Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/digital-forensics-moving-closer-to-the-center-of-the-clinton-email-drama/

DELETED EMAIL RECOVERY

How Forensic Examiners Reconstruct Deleted Executive Email, Off Channel Messages and Wiped Servers

Deleted messages, personal accounts and disappearing chat apps leave a distributed record across servers, recipients and handsets, well beyond any single mailbox. Preserve every endpoint and account that touched the communications first, and leave recovery to the examiner. Call (800) 868-8189 at any hour.

Published August 24, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

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

How Deleted Email and Personal Accounts Leave an Evidentiary Trail

In high profile regulatory inquiries, government investigations and complex commercial litigation, disputes frequently center on whether executives used unapproved personal email accounts, communicated via off channel messaging applications like WhatsApp or Signal, or attempted to purge email servers prior to a subpoena. Emptying the Deleted Items folder or wiping a single server touches one copy of a communication, and the examination looks for the others.

Multi Endpoint Correlation and Server Artifact Recovery

Electronic communication is inherently distributed: every email or message sent by one custodian leaves independent forensic traces across sending servers, intermediate transport gateways, cloud recoverable item substrates in Microsoft Purview, recipient mailboxes and synchronized mobile handsets. Working directly for retained litigation and regulatory counsel, Global Digital Forensics reconstructs deleted communication records by examining Exchange EDB databases, PST and OST local cache files, unallocated disk space, mobile SQLite write ahead logs and counterparty server headers. When a party uses specialized wiping utilities to purge records after a preservation duty attaches, our examiners document the exact execution artifacts of those wiping tools to support Rule 37(e) spoliation remedies.

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

Rule 37(e) and the Facts an Examiner Supplies

Spoliation disputes over electronic communications are decided under Rule 37(e), and the rule's structure tells us what the examination must establish. It applies when electronically stored information "that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery". Each clause is a technical question before it is a legal one. Was the information lost, or does it survive in a recoverable items folder, a backup, a recipient's mailbox or a synced handset? Were the steps taken reasonable in light of the retention settings and holds available on the platform? Can the content be restored or replaced from another source? The examiner works those questions through the platform's own records, and counsel argue from the answers.

The remedies turn on two further findings. Under subsection (e)(1), a court that finds prejudice "may order measures no greater than necessary to cure the prejudice". Under subsection (e)(2), the severe remedies of an adverse inference, a presumption instruction, dismissal or default are available "only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation". Intent is where forensic evidence matters most. The execution of a wiping utility days after a preservation letter, a retention policy shortened the week a subpoena arrived, a mailbox purged through a hard delete that bypassed the ordinary deleted items path, or a phone reset the night before a collection are the kinds of events the record captures with timestamps. We lay those sequences out as a timeline and let the court draw the inference. Our email forensics practice has supported hundreds of email related depositions and testimony engagements built on exactly this kind of analysis.

Where Deleted Email Persists and What Each Copy Shows

A message that a custodian believes is gone usually survives in several places, each with different evidentiary value. In Microsoft 365, deleted items move through the Recoverable Items folder, where retention policies and litigation holds can keep them long after the user has emptied every visible folder, and the unified audit log records SoftDelete, HardDelete, MoveToDeletedItems and MailItemsAccessed events by account, client and time. Microsoft publishes how long those audit records are kept by license level, and we export them before the window closes. Google Workspace keeps comparable records in Vault and in the Gmail log events. On the server side, Exchange database files and their transaction logs, and on the client side the OST and PST caches, retain message fragments in unallocated space that carving can recover. Every recipient's mailbox holds an independent copy, and every synced phone holds another.

Each source establishes something different, and the report says which. Audit logs record that a message existed and when it was deleted, by which account and through which client, which stands as evidence in its own right alongside any recovered content. Recoverable Items and backups establish content, and their metadata establishes the original dates. Recipient copies establish content and transmission, and the sender's own mailbox and server records are where we look for what became of the sender's copy. Handset databases show the message as the custodian saw it, together with read status and attachments. The scope of each source matters as much. For a retention window that closed before the engagement began, the examination turns to backups, recipients and handsets, and carved fragments are dated through surrounding records when

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

their headers are incomplete. When a personal account is involved, counsel pursues the provider's records through the available legal process and the account holder's own access, and we tell counsel early what to ask for. The Microsoft 365 forensics page describes the sources in more depth.

