Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/preserve-teams-slack-email/

COLLABORATION EVIDENCE

Reconciling Teams, Slack and Email Collections Before Review

Decisions that once lived in email now sit across Teams channels, Slack threads and linked cloud documents, and a collection planned for all three looks for the edits, deletions and versions that decide a dispute. Freeze retention and map the channels before collection, then call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why Workplace Chat Calls for Its Own Collection Method

Modern business decisions rarely happen inside standalone email threads anymore. Key negotiations, engineering warnings and executive approvals move fluidly between Microsoft Outlook, Microsoft Teams channels, Slack workspaces and cloud storage links in SharePoint or Google Drive. When legal teams or internal IT staff plan a collection, the method is built to reach edited or deleted chat messages, ephemeral channel reactions and cloud modern attachments, where an email or chat message only contains a hyperlink to a live document that changes over time. A complete, connected chat collection keeps attorney review time focused and prepares the client to answer a motion to compel under Federal Rule of Civil Procedure 37(a) and, where data is lost, the measures Rule 37(e) allows.

Reconciling Message Versions, Channel Membership and Linked Cloud Files

Global Digital Forensics performs defensible eDiscovery collection and technical reconciliation engagements under the direction of retained litigation counsel, internal auditors and corporate legal departments. Rather than dumping unreadable JSON chat files into a review folder, our engineers map the complete communication ecosystem before review begins. We reconcile Microsoft Purview premium eDiscovery exports and Slack Discovery API feeds so that parent messages, threaded replies, participant join and leave timestamps and historical document versions linked via SharePoint or OneDrive are captured together as cohesive conversational records.

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

Rule 37(e) and the Duty That Attaches Before the Complaint

Federal courts measure chat preservation by the same rule they apply to email. Rule 37(e) permits curative measures when electronically stored information “is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery,” and it permits severe sanctions only on a finding of intent to deprive (Federal Rule of Civil Procedure 37(e)). The duty attaches when litigation is reasonably anticipated, which for most organizations is well before a complaint arrives. For collaboration platforms, reasonable steps reach the retention and auto delete settings that sit in the admin console, so the first thing we examine is the policy state, ahead of the messages.

Teams retention is governed by Microsoft Purview retention policies applied to Teams chats and channel messages, and a policy set to delete after a fixed period keeps running during a dispute until a hold is applied or the policy is changed, which is why the hold comes first. Slack retention is set per workspace and can differ for public channels, private channels and direct messages, and some plans let individual users shorten retention on their own conversations. We document the policy state at the moment of the hold with screenshots from the admin console, exports of the policy configuration and the timestamps of any changes, so counsel can show what reasonable steps were taken and when.

That documentation protects the client in two directions. If messages were already gone when the duty attached, the policy record is where the examiner documents whether the deletion was routine rather than reactive. If a custodian deleted a message after the hold, the platform's own audit trail, which we also preserve, is where we look for the deletion event and often the content or a version of it. Our guide to preventing evidence loss at enterprise handoffs covers the departure scenario, where this matters most, and the same preservation gate applies to chat platforms as to laptops.

What an Export Can Tell the Reviewer

A Purview eDiscovery export of Teams content yields messages with their timestamps in UTC, sender identity, thread and reply relationships, reactions, edit and deletion markers and the identity of the channel or chat. Slack exports and Discovery API feeds deliver JSON with message text, user identifiers, thread timestamps, edit history and file references. Both can show that a message existed, when it was posted and edited, and who was in the conversation. What a participant actually read is a separate question, approached through read receipts where they exist and are enabled, together with membership records and testimony. We explain how each fact is sourced at the outset so the review team presents the court with the facts the platform recorded.

The linked file deserves the closest attention. A Teams message that shares a document often contains only a reference to a file in SharePoint or OneDrive, and the file at that location may have been edited many times since. The review question is what the document said when it was shared, which the examiner reads from the SharePoint version history rather than the current file. Slack files are stored with the workspace, but files linked from Google Drive or Box behave the same way. Our collection reconciles each message reference to the version that existed at the message timestamp where the platform preserved it, and labels the current file as current wherever version history ends.

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

Membership and permission history matters almost as much. Whether an executive was in a channel on the day a warning was posted is a membership question, and Teams and Slack record join and leave events in their audit logs rather than in the message export. We collect those logs alongside the messages so the chronology can answer who could have seen what. The eDiscovery collections page describes the platforms and export methods this work covers, and the email forensics page describes how the mail side is handled in parallel. Collecting the three together is what lets a chronology stand on its own.

