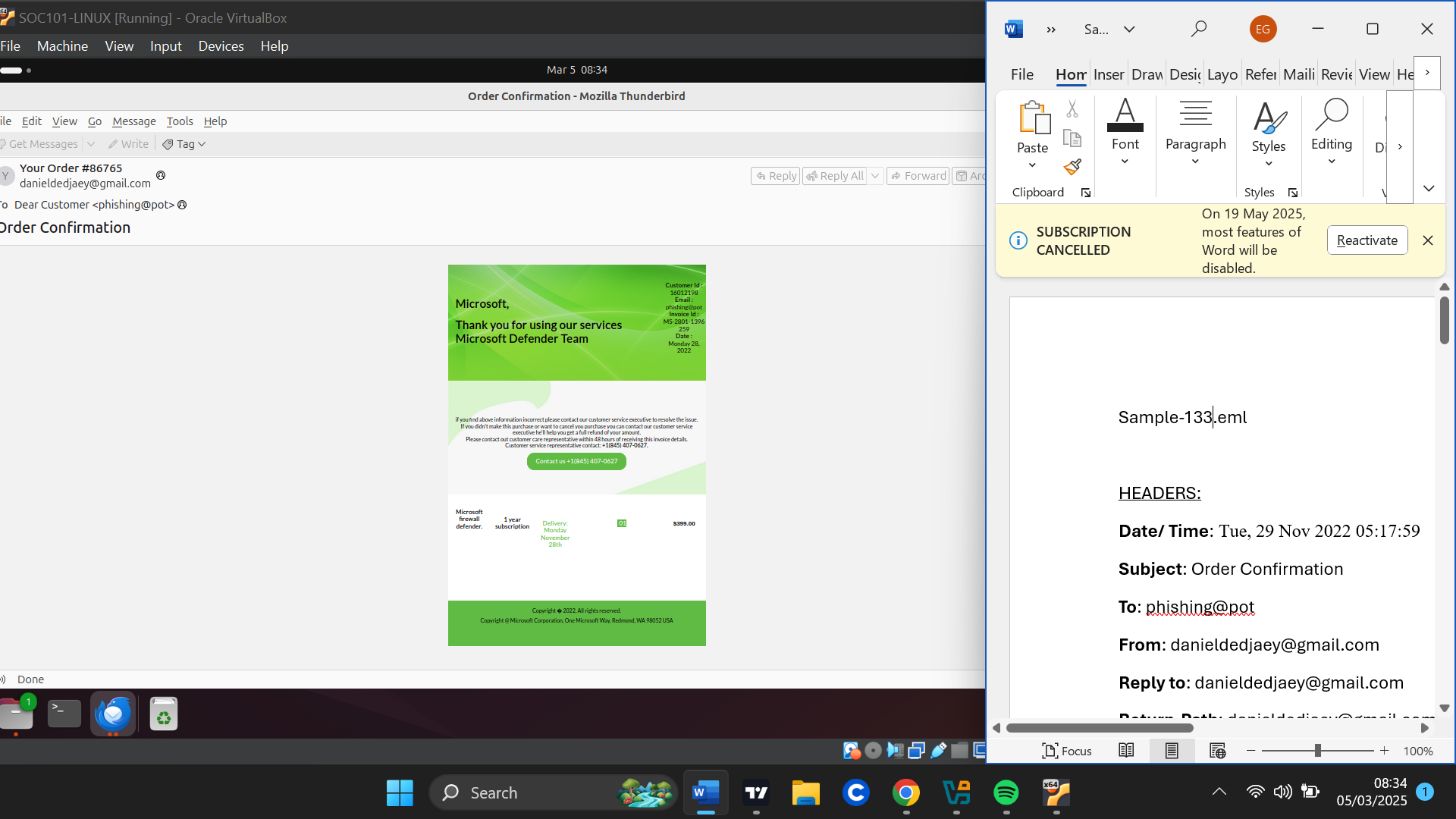
Sample-133.eml



HEADERS:

