COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

# Shared Mailboxes, Delegated Access and Who Really Sent the Email

## Attribution When the Sender Field Names an Inbox, Not a Person

The email came from finance@ or from the managing director's address; it committed the company, or made the threat, or approved the payment. Who actually sent it? In modern Microsoft 365 and Google Workspace estates the answer is frequently not the name on the From line: shared mailboxes are used by teams, executives' mailboxes are worked by assistants under delegated permissions, "send as" and "send on behalf" rights let one person write in another's name, and mailbox rules and auto-forwards move mail without anyone touching it. For the lawyer, this collapses two separate questions: what did the mailbox send and receive (a collection problem with its own traps: shared mailboxes are often omitted from custodian-based scoping), and which human being acted (an attribution problem answered from audit logs, permission histories and device artefacts rather than the header). This guide covers both for UK lawyers: how shared and delegated access works, where the evidence of who-did-what lives, and how to collect and prove it.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

**PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM**

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Attribution questions in shared and delegated mailboxes are a recurring instruction: the executive who denies sending, the assistant who did, the shared inbox from which a mandate was approved, the auto-forward that leaked the deal: answered from audit logs, permission histories and endpoint artefacts rather than the From line, and reported under CPR Part 35 where the sender is the case.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | MAILBOX ATTRIBUTION ANALYSIS | DELEGATION & RULE FORENSICS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

# In this guide

§ 0 1 · ORIENTATION

# Executive summary

THE HEADLINE POINT: SHARED AND DELEGATED MAILBOXES SEPARATE THE MAILBOX FROM THE PERSON: COLLECT THE MAILBOX AS ITS OWN SOURCE, AND ATTRIBUTE THE ACT FROM THE AUDIT TRAIL, THE PERMISSION HISTORY AND THE DEVICE, NEVER FROM THE FROM LINE ALONE

**The models (§3):** a shared mailbox has no user of its own and is accessed by members with full-access permissions; delegation grants one user access to another's mailbox at folder or mailbox level; *send-as* permission lets the delegate send mail that appears to come from the owner with no trace in the header; *send-on-behalf* produces a visible "on behalf of" marker; and automated rules, auto-forwards and connectors move mail without any human action at all (§4). Each model leaves different evidence: send-on-behalf is header-visible; send-as is not, and is proven only from server-side logs. **Collection (§5):** shared mailboxes are not custodians and are routinely missed by custodian-based scoping; delegated mailboxes are collected as the owner's source but the delegates' activity within them is a separate question; the census of mailbox permissions (who could access what, when, with which rights) is the scoping document, drawn from directory and Exchange administration data. **Attribution (§6):** Exchange mailbox audit logging records who accessed which mailbox and performed which action (send-as, send-on-behalf, create, move, delete) with the acting account, session and client details; Entra sign-in logs supply the device, IP and authentication context; endpoint artefacts corroborate the hands at the keyboard: the guide 105-107 attribution disciplines applied to mail. **Deployment (§7):** the same evidence distinguishes the assistant's sanctioned send from the executive's disavowal, the compromised account from the malicious insider (guide 98 §3's mandate fraud), and the negligent auto-forward from the deliberate leak: findings that reach employment, fraud, contract-formation and data-breach questions, evidenced under CPR Part 35 where the sender is disputed.

- **Send-as leaves no header trace:** the From line is the owner's; the audit log is the only witness to the delegate.
- **Shared mailboxes are not custodians:** scope by permission census, or the finance@ inbox never enters the production.
- **Mailbox audit logging is the spine:** acting account per action, per mailbox: verified enabled and exported inside retention.
- **Rules act without hands:** forwards, moves and deletions by rule are logged as rule events: the "who" is whoever created the rule, and when.
- **Attribution is a lattice:** audit log, sign-in context, device artefact, physical presence: guide 96's corroboration applied to a single click.