From Hold to Production: How the Collection Runs

The engagement opens with a policy and scope phase. We confirm the Microsoft 365 or Slack plan, inventory the retention and deletion settings, identify custodians and the channels, chats and workspaces they used, and apply or verify holds before any export begins. We ask whether custodians used personal devices with corporate apps, whether guest or shared channels cross into other tenants, and whether archived or deleted users still have recoverable data. Each answer shapes what is reachable, and settling them first keeps the work to a single planned collection.

Collection follows using the platform's native eDiscovery tooling or compliance export where it exists, with every export hashed and logged. Teams content is collected through Purview eDiscovery with the associated SharePoint and OneDrive files and their version history. Slack content is exported through the workspace export or Discovery API appropriate to the plan, with private channels and direct messages included where licensing permits. Email is collected from Exchange Online or Google Workspace in native format so headers and attachments remain intact. We record the parameters of each job so a later reviewer can reproduce it.

Reconciliation and production close the engagement. Raw JSON and loose files are threaded into chronological conversations with participants, edits, deletions and linked file versions resolved, and the result is loaded for review or produced with a load file that fits the receiving platform. Our eCloud Discovery platform performs this threading across Teams, Slack and email so a reviewer reads one conversation rather than three exports. Where the collection or its reconciliation is challenged, the examiner who ran it can sign a declaration describing the method and the parameters used. That declaration is far easier to write when the parameters were recorded as the job ran.

Collection Choices That Produce Evidence Rather Than Motions

The first choice is a planned collection in place of a convenience export. A planned collection reaches private channels, direct messages, edit history and linked file versions and documents the parameters used, which keeps the work to one collection rather than a second one under a court's eye. The second is collecting from the platform itself, because the platform's record carries the timestamps, participants and edits that screenshots of chat threads on a custodian's phone leave behind. A proper collection at the start costs less than any repair afterward.

Departing users call for their own planning. Deleting a Slack user or removing a Microsoft 365 license can start a deletion timer on the user's data, and in some configurations the user's direct messages move out of administrators' reach, so the hold is confirmed before any offboarding step. Retention policies set for storage

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

management keep running during a dispute until someone adjusts them. We recommend that legal hold procedures explicitly cover collaboration platforms and that offboarding scripts check for holds before they revoke licenses or delete accounts, so the hold travels with the account.

The third choice is proportion: mapping which channels matter so the collection covers them fully and stops there, which keeps review cost down and the answer timely. The scope phase described above does that, and our audit and discovery preparation guide lists the questions that narrow a collection while keeping it complete. A collection that is both complete for the custodians at issue and no wider than the dispute requires is the goal, and it is reachable when the mapping happens first. Review budgets are protected the same way.

Practical Steps to Scope a Defensible Multi Platform Collection

Before issuing collection instructions to corporate IT, confirm the organization specific licensing tier in Microsoft 365 or Slack, verify whether chat retention policies or auto delete rules are active on custodian accounts, and identify whether custodians used personal mobile apps alongside corporate workspaces. Our eCloud Discovery platform threads multi platform conversations into clean chronological transcripts that reduce attorney review time.

Call Global Digital Forensics at (800) 868-8189 to scope your next cloud and workplace chat collection with a senior eDiscovery examiner, or start with our guide to mapping cloud evidence across tenants. The initial consultation is free.

What Each Platform Export Carries and Omits

The body of the guide explains why a planned collection serves a matter better than a convenience export. This table shows, platform by platform, the method a defensible collection uses, what the resulting export contains and what the examiner collects alongside it. Use it when drafting the collection plan or when reading an opposing production, because the last column is where a complete collection is planned. Each row assumes the hold was confirmed before the export ran.

Collection method, contents and companion sources for each collaboration and email source.