**Date/ Time**: Tue, 29 Nov 2022 05:17:59

**Subject**: Order Confirmation

**To**: phishing@pot

**From**: danieldedjaey@gmail.com

**Reply to**: danieldedjaey@gmail.com

|  |  |
| --- | --- |
|  |  |

**Return-Path**: danieldedjaey@gmail.com

**Sender IP**: 209.85.221.48

**Resolved host**: mail-wr1-f48.google.com

**Message – ID:** <054c1c77-44894-0ee72214940278@desktop-k6m8mnh>

URLS

-www.example[.]com

ATTACHMENTS

-

EMAIL DESCRIPTION

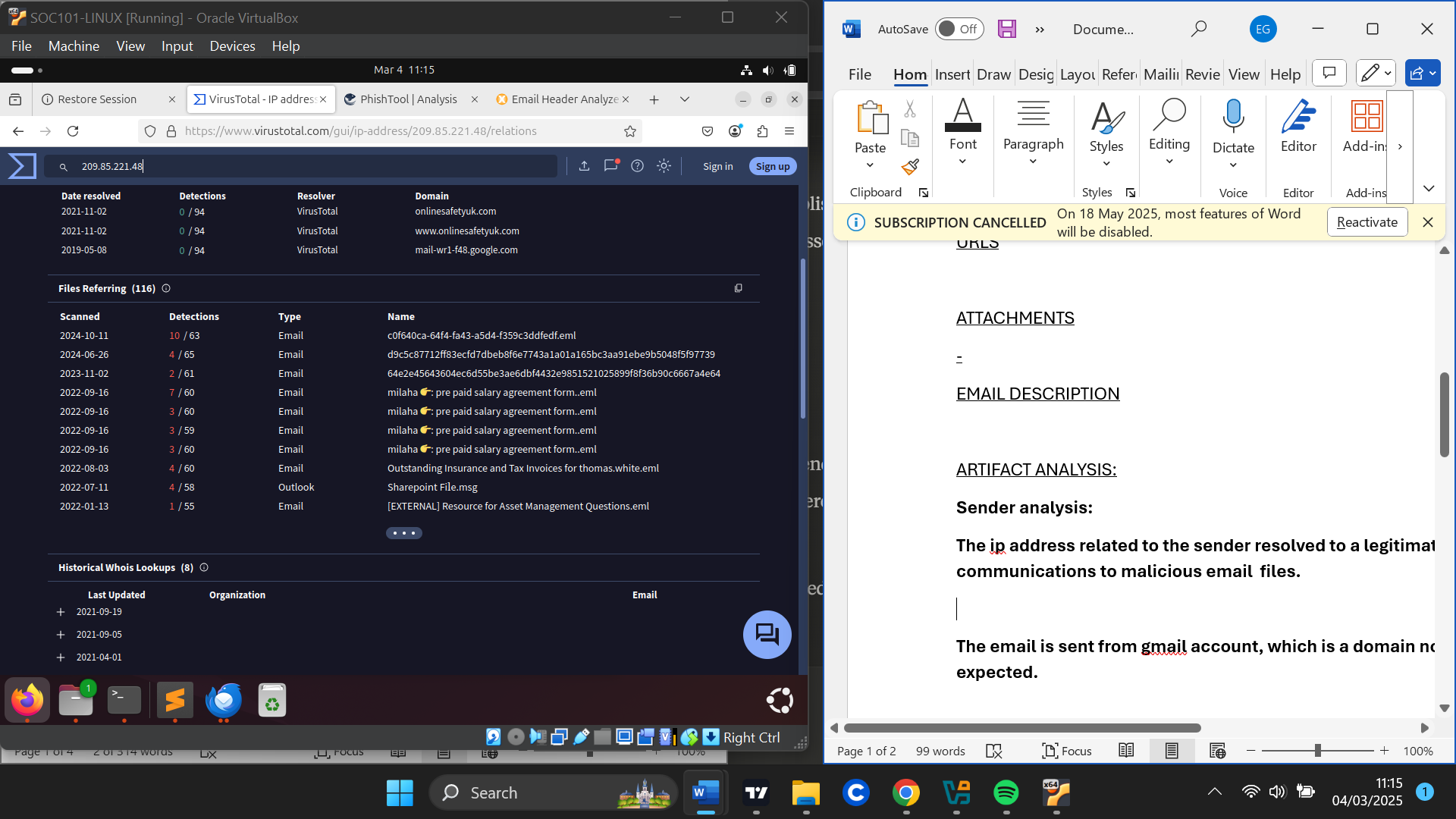
The email appears to be an order confirmation for Microsoft Firewall Defender on Monday 28th November,2002 for $399.0. It has an invoice ID for the purchase and directs the recipient to contact the customer Service Executive if any details are incorrect, if the recipient did no make this purchase or would want to cancel the purchase.

There is a “contact us” button where the recipient is supposed to click to reach the Customer Service Executive.