§ 0 2 · FIRST PRINCIPLES

## The problem in plain English: the From line is a label, not a signature

Email's oldest design assumption is that an address belongs to a person. Corporate estates broke it decades ago: teams share inboxes, executives' correspondence is run by assistants, cover arrangements grant colleagues each other's mailboxes, and automation routes messages by rule. The platforms accommodate all of it with permission models whose evidential consequences are invisible to users: an assistant with send-as rights produces an email indistinguishable, to any recipient, from one the executive typed. A rule created in a compromised mailbox forwards every message to an attacker with no human sender at all.

Litigation then asks the naive question: "did you send this?" The honest answer is often "my mailbox did". Resolving that is not a matter of header analysis (guide 87's tools stop at the server that accepted the message) but of server-side audit: the platform records which authenticated account performed the send, from which session, using which permission: if the logging was on, and if the logs were kept. This guide is the discipline for collecting shared and delegated mailboxes without missing them, and for turning "my mailbox did" into a named account, a session and, with corroboration, a person.

§ 0 3 · THE ACCESS MODELS

# The access models: shared mailboxes, delegation, send-as and send-on-behalf

- **Shared mailboxes:** a mailbox without its own user or licence (in Microsoft 365) or a collaborative inbox or group (in Google Workspace), accessed by members holding full-access permission: everything in it is the team's, and nothing in it is anyone's personal store: collected as a source in its own right.
- **Delegated access:** a user grants another (an assistant, a colleague on cover) access to their mailbox at folder or full-mailbox level: the delegate reads, replies, files and deletes inside the owner's mailbox; the owner's mailbox is the store; the delegate's actions are the attribution question.
- **Send-as:** the permission to send messages that show the owner (or shared mailbox) as the sender with no indication of the actual sender: recipients see the owner's name; the header shows the owner's address; only the platform's audit trail records the delegate's account as the actor.
- **Send-on-behalf:** the permission to send with a visible marker ("Assistant on behalf of Executive"): the header and the recipient's view both show the real sender: the attribution question answered on the face of the message, if the marker survived the recipient's client and the production.
- **Permission histories:** who held which right on which mailbox, granted and revoked when: recorded in Exchange and directory administration audit data: the census that says who *could* have acted, narrowing who *did*: with the caveat that historic permission records are bounded by audit retention.

§ 0 4 · MAIL WITHOUT HANDS

# Rules, forwards and automation: mail that moves without a human

- **Inbox rules:** user- or delegate-created rules that forward, redirect, move, mark or delete matching mail: the mechanism behind the missing message (moved to an obscure folder), the leaked message (forwarded externally), and the concealed compromise (attacker rules hiding replies): each rule's creation is an audited event naming the creating account and session.
- **Auto-forwarding and redirection:** mailbox-level forwarding to internal or external addresses, set by user or administrator: the guide 97 §4 exfiltration route and the guide 98 §3 mandate-fraud precursor: logged at creation and, where transport rules capture it, at each forward.
- **Transport and organisation rules:** tenant-level mail-flow rules (journaling, DLP, auto-forward blocks) that move, copy or block mail: administrator-created, audited, and sometimes the reason a message never arrived or a copy exists nobody expected.
- **Connectors, apps and automation:** third-party apps granted mailbox access, Power Automate flows sending mail, integration connectors: senders that are neither people nor rules: enumerated from app-permission and consent records, and the source of "who sent this?" answers that are "a workflow, created by X on Y".
- **The evidential point:** every automated action traces to a creating account and a creation time: attribution shifts from the message to the rule, and from the rule to whoever made it: with the rule's creation timing (guide 95 §4's selectivity) frequently the most telling fact in the case.