Off Channel Messaging and the Handset Collection

Regulators and courts have made off channel communications a central discovery issue, and the handset is where the record lives. iMessage, WhatsApp, Signal and Telegram each store messages in SQLite databases on the device, and the write ahead log files beside those databases frequently retain records of messages that the application no longer displays. Disappearing message settings are themselves recorded, so a conversation set to vanish after one day leaves evidence that the setting was chosen and when, which is often the point for a spoliation argument. Cloud backups of the handset, when they exist, carry earlier states of those databases. Veronica Perez leads our mobile work, and her examinations of mobile communications, application activity and location records have been designated in state superior courts and in federal court.

Collection can leave the phone with its owner. Our supported remote collection works through a link and a computer connection, normally with the custodian keeping the phone in use, and the collection usually runs from a few minutes to overnight depending on the setup. For executives whose phones hold both personal and business communications, counsel typically agree an inspection protocol that limits the examination to the accounts, contacts and date ranges at issue, and we document what was reviewed against the protocol so its observance is on the record. The full examination then ties the handset record to the server and mailbox record, so that a message deleted from the mailbox but present on the phone, or present in a recipient's handset but absent from the custodian's, is placed in a single timeline the court can follow.

Building the Spoliation Timeline Into a Declaration

A spoliation motion rises or falls on sequence, and the examiner's product is a timeline in which each entry is tied to an artifact. The preservation letter date comes from counsel. The retention policy change comes from the tenant's configuration audit log. The execution of the wiping utility comes from Prefetch, Amcache and the UserAssist key on the workstation, and from the SRUM database that records how much data the program read and wrote. The hard delete of the mailbox contents comes from the unified audit log, with the client application and IP address attached. The phone reset comes from the device's own logs and from the gap between the cloud backup date and the collection. Laid side by side, these entries show what happened and in what order, and they are the facts that support a finding of intent or refute one.

The declaration that carries the timeline is written to be tested. Each entry states the source, the tool used to parse it and how the result was validated, so that the opposing expert has to dispute the artifacts themselves rather than the examiner's description of them. Where the record supports more than one reading, the declaration sets out each, because candor on the small points earns trust on the large ones. Testimony follows the same discipline under Rule 702, and the examiner who built the timeline is the one who defends it at deposition. The digital forensics process guide explains how collection, examination, analysis and reporting fit together.

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

The same method serves a party accused of spoliation. A retention policy that deleted messages on schedule, a device replaced in the ordinary course or a mailbox cleaned under a documented records program all produce timelines in which the sequence shows routine administration rather than destruction, and the examiner's job is to present that sequence with the same precision. Counsel defending a motion need the configuration history of the tenant, the records policy in force and the dates on which each applied, laid against the date the preservation duty arose. A timeline that shows the deletions predated the duty, or followed a policy adopted long before the dispute, answers the intent prong directly and often narrows the remaining question to whether the content can be restored from another source.

Consult With a Senior Email and Messaging Forensic Examiner

Call Global Digital Forensics at (800) 868-8189 to discuss email recovery, off channel mobile collection or spoliation analysis for your matter. Our email forensics page describes what the examination covers. The initial consultation is free.

Where Deleted Email Still Lives and What Each Copy Establishes

The guide explains that a message a custodian believes is gone usually survives in several places, each with different evidentiary value. This table lists those sources, what each establishes and how the examiner reads it, so counsel can see which copy answers which question in a spoliation dispute. Read the last column alongside the dates of your matter, because retention windows and fragment headers shape which copy carries each point. Audit logs record that a message existed and when it was deleted, which stands on its own alongside any recovered content.

Where deleted email survives, what each copy establishes and how the examiner reads it.

Source	What it establishes	How the examiner reads it
Recoverable Items folder	Content kept by a hold after the user emptied folders	Governed by the retention and hold settings
Unified Audit Log delete events	That a message existed and when it was deleted	180 days standard per Microsoft
Exchange database and transaction logs	Message fragments in unallocated space	Dated through surrounding records when headers are incomplete
OST and PST client caches	Carved fragments on the workstation	Imaged early to capture unallocated space
Each recipient mailbox	Content and transmission	The sender's mailbox is checked for the sender's copy
Synced handset database	The message as the custodian saw it	Disappearing settings are recorded alongside the content
Personal account records	Content held by the provider	Reached through counsel's subpoena

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

The COMLAB v. Kal Tire matter turned on a claimed deletion after an alleged virus, where metadata analysis contradicted the explanation, the multi source reconstruction this guide applies to deleted email.

