Forensic Collection Of Exchange Online Mailboxes

This guide addresses the forensic collection of Exchange Online mailboxes, detailing how to access all layers of mail, including deleted and archived items, while preserving critical metadata. It covers mailbox anatomy, common mistakes, and the importance of expert involvement for UK litigators.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/forensic-collection-of-exchange-online-mailboxes

EXCHANGEONLINEEVIDENCE · A GUIDE FOR UK LAWYERS Forensic Collection of Exchange Online Mailboxes Active, Archived, Deleted and Recoverable Mail: Reaching Every Layer of the Mailbox, with Metadata Intact COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the mailbox beneath the mailbox 03 Mailbox anatomy: the layers and what each holds 04 What deleted means, layer by layer 05 Collection: reaching every layer with metadata intact 06 Permissions, delegation and who-read-what 07 Message metadata and authenticity 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: AMAILBOXISALAYEREDSTORE, ANDMOST " DELETED " MAILIS ALAYERQUESTION

§ 02 · FIRST PRINCIPLES The problem in plain English: the mailbox beneath the mailbox

§ 03 · ANATOMY Mailbox anatomy: the layers and what each holds LAYER WHAT IT HOLDS · HABITS THAT MATTER

§ 04 · DELETED, REALLY? What deleted means, layer by layer

§ 05 · GETTINGITOUT Collection: reaching every layer with metadata intact

§ 06 · OTHERHANDS Permissions, delegation and who-read-what

§ 07 · ISITREAL? Message metadata and authenticity

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE JOURNAL / + AUDIT MAILBOX CACHES COUNTERPART DELETED / STACK (OST/ TENANTS RECOVERABLE DEVICE MOBILE) BACKUP / TRANSPORT ARCHIVE LOGS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEPURGEPRESERVEDBYTHEHOLD EXAMPLE2 · THEARCHIVETHATHELDTHEMISSINGYEARS EXAMPLE3 · THEEMAILTHATEXISTEDINONLYONEMAILBOX

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · MAILB OX LIMBFORTHECOLLECTIONSPECIFIC AT ION

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The Exchange Online checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions The custodian deleted emails months ago. Can they be recovered? Can a user or admin permanently destroy mail on a held mailbox? How do we prove the other side received and read an email? What about the OST file on the laptop: is it worth collecting? Are auto-forwarding rules really that significant? Our exhibit email is challenged as fabricated. What should we commission?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

The custodian deleted emails months ago. Can they be recovered?

Run the four facts: if a hold predated the deletion, yes: the Purges/Versions layers kept them, dated; if no hold and the recoverable window has passed, not from the mailbox: and the architecture paths (device caches, counterpart tenants, backups, journals) take over, frequently successfully. The answer is never "probably": it is an hour's tenant lookup, and the honest report states which case applies and why.

Can a user or admin permanently destroy mail on a held mailbox?

Users, no: every user-level deletion route ends in a preserved layer while the hold stands, and the attempts are enumerable (Example 1). Admins can release holds and alter retention: actions that are themselves audit-logged and, mid-dispute, approximately confessional. The practical assurance: a hold placed early and left alone converts the mailbox into an append-only record: which is why the week-one hold is this block's recurring hero.

How do we prove the other side received and read an email?

In layers of strength: transport trace (delivery to their tenant: strong, window-bound); their mailbox's collected copy (existence at collection); audit read-events where licensing and configuration recorded them (guide 57: genuine read evidence, not universal); and conduct corroboration (replies, forwards, actions consistent with knowledge). Read receipts are weak and refusable. The report stacks what exists and names each layer's weight: "delivered, present, and acted upon" usually suffices where "read at 14:32" is unavailable.

What about the OST file on the laptop: is it worth collecting?

Frequently decisive: the OST is the mailbox as last synced: which means it can preserve what tenant-side deletion later removed, capture the pre-purge state of a mailbox whose hold came late, and survive the account's deletion entirely. Guides 41 and 48's imaging disciplines apply; the comparison of OST contra tenant is itself a deletion chronology. In leaver and spoliation matters, the device cache is standard scope, not an afterthought.

Are auto-forwarding rules really that significant?

Repeatedly: a rule forwarding to a personal account is a continuous exfiltration channel with a creation date, an author context and (in audit) a paper trail: and its discovery reframes matters instantly ("what left, since when, and where did it go" becomes computable). The configuration export costs minutes; check it in every departure, leak and fraud matter before anything else is theorised.

Our exhibit email is challenged as fabricated. What should we commission?

The Example 3 workup, from your side: full item with headers and properties from every layer of your mailbox; counterpart collection or requests at the other end; transport and authentication analysis; and layer-coherence review (does the item sit in the stores a genuine message of its date would occupy, including hold structures?). Genuine messages pass this convergently and fast; the report then carries CPR 35 weight the bare exhibit never could. Commission it before the hearing, not after the insinuation lands. cflab. u k · e-disc ove r y. u k