ARTIFACT ANALYSIS:

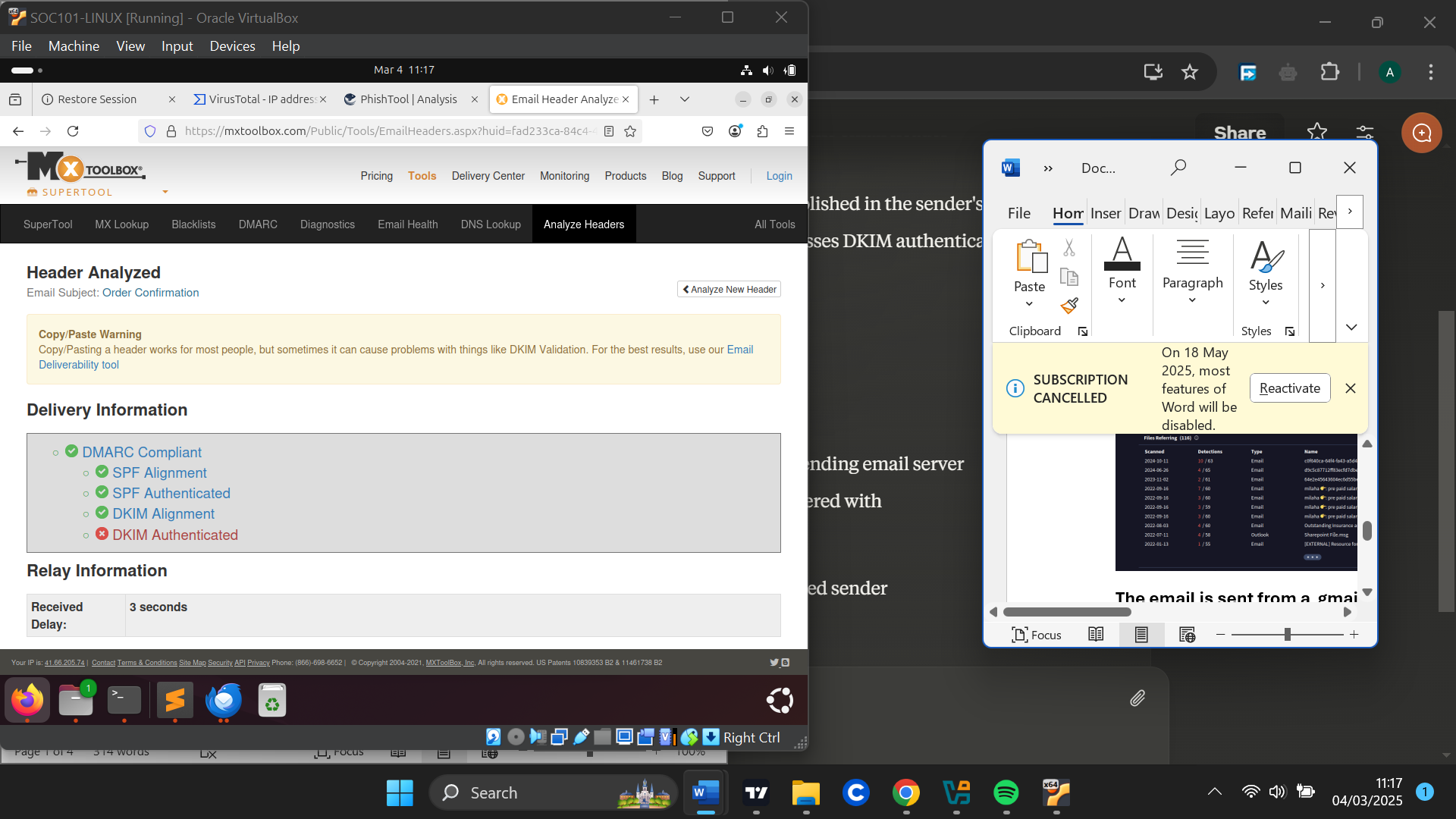
**Sender analysis:**

The IP address related to the sender resolved to a legitimate google server but has had communications with malicious email files or had malicious email files which referred this IP address.



