Shared Mailboxes Delegated Access And Who Really Sent The Email

Shared mailboxes and delegated access complicate email attribution, as the 'From' line is a label, not a signature. This guide details access models, collection strategies, and attribution methods using logs, permissions, and devices to prove who acted, not just which mailbox sent the email.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/shared-mailboxes-delegated-access-and-who-really-sent-the-email

SHAREDMAILBOXES & DELEGATION · A GUIDE FOR UK LAWYERS Shared Mailboxes, Delegated Access and Who Really Sent the Email Attribution When the Sender Field Names an Inbox, Not a Person COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES MAILBOX ATTRIBUTION ANALYSIS

§ CONTENTS

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: SHAREDANDDELEGATEDMAILBOXESSEPARATETHEMAILBOX FROM THE PER S ON: COLLECTTHEMAILBOXASITSOWNSOURCE, ANDATTRIBUTETHE ACTFROMTHEAUDITTRAIL, THEPERMISSIONHISTORYANDTHEDEVICE, NEVER FROM THEFROMLINEALONE

§ 02 · FIRST PRINCIPLES The problem in plain English: the From line is a label, not a signature

§ 03 · THE ACCESS MODEL S The access models: shared mailboxes, delegation, send-as and send-on-behalf

§ 04 · MAILWITHOUTHANDS Rules, forwards and automation: mail that moves without a human 95

§ 4's selectivity) frequently the most telling fact in the case.

§ 05 · COLLECTION Collection: scoping shared and delegated mailboxes so nothing is missed

§ 06 · WHOACTED Attribution: proving which person acted from logs, permissions and devices

§ 07 · DEPLOYMENT Compromise, misuse and the legal deployment of attribution findings

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION MAILBOX AUDIT CONFIGURATION SESSION COUNTERPART THE MAILBOX PERMISSION / SIGN-IN / RECIPIENT + ITSELF LOG LAYER LAYER COPIES END POINT ARTEFACTS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEAPPROVALTHEFINANCEDIRECTORNEVERGAVE EXAMPLE2 · THESHAREDMAILBOXTHATWASNEVERCOLLECTED EXAMPLE3 · THERULECREATEDAT02: 1

§ 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 PROTOCOL

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The shared and delegated mailbox checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions The email came from the executive's address. Isn't that proof she sent it? Why would a shared mailbox be missed in disclosure? What is the difference between send-as and send-on-behalf, and why does it matter? Can we prove who created a forwarding rule? Mailbox audit logging was off. Is attribution impossible? The assist an t sent it under standing instructions. Does attribution even matter?

§ 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 email came from the executive's address. Isn't that proof she sent it?

No: a delegate with send-as rights produces an identical header, and a compromised session produces the same again (§3, §7): Example 1's approval was sent by an assist an t and looked exactly like the director's own. The audit log, permission history and sign-in context prove the actor; the From line proves only the mailbox.

Why would a shared mailbox be missed in disclosure?

Because it is not a custodian: scoping by named individuals collects their mailboxes and leaves the team inbox untouched, unheld and expiring on its own retention (§5, Example 2). The permission census finds it; the DRD names it as a source; the hold reaches it. Ask every relevant team which inboxes they actually work from.

What is the difference between send-as and send-on-behalf, and why does it matter?

Send-on-behalf marks the real sender visibly ("A on behalf of B"); send-as does not: the message appears to be B's alone. For attribution, send-on-behalf is answered on the face of the message (if the marker survived production); send-as is answered only from the mailbox audit log (§3, §6): which is why logging status is the first question in any disavowal.

Can we prove who created a forwarding rule?

Usually: rule creation is an audited event recording the acting account, session and time, and the sign-in log joins the session to a device and location (§4, §6): Example 3's rule was attributed to an external session without MFA. The rule's timing against the dispute is often the most telling fact, and the configuration export documents exactly what it did.

Mailbox audit logging was off. Is attribution impossible?

Harder, not impossible: the permission census bounds who could have acted, sign-in logs date sessions, recipients' copies prove the send and may hold on-behalf markers, end point artefacts show drafts and client activity (§8). The report states the missing spine and builds the lattice from the rest: and the or g an is at i on turns logging on for next time.

The assist an t sent it under standing instructions. Does attribution even matter?

It settles the facts so the law can do its work: once the assist an t is established as the sender, the questions become authority, ratification and reliance: Example 1's second half: which the same evidence (the assistant's send-as history, the instructions' scope) informs. Attribution rarely ends a dispute; it ends the argument about what happened so the argument about what it means can be had properly. cflab. u k · e-disc ove r y. u k