case.

The Volatility Challenge

Cloud data is not static. It is ephemeral, easily altered, and often controlled by third parties. Without immediate and correct action, critical evidence can be lost forever.

90

Days or less is the typical retention period for critical cloud audit logs before they are permanently deleted.

1 Click

Is all it takes for a custodian to permanently delete a file or email, risking spoliation.

The Preservation Protocol: A 3-Step Mandate

The instant an investigation is anticipated, this sequence must be executed to freeze data in time and prevent evidence spoliation.

1. Issue Legal Hold

Formally notify all custodians to preserve relevant data, even if it's on a third-party server.

→

2. Notify Cloud Provider

Issue a preservation letter to the service provider, placing the legal burden of non-deletion on them.

→

3. Lock Down Access

Change user permissions to read-only or enable the service's built-in litigation hold features (e.g., M365 Litigation Hold).

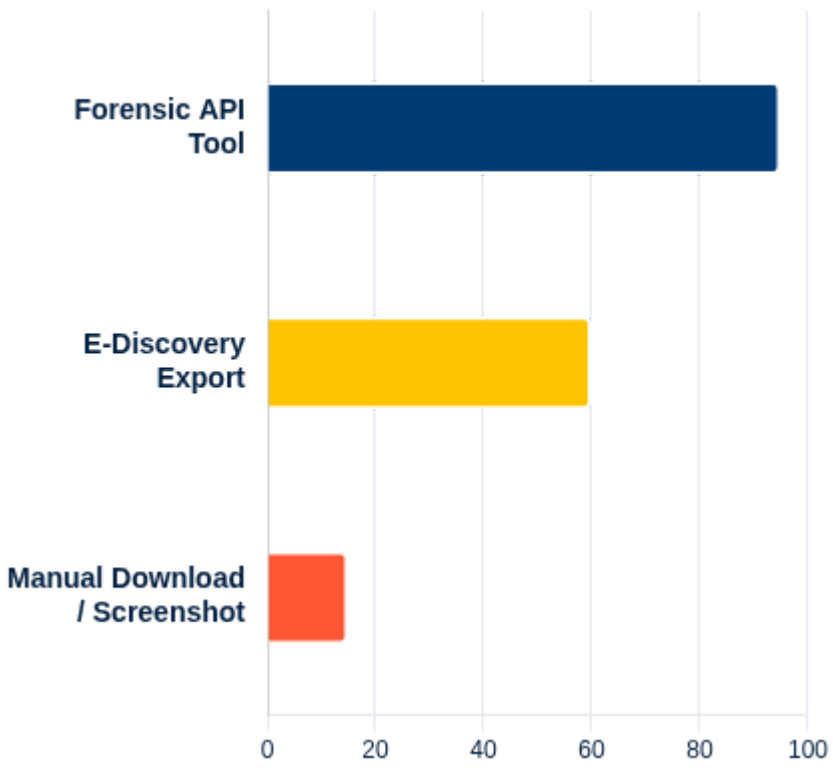
The Collection Hierarchy

Not all collection methods are created equal. Proving the authenticity of cloud evidence requires forensically sound techniques. A manual download is easily challenged in court; an API-based collection with full metadata is the gold standard.

Forensic API Tool: Highest legal soundness, full control.

E-Discovery Export: Medium soundness, partial control.

Manual Download: Lowest soundness, minimal control.



The Audit Log: The Cloud's Chain of Custody

The cloud provider's audit log is the single most important piece of evidence. It is the definitive, chronological record of every user action: who logged in, what they accessed, and what they changed.

1. Check Retention Policy

Immediately confirm the log retention period (often 30-90 days) and request an extension.

→

2. Export Raw Data

Export the raw audit log data (JSON or CSV) for the entire relevant time frame.

→

3. Generate Hash

Immediately generate a cryptographic hash (SHA-256) of the exported file to prove its integrity and lock in the Chain of Custody.

An audit log showing a "File Deleted" event is an irrefutable fact, regardless of a user's verbal claims.

Infographic generated from Knowledge Article KA-FH-602. This visualization does not use Mermaid JS or SVG graphics.