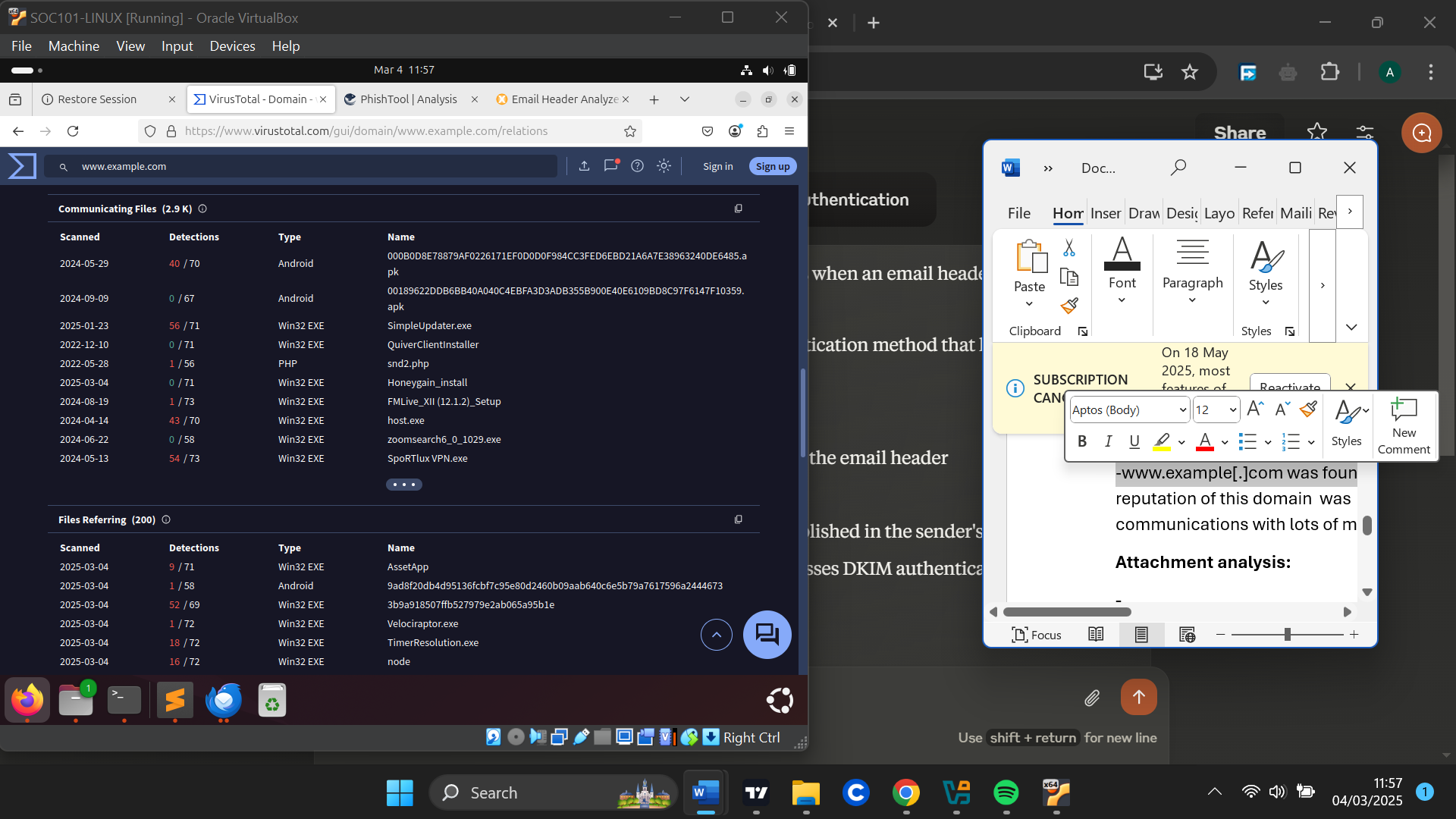
The email is sent from a gmail account which is not related to Microsoft as expected.

The email header failed DKIM email authentication method suggesting the email could have been spoofed.



**URL analysis:**

-www.example[.]com was found embedded in the email and extracted . When the reputation of this domain was checked, it was found to be legitimate but had communications with lots of malicious files.



**Attachment analysis:**

**-**

VERDICT

Due to the Ip address of the sender, although being legitimate, had communications with malicious files making it suspicious . The email header also failed DKIM authentication methods . The email had no relations to Microsoft but rather a personal google mail address and the link embedded in the email was found to be suspicious.

It is safe to say this was a phishing email .

DEFENSE ACTIONS

I blocked the personal email address (danieldedjaey@gmail.com) from sending any emails I Configured email filters to quarantine emails from the senders IP address.