Source	Collection method	What the export carries	What the examiner collects alongside it
Teams chats and channels	Purview eDiscovery with hold applied	UTC timestamps, sender, thread and reply links, edit and delete markers	SharePoint version history for linked files
SharePoint and OneDrive linked files	Export with version history	The document as it existed at each saved version	A note of where retained version history begins
Slack public channels	Workspace export for the plan in use	Message text, user identifiers, thread timestamps, edit history	Private channels and direct messages through the Discovery API
Slack private channels and direct messages	Discovery API where licensing permits	The same fields for the covered users	A check for records of users deleted before the hold

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

Source	Collection method	What the export carries	What the examiner collects alongside it
Exchange Online email	Native export with headers intact	Headers, attachments, folder structure, item metadata	A check of recoverable items for the period before the hold
Google Workspace Gmail	Vault export under the hold	Messages with headers and labels	The retention setting in force, documented
Platform audit logs	Export from the admin console or API	Channel membership changes, deletions, sharing events	The retention window, documented with the export

In the massive data discovery case study, emails and documents supplied raw were extracted with metadata and correlated into timelines so the legal team could follow a system's history, the reconciliation this guide applies to chat.

How to Begin and What Happens on the First Call

Have the platform plans and license tiers, the custodian list, the channels and workspaces at issue, the current retention settings if known, and the dates of any departures or account deletions. The examiner asks what the dispute concerns, whether a hold has issued, who administers each platform, whether guest or cross tenant channels are involved and what the review platform will be. From that conversation you receive a written proposal listing the sources, the export method for each, the reconciliation steps, the production format and the timing drivers specific to your environment. The initial consultation is free. Call (800) 868-8189 at any hour, or ask for a scheduled call through the contact form.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: Microsoft Teams eDiscovery and Slack import and export options.

Authorities cited in this guide: Federal Rule of Civil Procedure 37(e). Supplies the reasonable steps language quoted in the guide and the intent standard for severe sanctions, current text at Cornell LII. Microsoft Purview eDiscovery documentation. Establishes how Teams, SharePoint and Exchange content is placed on hold and exported through Purview, as published by Microsoft and consulted October 2026. Slack guide to import and export tools. Establishes which Slack plans and permissions govern export of public channels, private channels and direct messages, as published by Slack and consulted October 2026. Microsoft Purview audit log retention policies. Establishes the retention of the audit records that document channel membership and deletion events, as published by Microsoft and consulted October 2026.

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

FREQUENTLY ASKED

Before Collecting Teams and Slack

Can deleted Teams or Slack messages be recovered?

Often, within the bounds the platform and the retention configuration set. Teams messages deleted by a user are typically retained in the service for a period and remain discoverable through Purview eDiscovery if a retention policy or hold covers them. Slack preserves edit and deletion history on plans with compliance exports, and messages deleted before retention expired may remain in exports. The policy state determines what the platform still holds, which is why we examine it before anything else.

Do we need a particular Slack plan to collect direct messages?

It depends on the plan and the settings. Standard workspace exports cover public channels, and access to private channels and direct messages requires the plan tier and the export permissions that Slack grants for compliance purposes, in some cases after an application to Slack. We confirm the plan on the first call, identify what the current licensing can reach, and advise you on the path to the remaining content before collection begins so the review starts with a clear picture.

How do you handle files that were shared as links rather than attachments?

We treat the link as a pointer to a versioned document and collect the version history from SharePoint, OneDrive or the equivalent store, then reconcile each message to the version that existed at the message timestamp where the platform preserved it. Where version history was off or has been trimmed, the report records it, and the review team sees the current file clearly labeled as the current version.

What determines how long a collaboration platform collection takes?

The number of custodians and channels, the plan tier and export method available, whether holds were already in place, the volume of linked files and version history to reconcile, export throttling imposed by the platform, and whether a declaration is needed. A single workspace with holds in place collects far faster than a multi tenant environment with guest channels and departed users. We give a timing estimate in the written proposal after the first call, once the environment is known.

Are employees' personal phones with corporate chat apps in scope?

That is a legal question for counsel, and the technical answer informs it. If the corporate Teams or Slack app on a personal device synchronized with the corporate tenant, the content exists in the tenant and is collected there without touching the phone. If employees used personal messaging apps for business, the examination moves to the devices themselves, using the mobile forensics approach described on our mobile device forensics page.

Web Addresses for the Sources Cited

1. Federal Rule of Civil Procedure 37(e): https://www.law.cornell.edu/rules/frcp/rule_37
2. Microsoft Teams eDiscovery: https://learn.microsoft.com/en-us/purview/edisc
3. Slack import and export options: https://slack.com/help/articles/204897248-Guide-to-Slack-import-and-export-tools

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

4. Microsoft Purview audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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