§ 0 5 · COLLECTION

# Collection: scoping shared and delegated mailboxes so nothing is missed

- **The permission census:** before scoping: every shared mailbox relevant to the issues, every delegation touching relevant custodians, every send-as and send-on-behalf grant, and their histories: drawn from Exchange and directory administration data and recorded as the scoping exhibit: the guide 101 census discipline, applied to permissions.
- **Shared mailboxes as sources:** named in the DRD and the collection plan as sources distinct from custodians, held (shared mailboxes need holds too, and are often missed), and collected with their folder structures and the sent-items that record what the team sent under the shared name.
- **Delegated mailboxes:** the owner's mailbox collected as their source; the delegate's own mailbox collected as theirs; the delegate's actions within the owner's mailbox obtained from the audit layer (§6), not from either mailbox's content: three collections for one relationship.
- **Sent-items and copies:** where a delegate sends as the owner, the sent item may land in the owner's sent-items, the delegate's, both or neither depending on configuration: the census establishes the setting, and the collection checks both stores rather than assuming.
- **Rules and configuration exported:** inbox rules, forwarding settings, transport rules and app permissions collected as configuration artefacts alongside content, with their audit histories: the §4 mechanisms documented, not inferred from their effects.

§ 0 6 · WHO ACTED

# Attribution: proving which person acted from logs, permissions and devices

- **Mailbox audit logging:** Exchange records per-mailbox actions (send-as, send-on-behalf, create, update, move, soft- and hard-delete, folder binds) with the acting account, the logon type (owner, delegate, admin), client information, session identifiers and timestamps: the direct record of who did what in whose mailbox: subject to logging having been enabled for the actions and mailboxes concerned (default coverage has improved but is verified per tenant) and to retention (guide 105's windows).
- **Sign-in and session context:** Entra sign-in logs join the acting account's session to a device, IP address, location, authentication method and application: distinguishing the assistant's desk from the executive's phone, and either from an attacker's session abroad.
- **Permission-history narrowing:** the §3 census says who held send-as at the moment of sending: a message sent-as the owner while only one delegate held the right is attributed at the permission layer before the audit log is opened.
- **Endpoint corroboration:** the acting account's device artefacts (client caches, application logs, the message's draft traces) and the physical layer (badge, CCTV, calendar) per guide 96's lattice: the hands-at-the-keyboard question closed with independent sources.
- **The honest ceiling:** attribution reaches the authenticated account and its session; shared credentials, unlocked workstations and compromised accounts (§7) are the alternatives the report must address: guides 105-107's standing caveat, with the corroboration lattice as the answer.

§ 0 7 · DEPLOYMENT

# Compromise, misuse and the legal deployment of attribution findings

- **Sanctioned delegation:** the assistant who sent as the executive under standing authority: attribution establishes the mechanics; the legal question is authority and ratification: contract formation, authorised communication, employment disputes about who said what: the evidence supports whichever side the authority facts favour.
- **Disavowal:** the executive who denies sending the message that bears their name: the audit log names the account and logon type; the sign-in log names the device; the permission census names who could: disavowal becomes either corroborated (a delegate or attacker acted) or refuted (the owner's own session, own device, own desk).
- **Compromise:** the attacker's session, rules and sends (guide 98 Example 3's mandate fraud, guide 99 §4's entry phase): distinguished from insider misuse by session context, rule-creation patterns and the attacker's infrastructure: with the organisation's own control failures (no MFA, forwarding allowed) documented for the liability allocation.
- **Insider misuse:** the delegate exceeding authority, the colleague on cover reading what they should not, the forward set up before resignation (guide 97): audit-logged actions against permission scope and role: the employment and confidence claims grounded in the record.
- **Data-breach dimensions:** auto-forwards and misdirected sends as personal-data breaches with ICO notification questions (guide 99 §6): the attribution work feeding the breach assessment as much as the litigation.

§ 0 8 · THE WIDER MAP

# Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the shared or delegated mailbox is one store; the evidence of who acted in it is distributed across the platform and beyond. The mailbox itself (content, sent-items, folder state) shows what happened to messages. The mailbox audit log shows who did it, by account and session. The permission and configuration layer (delegation grants, send-as rights, rules, forwards, app consents, with their administration audit histories) shows who could, and what automation was in play. The sign-in layer joins accounts to devices and locations. The recipients' mailboxes hold the messages as received, including send-on-behalf markers the sender's production may have lost, and the external counterpart's copy that proves a send occurred whatever the sender's sent-items show. Endpoints hold client caches and draft artefacts. When one layer is missing: audit logging disabled, retention expired, the mailbox purged (guide 103): the table names the survivors: the recipient's copy proves the send; the permission history bounds the actor; the sign-in log dates the session; the rule's creation record names its author.

