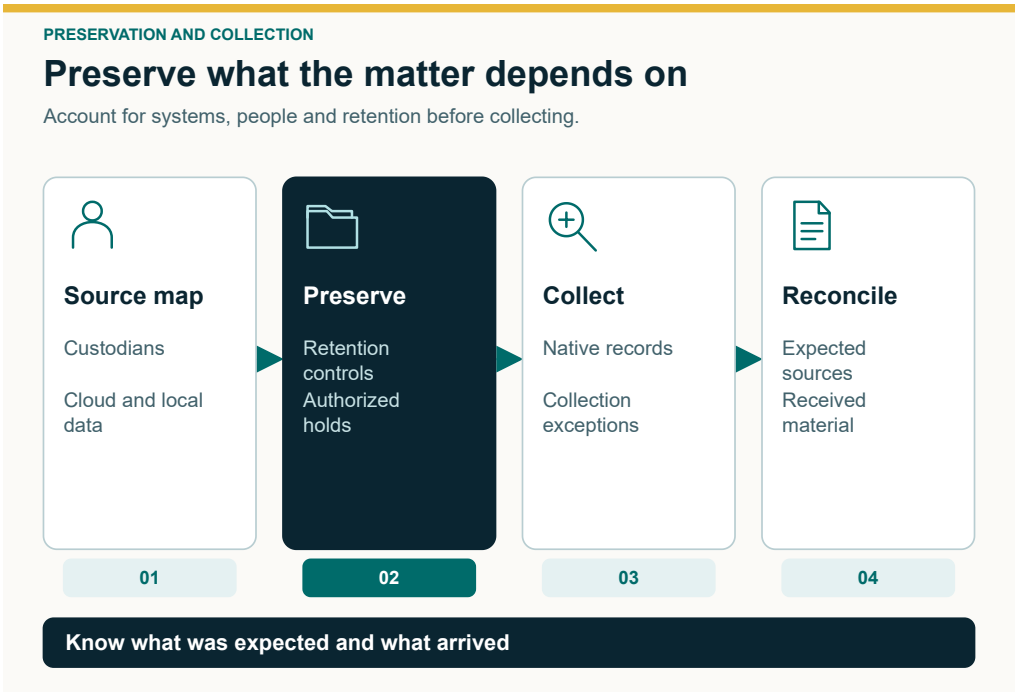
Preserve Teams, Slack and Email Before Retention Wins

Messages, edits, reactions, attachments and audit events in Teams, Slack and email each follow their own retention clock. This note shows how to freeze routine change without stopping the business and how to collect the context that gives messages meaning. Remediation and the evidence of who did what can run side by side.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/insights/preserve-teams-slack-email/

A threatened restraining order, employee departure, transaction dispute, or suspected data transfer can create an immediate preservation problem. Collaboration content spans several datasets. The message body, attachment, version history, channel membership, deletion event, audit record, and identity context may live in separate systems, each with its own retention period.



The collection scope is checked against retention, source coverage and the material actually received.

Identify Retention Settings and Records at Risk

Once the legal scope is set, IT can identify the tenant, accounts, channels, shared mailboxes, cloud drives, endpoints, mobile devices, retention rules, licenses, backup sources, and departed user workflows involved. Before changing an account, record what suspension, deletion, reassignment, license removal, or mailbox conversion will do to preserved material.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Immediate collection may be necessary for audit or identity records with short availability. Other sources can be held in place. The source map should state which decision applies to each record and who owns the next action.

Collect Conversation Context and Administrative Evidence

For Microsoft 365, relevant sources may include mailbox content, Teams messages, SharePoint or OneDrive files, Purview holds or exports, unified audit data, Entra sign ins, application consent, inbox rules, and endpoints. Slack may require workspace exports, channel and membership context, attached files, audit logs, retention settings, and connected services. Native files and provider generated identifiers are retained where available.

A typical engagement records the tenant, license, retention settings, time zone, administrator and collection time, preserves edits, deletions, reactions, threads, attachments and membership context where the platform supports it, collects identity and administrative events before their retention expires, reconciles the expected custodians and channels against completed exports, and documents what the provider supplied.

Keep Attribution Evidence Through Remediation

Credential resets, token revocation, rule removal, account suspension, and device reimaging may be required. Sequence those changes with evidence preservation when possible, and record the exact time and reason. A later reviewer should be able to distinguish user activity from the response team's work.

Primary Sources and Technical References

- Microsoft Purview eDiscovery documentation https://learn.microsoft.com/purview/ediscovery
- Slack data exports documentation https://slack.com/help/articles/201658943-Export-your-workspace-data

Get a Free Consultation

The first call is a free consultation with a senior examiner. We review the matter, the evidence and the deadline, and outline the collection and analysis it needs. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.