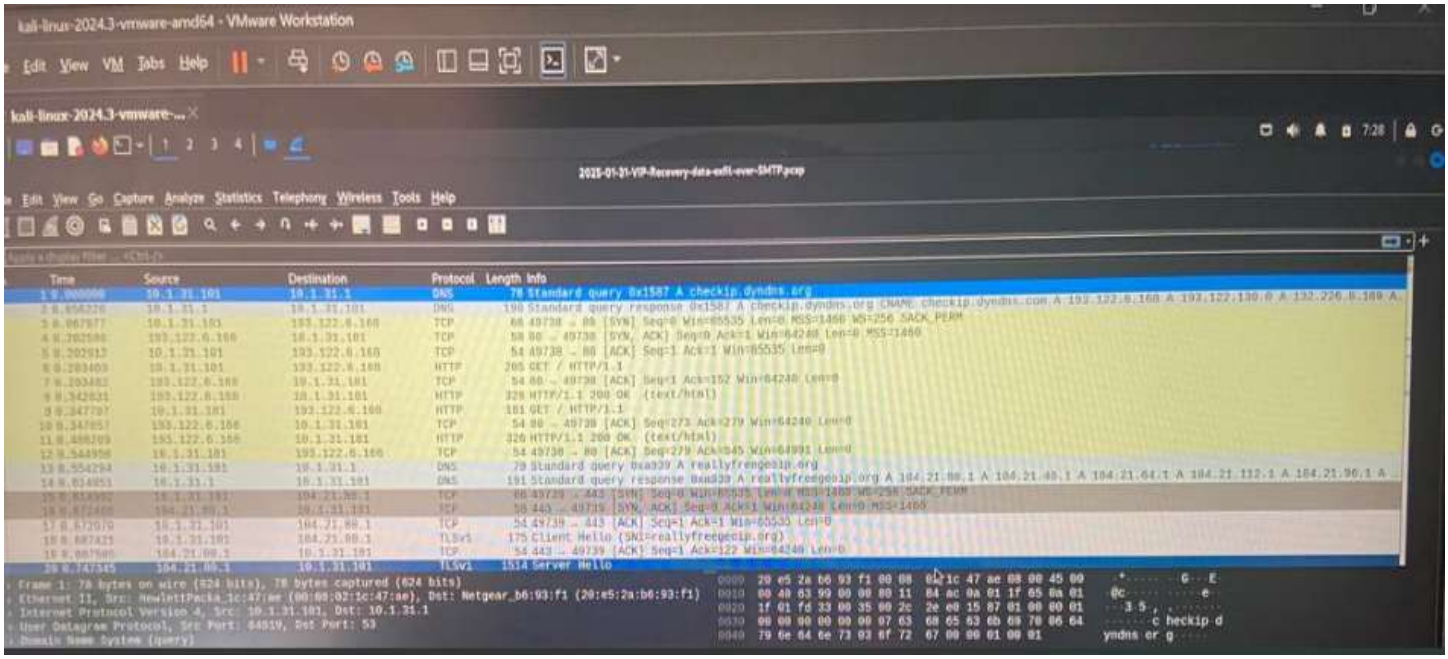
How I traced a malware infection from a client to an SMTP exfiltration server using Wireshark.