How to Begin and What Happens on the First Call

Have ready the accounts and devices involved, the platform and license tier for the corporate mailboxes, the dates that matter, including any preservation letter, subpoena or regulatory request, and what has already been done to recover or preserve messages. The examiner asks whether litigation holds are in place, whether audit logging was enabled and for how long records are kept, which messaging applications the custodians use, whether personal accounts or devices are implicated and what the court or regulator has asked for. Counsel then receive a written scope setting out the preservation steps in order of urgency, the recovery and analysis phases, the collection approach for handsets and the timing, with a proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers 24/7.

Technical References and Further Reading

Earlier reporting on this subject: The Washington Post on the court pressing the State Department about the Clinton email server, August 20, 2015.

Authorities cited in this guide: Federal Rule of Civil Procedure 37(e), Failure to Preserve Electronically Stored Information. Sets the threshold findings and the two tiers of remedies for lost electronically stored information, current rule text as amended in 2015. Microsoft Learn, Manage audit log retention policies. Documents how long Microsoft 365 mailbox audit events are retained by license level, current Microsoft documentation. Federal Rule of Evidence 702, Testimony by Expert Witnesses. Governs the reliability showing for the examiner's spoliation testimony, as amended effective December 1, 2023. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Describes the collection, examination, analysis and reporting phases applied to mailbox, server and handset evidence, final version 2006.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Deleted Email Recovery

Can deleted emails be recovered from Microsoft 365 after the user emptied the deleted items folder?

Frequently, yes. Emptying Deleted Items moves messages into the Recoverable Items folder, where they remain for the retention period configured on the mailbox, and far longer when a litigation hold or retention policy applies. Even when the content has aged out, the unified audit log records the deletion events themselves for as long as the license tier keeps audit data. Recipient mailboxes, server backups and synced phones hold independent copies. The first step is to place the mailbox on hold and export the audit records before anything else changes, which is why timing drives what can be recovered.

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

Can you tell when an email was deleted and by whom?

Usually, when audit logging was active. Microsoft 365 records SoftDelete, HardDelete and MoveToDeletedItems events with the account, the client application, the IP address and the time, and Google Workspace keeps comparable Gmail log events. Those records distinguish a user clicking delete in Outlook from an administrator purge or a retention policy sweep, which is often the central question in a spoliation dispute. For periods outside audit coverage, the examiner reads the deletion time from client cache files, backups and recipient copies, and the report states that inference with its basis.

Can disappearing messages in Signal or WhatsApp be recovered?

Sometimes, and the setting itself is always informative. Expired messages leave the application's visible database, and write ahead log files, cached attachments, notification records and device backups taken before expiry are where the examiner looks for content or metadata. The configuration record showing when a conversation was set to disappear, and by whom, survives and is frequently the more important finding for counsel, because it shows a choice made at a particular time. The counterparty's handset is an independent source, and we advise counsel on seeking it early.

Does a personal email account have to be produced in litigation?

That depends on the court, the claims and the showing that business was conducted through the account, and it is a question counsel answers. What the examination supplies is the showing: corporate messages forwarded to the personal address, replies from it in recipients' mailboxes, the account signed in on the corporate laptop or phone, and calendar entries or attachments that originated there. With that record in hand counsel can seek the account through a targeted request or subpoena, and when production is agreed we collect under a protocol that confines the review to the matters at issue.

How do you show that someone used wiping software before a collection?

Through the execution artifacts the operating system keeps regardless of what the tool deleted. Windows records program execution in Prefetch, Amcache, Shimcache and UserAssist, and the SRUM database logs how much data each program read and wrote by hour. The tool's installer, configuration files and its own logs often remain. The file system shows the pattern of what was removed and when, through the USN journal and the timestamps of surviving entries. We place those facts against the preservation letter date and the collection date, and the timeline speaks for itself in the declaration.

Web Addresses for the Sources Cited

1. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://csrc.nist.gov/pubs/sp/800/86/final
2. Rule 37(e): https://www.law.cornell.edu/rules/frcp/rule_37
3. Rule 702: https://www.law.cornell.edu/rules/fre/rule_702
4. The Washington Post on the court pressing the State Department about the Clinton email server, August 20, 2015: https://www.washingtonpost.com/news/post-politics/wp/2015/08/20/judge-presses-state-department-to-learn-more-about-clintons-e-mail-server/
5. Microsoft Learn, Manage 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 October 31, 2026.

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

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.