

Postfix Recipient Tracing

One message, five confirmed mailbox deliveries

Investigation findings, evidence and technical explanation

The laboratory and its technologies	02
Visible headers and the SMTP envelope	03
Correlating the message with server logs	04
Delivery timeline and interpretation	05
Evidence, conclusion and references	06

Abdellah Bayar

SOC LAB PORTFOLIO

5 October 2026

The laboratory and its purpose

A controlled delivery experiment on a personal Ubuntu mail server.

Investigation question

Starting with Alice's received email, can the mail server records establish who else received the same message? The experiment compares visible recipients with the complete set of confirmed local deliveries.

Result: five mailboxes received the message. Three recipients appear in Alice's To and Cc headers; Carol and Vittorio are identified through the SMTP envelope and Postfix delivery records.

Technologies used

Technology	Role in the experiment
Windows Hyper-V	Hosts the SOC-Mail-Lab virtual machine: Generation 2, 4 GB RAM, 2 vCPUs and a 40 GB virtual disk.
Ubuntu Server 24.04.5 LTS	Runs the local mail service and stores the recipient mailboxes.
Postfix 3.8.6	Accepts the SMTP message, assigns a queue ID and delivers it to local users.
Swaks 20240103.0	Generates a benign message and records the SMTP exchange.
rsyslog and Maildir	Write server events to mail.log and store each received message as a file.
OpenSSH and SCP	Provide remote terminal access from Windows and export the evidence.

Postfix listens on loopback only, with lab.test configured for local delivery. The harmless plain-text message is submitted to 127.0.0.1:25 inside the VM. Internet access through Hyper-V's Default Switch is used for installation; the SMTP test remains local.

Headers are not the envelope

The message shown to a reader can contain fewer addresses than the delivery instructions.

SMTP uses RCPT TO commands to identify delivery recipients. The To and Cc fields are part of the message content. They do not provide a complete delivery list. [1, 2]

EXCERPT FROM ALICE'S RECEIVED COPY

To: alice@lab.test
Cc: bob@lab.test, edoardo@lab.test
From: labadmin@lab.test
Subject: [SOC-LAB] Recipient tracing test 02
Message-Id: <20261005091903.003053@soc-mail-lab>

Recipient	Visible header	SMTP envelope	Local delivery
alice@lab.test	To	Included	Confirmed
bob@lab.test	Cc	Included	Confirmed
carol@lab.test	Absent	Included	Confirmed
edoardo@lab.test	Cc	Included	Confirmed
vittorio@lab.test	Absent	Included	Confirmed

Why Carol and Vittorio are missing

The controlled setup supplied all five addresses to Swaks for SMTP delivery, while explicitly setting To to Alice and Cc to Bob and Edoardo. Carol and Vittorio received blind-copy-equivalent delivery; no Bcc header was included.

Interpretation limit:

recipient roles are known from this setup. In a production investigation, an address absent from To and Cc could also be reached through forwarding or a distribution list. Header absence alone does not establish Bcc delivery.

Correlating the evidence

Follow the identifier in the received message to the server's delivery records.

- 1 Start with the received copy.** Record the Message-ID and the Postfix queue ID in the Received header. Delivered-To identifies Alice's local delivery.
- 2 Find the cleanup record.** The Postfix cleanup event associates this Message-ID with queue 20B261E01F8.
- 3 Follow the queue.** Collect every record for this queue during the test and inspect each recipient's delivery status.

REFERENCE IDENTIFIERS

```
Message-ID: <20261005091903.003053@soc-mail-lab>  
Postfix queue: 20B261E01F8  
Envelope sender: labadmin@lab.test
```

RECEIVED HEADER AND SELECTED LOG FIELDS

```
Received: from soc-mail-lab (localhost [127.0.0.1])  
  by soc-mail-lab.mshome.net (Postfix)  
  with ESMTP id 20B261E01F8;  
  Mon, 5 Oct 2026 09:20:34 +0000 (UTC)  
  
postfix/cleanup: 20B261E01F8:  
  message-id=<20261005091903.003053@soc-mail-lab>  
postfix/qmgr: 20B261E01F8: nrcpt=5 (queue active)
```

The second block wraps the Received header and shortens log prefixes for readability. The original .eml file and the nine unedited queue records are included in the repository.

Two identifiers, two jobs

The Message-ID identifies the message in its headers. The queue ID identifies its processing on this Postfix server. Here, the cleanup record connects the two. A production search also needs the server and time window because a queue identifier is not a universal identifier across mail systems.

Delivery timeline

The reference message was submitted on 5 October 2026; all times below are UTC.

Delivered at	Recipient	Recorded outcome
09:20:34.148495	alice@lab.test	sent / delivered to maildir
09:20:34.150859	bob@lab.test	sent / delivered to maildir
09:20:34.152450	carol@lab.test	sent / delivered to maildir
09:20:34.153637	edoardo@lab.test	sent / delivered to maildir
09:20:34.153883	vittorio@lab.test	sent / delivered to maildir

Every recipient has a local delivery record with dsn=2.0.0 and status=sent (delivered to maildir). Together, these records confirm five successful mailbox deliveries in this run.

What the other records mean

Field or response	Meaning in this run
250 ... queued as 20B261E01F8	The SMTP server accepted the message into its queue. This response alone does not establish delivery to every mailbox.
nrcpt=5	The queue contains five envelope recipients. Individual delivery records establish their outcomes.
removed at 09:20:34.153914	Postfix finished processing this queue item. This is not deletion from the recipients' mailboxes.
Date: 09:19:03 / delivery: 09:20:34	The message was prepared first and transmitted later. The header Date is not the delivery timestamp.

Observed scope: five successful local deliveries. Opening, clicking, replying and account compromise were not measured. The test message contained no credential form, attachment or tracking URL.

Evidence and conclusion

The investigation is supported by native message files, an SMTP transcript and server logs.

Evidence file	Purpose	Bytes
soc-trace-alice-02.eml	Received copy from Alice's Maildir	587
soc-trace-message-02.eml	Prepared message before submission	349
soc-trace-smtp-02.txt	SMTP envelope and server responses	1180
soc-trace-delivery-02.log	Nine records for the reference queue	1436

The evidence exports are preserved byte for byte. Recipient-Tracing-Checksums.sha256 records their SHA-256 hashes, and .gitattributes disables line-ending conversion for the evidence files. Hashes allow later copies to be compared with these exports; they do not independently prove that a server record is true.

Investigation conclusion

Starting from Alice's received copy, the Message-ID was matched to Postfix queue 20B261E01F8. The corresponding records confirm delivery to Alice, Bob, Carol, Edoardo and Vittorio. This expands the observed recipient set from three visible addresses to five delivered addresses.

The experiment demonstrates a repeatable recipient-tracing method: inspect the message, correlate its identifiers, check each delivery outcome, and compare the results with the visible headers.

Practical boundary: this lab reconstructs delivery on one local server with five test accounts. Determining exposure in a real campaign requires access to the relevant mail logs and separate evidence of user interaction.

References

- [1] RFC 5321: SMTP - mail transactions and envelope recipients
- [2] RFC 5322: Internet Message Format - destination address fields
- [3] Ubuntu Server: Postfix - Maildir configuration and logs
- [4] Swaks reference - message generation and SMTP testing
- [5] Git attributes - preserving evidence line endings