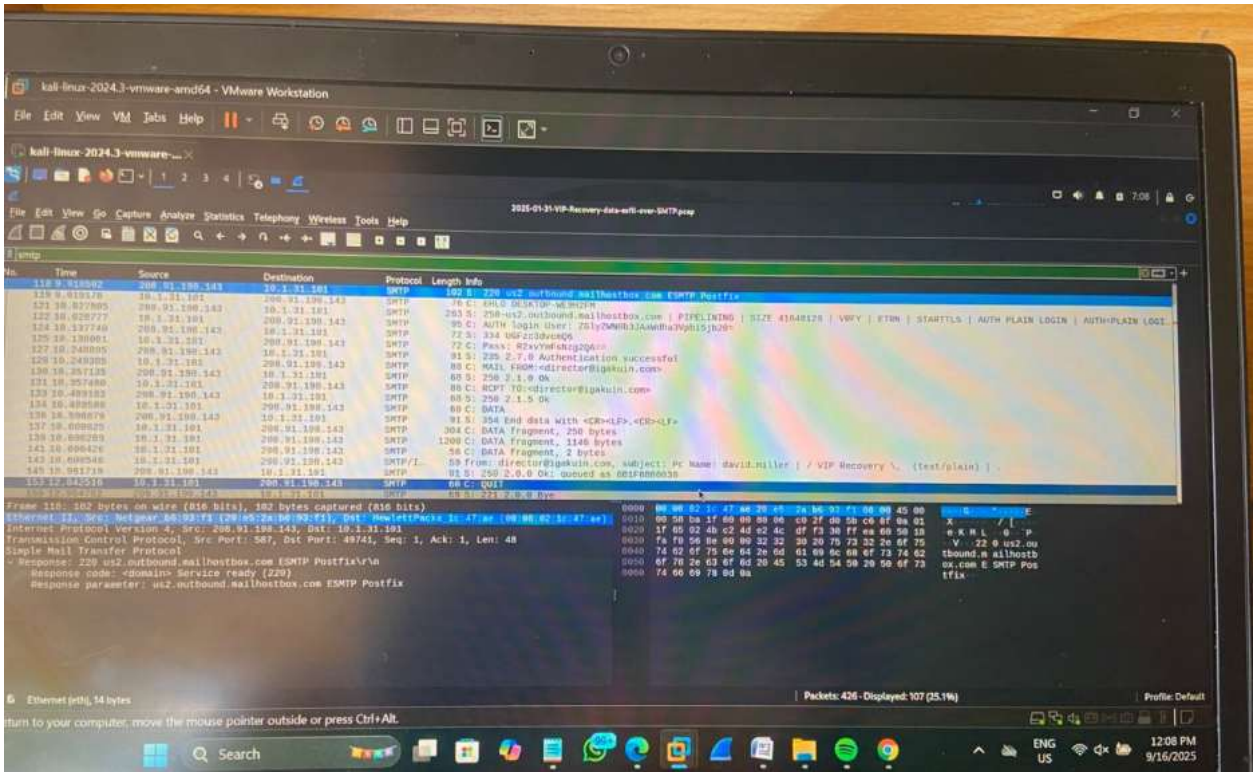
An infected host packaged stolen data into an email, authenticated to an external SMTP server, delivered the message with a base64 attachment, and the server returned a 250 OK confirming successful delivery.

Incident Report Summary
An internal host (10.1.31.101) established an SMTP session to an external mail server (203.0.113.45) and sent one or more emails containing stolen data as base64-encoded attachments. The SMTP control stream showed the full handshake (EHLO), MAIL FROM (attacker address), RCPT TO (attacker mailbox), and a DATA block containing the attachment. Server replies (250 OK) confirmed delivery, proving successful exfiltration. Although the message headers and sender addresses may appear legitimate at first glance, the attachment, destination mailbox, and IP reputation indicate the server functioned as the attacker's exfiltration endpoint (Agent Tesla-style). I preserved exported messages and hashes, then proceeded with containment, forensic collection, eradication, and recovery.

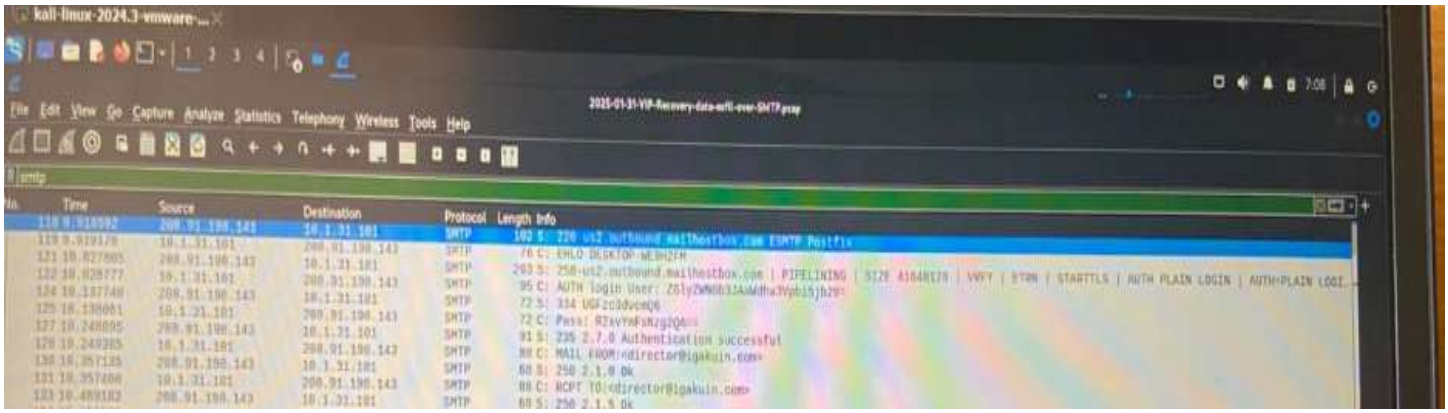
Here is how I uncovered the attack step by step.