| QUESTION | THE MAILBOX ITSELF | MAILBOX AUDIT LOG | PERMISSION / CONFIGURATION LAYER | SIGN-IN / SESSION LAYER | RECIPIENT + COUNTERPART COPIES | ENDPOINT ARTEFACTS |
|---|---|---|---|---|---|---|
| **What was sent / received** | Y: content + folders | Send events | n/a | n/a | Y: as received | Client caches |
| **Which account acted** | n/a | Y: the direct record | Who could: the bound | Session attribution | On-behalf markers | Draft + app traces |
| **From which device, where** | n/a | Client info | n/a | Y: device, IP, method | n/a | Y: the device itself |
| **Was it automated** | Rule effects visible | Rule-triggered events | Y: rules, forwards, apps | App sign-ins | Forwarded copies | n/a |
| **Who created the rule, when** | n/a | Y: rule creation events | Y: configuration history | Session at creation | n/a | Client-side rule artefacts |

Fallback strategy in one line: when the audit log is silent, bound the actor from permissions, date the session from sign-ins, prove the send from the recipient, and read the rule from its creation record: the From line is the last source consulted, not the first.

§ 0 9 · IN THE WILD

# Worked examples

### EXAMPLE 1 · THE APPROVAL THE FINANCE DIRECTOR NEVER GAVE

A supplier sued on a payment approval emailed from the finance director's address; the director swore she had not sent it. The header supported the supplier: her address, no on-behalf marker. The §6 work reversed the inference: mailbox audit logging showed the send as a *send-as* action by a delegate account: the accounts-payable assistant, who held send-as rights on the director's mailbox for routine correspondence; the sign-in log placed the session on the assistant's workstation; and the permission census showed the assistant as the only delegate with the right that week. Attribution was settled: the assistant sent it. The legal case then turned on authority: whether the assistant's standing instructions covered approvals of that size: an issue the same evidence (the assistant's prior send-as history, all routine) informed. The From line had named the wrong person; the audit log named the right one; the law decided what that meant.

### EXAMPLE 2 · THE SHARED MAILBOX THAT WAS NEVER COLLECTED

A regulatory investigation into a firm's complaints handling scoped custodians by name: the complaints manager, two handlers, the compliance officer. The production was thin on the very correspondence the regulator wanted. The §5 permission census, run belatedly, found the reason: complaints@ was a shared mailbox with six members, holding four years of inbound complaints and the team's replies sent under the shared name: none of it in any custodian's mailbox, none of it held, and eleven months of it already past the tenant's retention. The re-collection covered what survived; the regulator's questions about the gap were answered from the retention records and the census; the firm's disclosure statement was corrected. The lesson is §5's first line: shared mailboxes are sources, and a custodian list that never asked "which inboxes does this team work from?" has missed them by design.

### EXAMPLE 3 · THE RULE CREATED AT 02:14

A deal's confidential terms reached a competitor. The leak inquiry started with people and ended with a rule: the mailbox audit log for the deal lead's account recorded an inbox rule created at 02:14 on a Sunday, forwarding all mail containing the project codename to an external address, with the session's sign-in from an IP range in another country and an authentication without MFA (the account had been excluded from the MFA rollout as a "VIP exception"). The compromise was external; the control failure was internal; the forwarding had run for nineteen days before the leak surfaced, the rule hidden in a folder-move configuration that kept the forwarded items out of sight. The §7 deployment ran three ways: the data-breach notification assessed from the rule's match history, the insurance claim on the compromise evidence, and the deal counterparty's negligence allegation answered with the control record and the remediation. Nobody at the firm had sent anything; a rule created by an attacker had, under a name that was not theirs.