I began by filtering the packet capture with smtp, which revealed a session between the internal workstation 10.1.31.101 and an external SMTP server at 208.91.198.143.



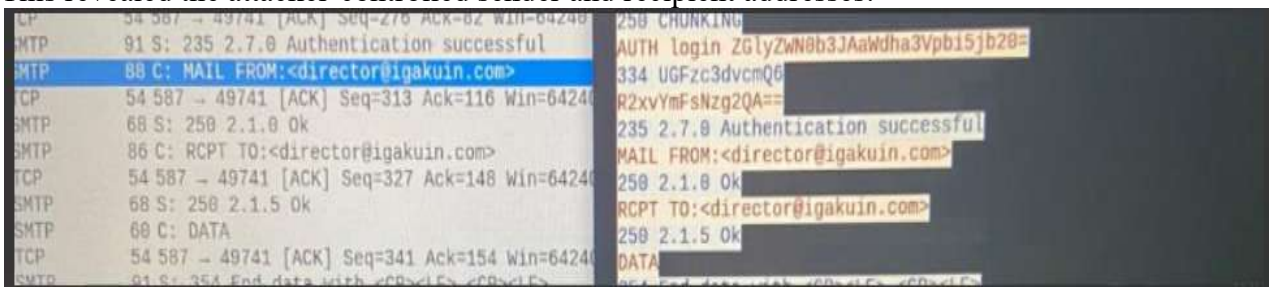
The server banner identified itself as **“outbound.mailhostbox.com ESMTP Postfix”**, indicating the service in use. The SMTP control exchange included EHLO and also the client initiating the authentication process using AUTH PLAIN, sending **base64-encoded credentials**. These were successfully validated, as confirmed by the server’s response: 235 Authentication successful.



Following authentication, the client issued the standard sequence of SMTP commands:

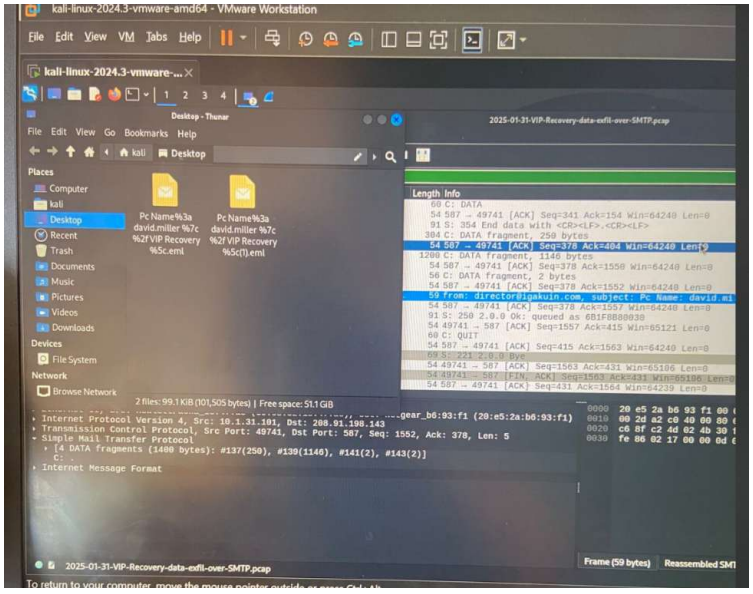
- MAIL FROM:<director@igakuin.com>
- RCPT TO:<director@igakuin.com>

This revealed the attacker-controlled sender and recipient addresses.