§ 10 · WHERE IT GOES WRONG

# Common mistakes and technical limitations

## Common mistakes

- **Attribution from the From line:** Example 1's initial inference: the header treated as a signature.
- **Shared mailboxes outside scope:** Example 2's gap: custodian lists that never asked about team inboxes.
- **Holds that miss shared mailboxes:** retention running on the finance@ inbox while custodians' mailboxes were held.
- **Audit logging assumed enabled:** the attribution spine discovered to be off, or off for the relevant actions, when the question arrives.
- **Audit retention missed:** the log that would have named the actor expired during the pleadings: guide 105's windows, again.
- **Rules never exported:** the forwarding that explains the leak inferred from effects instead of read from configuration: Example 3's rule found late.
- **Send-on-behalf markers lost in production:** the visible attribution stripped by conversion (guide 88): the honest sender made invisible by processing.
- **Delegation collected once:** the owner's mailbox produced, the delegate's mailbox and the audit layer never touched: one collection where three were needed.

## Technical limitations

- **Logging coverage is configurable:** which actions are audited, for which mailboxes, varies by tenant and licence: verified per matter, and stated in the methodology where gaps exist.
- **Retention bounds history:** audit and sign-in logs expire on licence-dependent schedules: attribution for older events rests on §8's alternates.
- **Accounts are not people:** shared credentials, unlocked sessions and compromise mean the audit log's account is the start of attribution, not its end: the corroboration lattice closes the gap, or the report states it open.
- **Platform behaviour moves:** default audit settings, sent-items behaviour for delegates and forwarding controls change with platform updates: current documentation checked per matter, per this series' standing rule.
- **Automation obscures intent:** a rule's effect is mechanical; its creator's purpose is inferred from timing, scope and context: stated as inference, per guide 95 §4's honesty.

§ 11 · INTERROGATORIES & DRAFTING AIDS

# Questions to ask · Suggested wording

## Ask your client

- Which shared mailboxes and group inboxes do the relevant teams work from, and who holds access to them: the §5 census?
- Who has delegated, send-as or send-on-behalf rights on the relevant individuals' mailboxes, and since when?
- Is mailbox audit logging enabled for the relevant mailboxes and actions, and what is the retention: and can the logs be exported today?

## Ask your opponent

- Please identify all shared mailboxes and group inboxes used by [the relevant teams] during [period], confirm whether each was placed under hold and collected, and state the retention applicable to each.
- Please disclose the mailbox permission history for [named mailboxes], including all full-access, delegate, send-as and send-on-behalf grants and revocations during [period], and the mailbox audit log entries for [the messages / actions in issue], identifying the acting account, logon type, session and client details.
- Please disclose all inbox rules, forwarding settings, transport rules and application permissions affecting [mailboxes] during [period], with their creation and modification histories.

## Ask your eDiscovery / forensic provider

- Does the permission census cover every relevant mailbox, with histories: and are shared mailboxes held and in the collection plan as sources?
- What does the audit log show for the actions in issue: account, logon type, session: and what corroborates the session to a device and a person?
- Have rules and forwarding configurations been exported with their creation records?

### SUGGESTED WORDING · SHARED AND DELEGATED MAILBOX PARAGRAPH FOR THE DRD / PROTOCOL

> "Shared mailboxes, group inboxes and mailboxes subject to delegated, send-as or send-on-behalf access used by relevant individuals or teams are data sources for the purposes of disclosure, distinct from individual custodians. Each party shall identify such mailboxes by a census of mailbox permissions (including their histories) drawn from administration records, shall place them under hold, and shall collect them as sources with folder structures and sent items intact. Where the identity of the person who sent, received, moved or deleted a message is or may be in issue, the parties shall preserve and, on request, disclose mailbox audit log entries, sign-in records, permission histories and mailbox rule and forwarding configurations relevant to the message or action, and shall ensure that send-on-behalf indications are preserved in any converted production format."