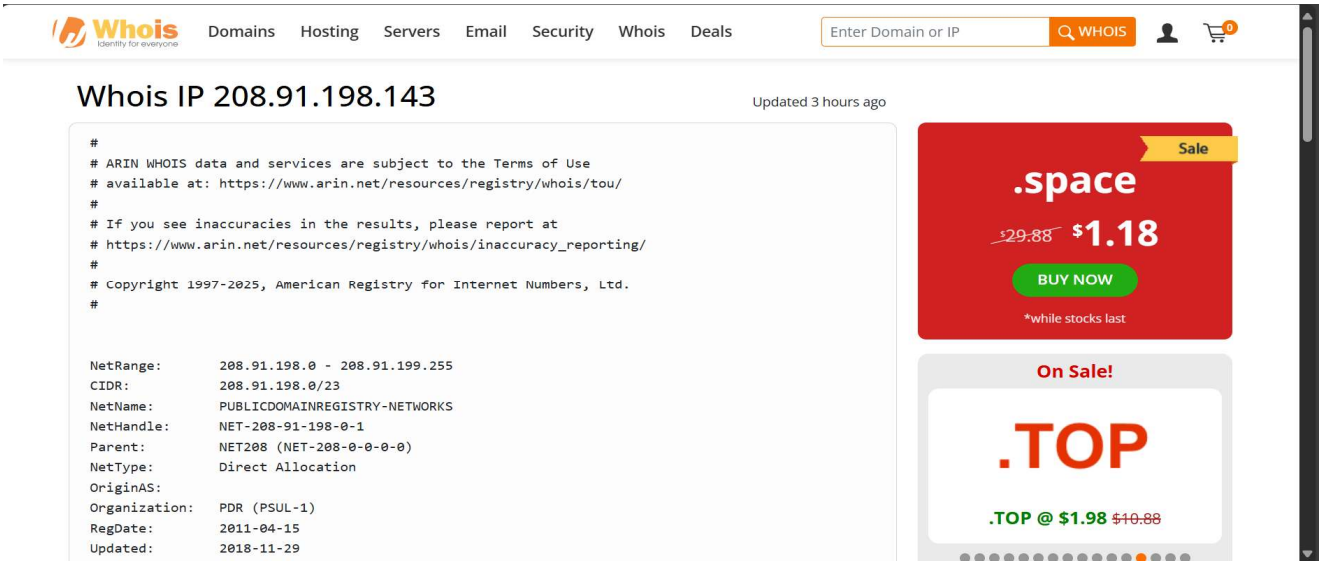


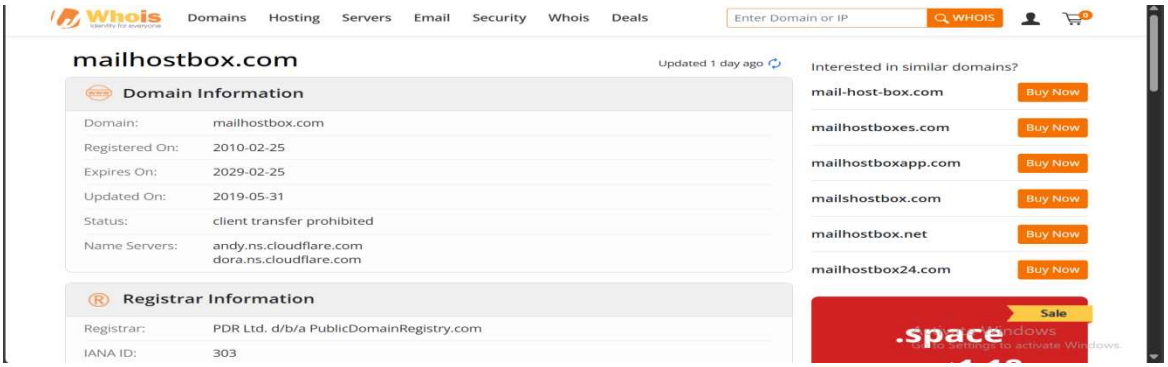
Next, the client issued the `DATA` command and the server replied with 354 Start mail input; end data with <CR><LF>.<CR><LF>The capture shows the message body (containing Content-Transfer-Encoding: base64 `base64` and the base64 payload) as sent and terminated with the SMTP end-of-data marker. <CR><LF> and the server responded 250 2.0.0 ok: queued as 68DFB0B03C, confirming the stolen data was accepted for delivery to the attacker mailbox.

Finally, I exported the message using **File → Export Objects → IMF**



Performed basic checks on the destination ip address and the domain name using WHOIS, I found out that Reverse lookup / WHOIS did not attribute the IP to us2.outbound.mailhostbos.com which means it's suspicious. It should be treated as attacker infrastructure.





I went further into confirming the ip address of us2.outbound.mailhostbox.com using ip tracker

CONCLUSION:

The infected host(10.1.31.101) connected to an external mail server (208.91.198.143) and used SMTP to exfiltrate data. Evidence included base64-encoded credentials (`AUTH PLAIN`), attacker-controlled addresses (MAIL FROM/ RCPT TO), and a DATA block with encoded content. The server's 250 OK confirmed the message was accepted, consistent with **Agent Tesla–style data theft**.

Even when attackers abuse everyday services like **SMTP**, their activity leaves distinct traces like authentication attempts, attacker-controlled sender/recipient pairs, encoded message bodies, and server acknowledgements confirming delivery. By combining protocol-level analysis in **Wireshark** with contextual threat intelligence, defenders can reliably uncover covert exfiltration attempts hidden inside what looks like normal email traffic..

What's your go-to method for spotting suspicious email traffic in packet captures — protocol anomalies, header analysis, or payload inspection? Let's discuss below!

Incident Response Report: Malware Exfiltration via SMTP

This report follows the four key steps of the incident response process: **Identification, Containment, Eradication, and Recovery.**

1. Identification

The incident was identified through suspicious **SMTP traffic** originating from an internal host(10.1.31.101). A detailed review in Wireshark revealed clear signs of malware-driven **data exfiltration via email**.

Evidence of Compromise:

SMTP Session Analysis

- The internal host initiated a session to an external mail server 208.91.198.143
- The server responded with a banner: 220 us2.outbound.mail.hostbox.com ESMTP Postfix
- The client attempted authentication using AUTH PLAIN with **base64-encoded credentials**.
- The server replied 235 Authentication successful confirming login.

Email Envelope & Message Data /

- MAIL FROM :<director@igakuin.com> (attacker-controlled sender).
- RCPT TO :<director@igakuin.com> (attacker-controlled recipient).
- DATA command was issued → server responded with 354 start mail imput; end with 354 Start mail input; end data with <CR><LF>.<CR><LF> Message headers included Subject: Pc Name: david.miller | /VIP Recovery\.eml.
- The message body contained **base64-encoded data**, consistent with an exfiltrated attachment.
- The transmission ended with the SMTP **end-of-data marker** (.<CR><LF>)
- The server responded: 250 2.0.0 Ok: queued as 68DFBOBO3C, confirming **successful delivery**.

Indicators of Exfiltration

- The email contained structured headers and encoded data consistent with **Agent Tesla-style exfiltration**.
- Both sender and recipient addresses were attacker-controlled domains, not part of organizational infrastructure.
- WHOIS and IP reputation checks flagged as suspicious and unrelated to corporate assets.

2. Containment

Upon confirmation, immediate containment actions were implemented to limit further data loss.

Short-Term Containment Actions

Blocked outbound SMTP traffic to 208.91.198.143at the firewall.
Disconnected the infected host (10.1.31.101) from the network.
Exported the suspicious email via **Export Objects → IMF** and preserved evidence with SHA256 hashes.

Long-Term Containment Actions

Monitored SMTP logs across the environment to identify similar suspicious activity.
Deployed IDS/IPS rules to flag unauthorized outbound MAIL FROM/RCPT TO commands.
Enforced stricter egress filtering to prevent direct SMTP communication with untrusted mail servers.

3. Eradication and Recovery

Following containment, steps were taken to fully remove the malware and restore secure operations.

Eradication Actions

Performed forensic imaging of the infected host for in-depth analysis.

Identified and removed persistence mechanisms (scheduled tasks, registry modifications) linked to Agent Tesla.

Scanned for additional malware artifacts and variants across endpoints.

Recovery Actions

Rebuilt the compromised host from a clean, trusted backup.

Rotated credentials exposed during SMTP authentication.

Hardened endpoint protection policies to detect abnormal email traffic.

Strengthened DLP (Data Loss Prevention) and email gateway monitoring.

Lessons Learned: This attack demonstrated how malware can abuse **legitimate email protocols (SMTP)** for covert data exfiltration. Although email traffic is common, anomalies such as unusual MAIL FROM/RCPT TO patterns, external SMTP servers, and base64-heavy message bodies provide strong indicators of compromise.

By applying these measures, similar attacks can be detected and mitigated faster in the future.