§ 12 · QUICK CONTROL

# Checklist and red flags · When to involve a digital forensic expert

## The shared and delegated mailbox checklist

- ☐ Permission census recorded: shared mailboxes, delegations, send-as, send-on-behalf, histories
- ☐ Shared mailboxes named as sources in the DRD; held; in the collection plan
- ☐ Owner, delegate and audit layers each collected for delegated relationships
- ☐ Mailbox audit logging status and retention verified; logs exported now
- ☐ Sign-in logs exported for the relevant accounts and period
- ☐ Rules, forwards, transport rules and app permissions exported with histories
- ☐ Sent-items behaviour for delegates established; both stores checked
- ☐ Send-on-behalf markers preserved through processing and production
- ☐ Attribution corroborated: account, session, device, physical layer
- ☐ Alternatives (shared credentials, compromise) addressed in the report

## Red flags

- Team correspondence absent from every custodian's mailbox: Example 2's shared inbox.
- Disavowed messages with no on-behalf marker: Example 1's send-as.
- Rules created out of hours, from unusual locations, without MFA: Example 3's 02:14.
- Forwarding to external addresses in any relevant mailbox.
- Audit logging disabled or unverified on a litigation-prone tenant.
- "VIP exceptions" to security controls on executive mailboxes.
- Opposing productions where delegated mailboxes appear but delegates' activity is never explained.

## When to involve a digital forensic expert

At scoping, where the permission census reveals the shared mailboxes and delegations a custodian list cannot (Example 2's morning); at collection, where the three layers of a delegated relationship are gathered and the audit logs exported inside retention; at attribution, where the acting account is joined to session, device and person with alternatives addressed (Example 1's reversal); and at deployment, where compromise, misuse and disavowal are distinguished for employment, fraud, contract and breach purposes under CPR Part 35 (Example 3's three tracks). Through **e-discovery.uk** and **cflab.uk**, mailbox attribution runs from the census to the corroborated actor: because "my mailbox sent it" is where the analysis starts, not where it ends.

§ 13 · COMMON QUESTIONS

# Frequently asked questions

### 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 assistant 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, endpoint artefacts show drafts and client activity (§8). The report states the missing spine and builds the lattice from the rest: and the organisation turns logging on for next time.

### The assistant sent it under standing instructions. Does attribution even matter?

It settles the facts so the law can do its work: once the assistant 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.

§ 14 · REFERENCE

# Glossary

**Delegated access**
One user's permission to work inside another's mailbox.

**Full-access permission**
The right to open and act in a mailbox as if the owner.

**Inbox rule**
A user- or delegate-created instruction that processes mail automatically.

**Logon type**
The audit log's record of owner, delegate or admin access.

**Mailbox audit log**
Exchange's per-mailbox record of actions and acting accounts.

**Permission census**
The recorded map of who held which mailbox rights, when.

**Send-as**
Sending in another's name with no visible trace of the actual sender.

**Send-on-behalf**
Sending in another's name with a visible "on behalf of" marker.

**Shared mailbox**
A mailbox with no user of its own, accessed by permitted members.

**Transport rule**
A tenant-level mail-flow rule set by administrators.

## Sources and authoritative references

The mailbox-attribution disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (mailbox attribution, rule and delegation forensics, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Identification and Phase 04 · Collection (permission censuses and shared-mailbox collection as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft Learn, mailbox auditing: learn.microsoft.com, mailbox auditing · Shared mailboxes: learn.microsoft.com, shared mailboxes · Google Workspace Admin Help, delegation and audit logs: support.google.com/a
- PD 57AD: justice.gov.uk, PD 57AD · CPR Part 31: justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- ICO, UK GDPR guidance (breach assessment for misdirected and forwarded mail): ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

# Working with Computer Forensics Lab

Mailbox work at **e-discovery.uk** opens with the permission census: shared mailboxes, delegations and send rights mapped with histories, so the sources a custodian list cannot see (Example 2's complaints@) enter the hold and the collection plan; delegated relationships are collected in all three layers; and rules, forwards and app permissions are exported as configuration evidence with their creation records. The laboratory side runs attribution to the corroborated actor: audit log, session, device and physical layer joined per guide 96's lattice, alternatives addressed: distinguishing the sanctioned delegate (Example 1), the compromised session (Example 3) and the disavowing owner, and reporting under CPR Part 35 where the sender is the case. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a disputed message is already in play, the mailbox audit log is on a retention clock: export it this week, before the argument about who sent it outlives the evidence that answers it.

INSTRUCT THE LAB

## Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace