Sample 188.eml

HEADERS:

**Date/ Time**: 08:57 am, Dec 26th 2022

**Subject**: Bitcoin.Transaction.0.7495.BTC

**To**: addedbad@gmail.com

**From**: dorothyleejux3@gmail.com

**Reply to**: -

**Return-Path**: dorothyleejux3@gmail.com

**Sender IP**: 209.85.128.170

**Resolved host**: mail-yw1-f170.google.com

**Message – ID: CANuHTRXFOT8K7kFdvBTavaCc7ecZa=SWyVURfjnHaSzBQ0p3qQ@mail.gmail.com**

URLS

-

ATTACHMENTS

**Attachment name**: GO.Get.Bitcoin.0.7495.BTCwkS9HOxBaj6TeHJUKYMScs24gJigILcOkRvO.pdf

**MD5**: a5d70896b806e92178be8052b8c58dab

**SHA1**: c9bc2d669272e32e8e6d448f797ccb17c9b296a8

**SHA256**: f15eb09e6ae033eba03bbd7cc8044383cb66b392f93c85ec8dc1bd023d4aa460

EMAIL DESCRIPTION

The email appears to be notifying the recipient of a bitcoin transaction stating that the main thing to do now is to withdraw an amount of $11736 .

The email also has a file attachment

ARTIFACT ANALYSIS

I run the eioc.py script to give an overview of what the email contains and its headers.

A screenshot of a computer

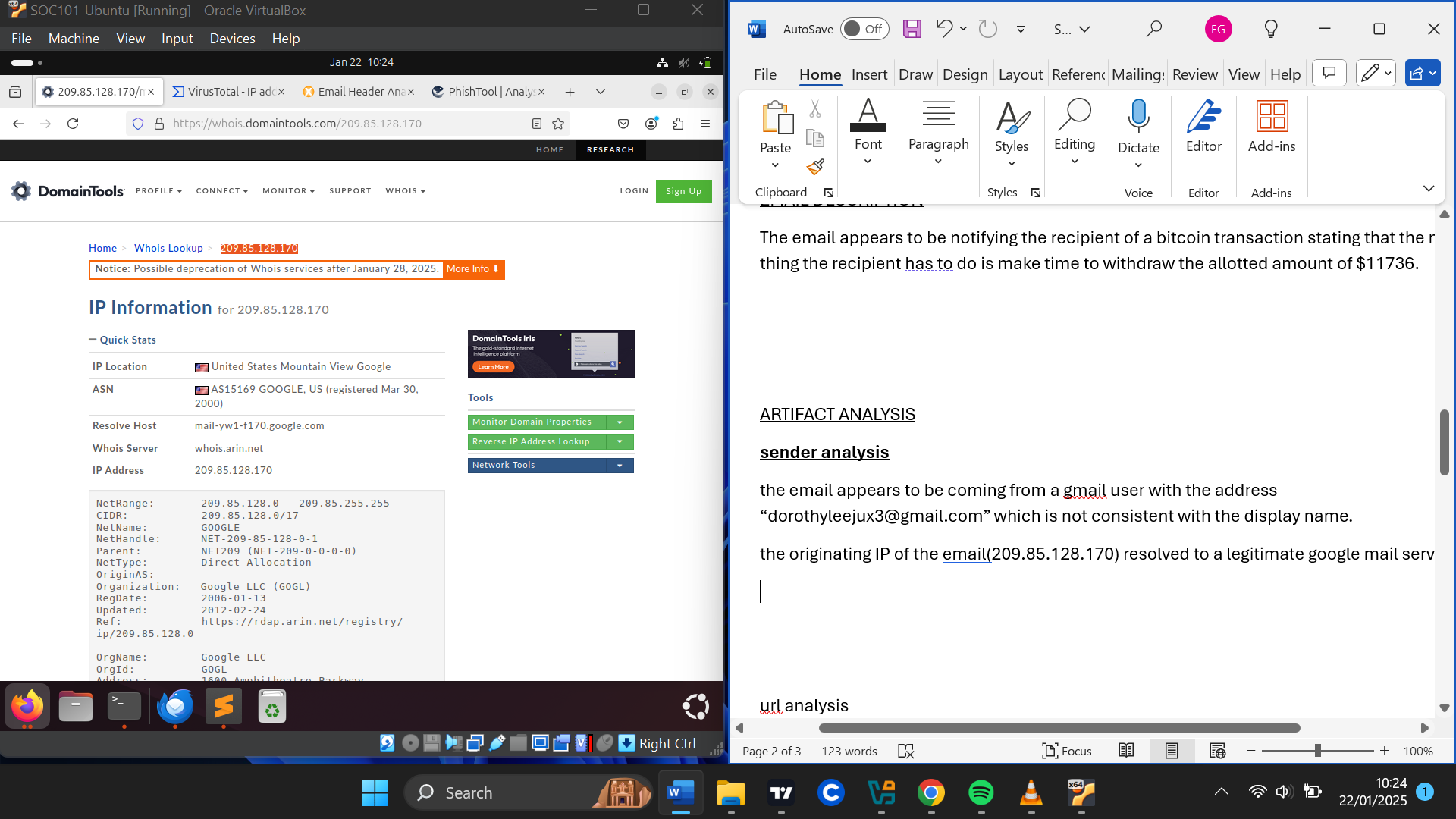
AI-generated content may be incorrect.

And confirmed these details with the results from Phishtool.com when I submitted the email for automated email phishing analysis.

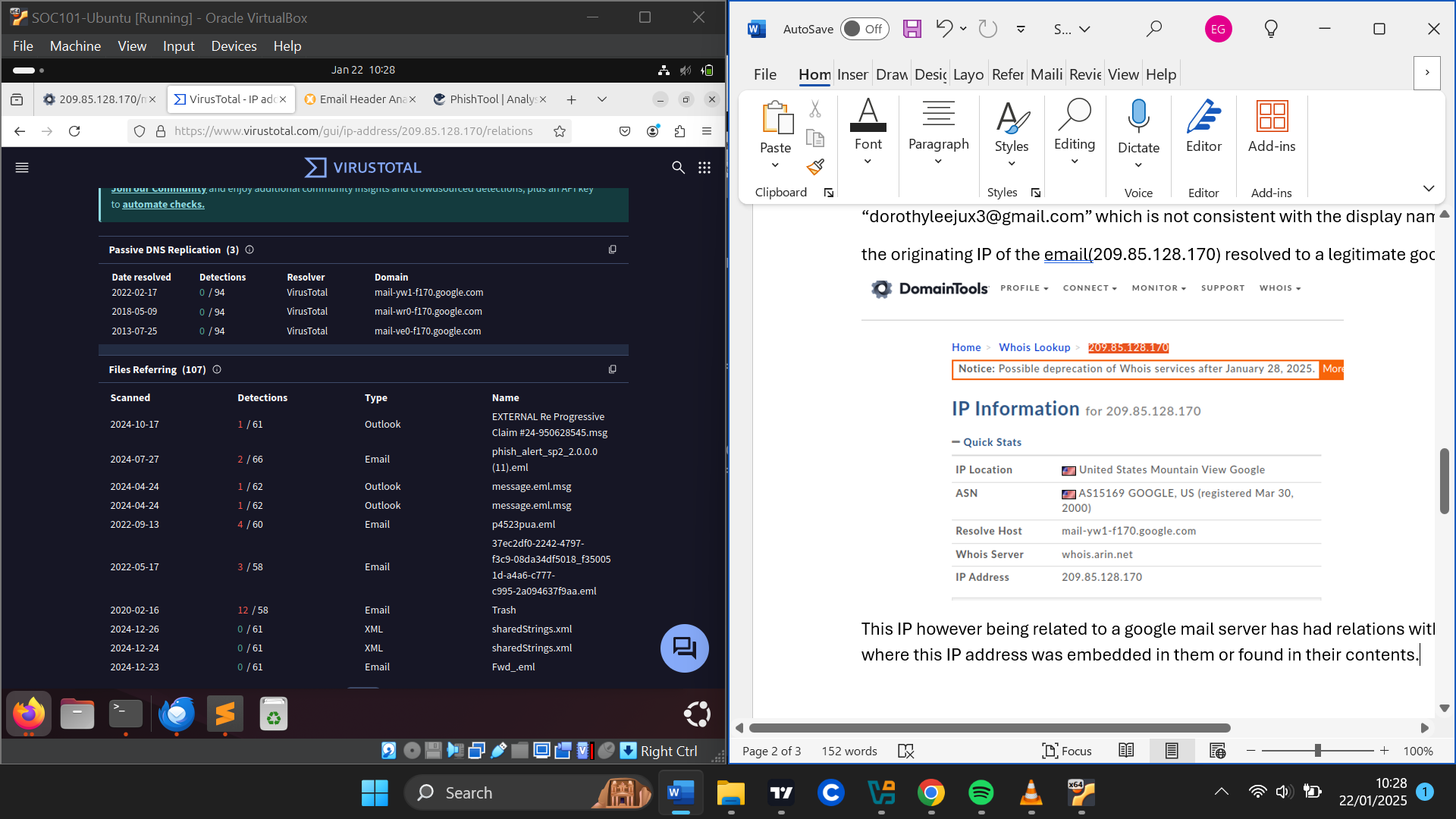
**sender analysis:**

the email appears to be coming from a gmail user with the address “dorothyleejux3@gmail.com” which is not consistent with the display name and not affiliated with any bitcoin company as expected.

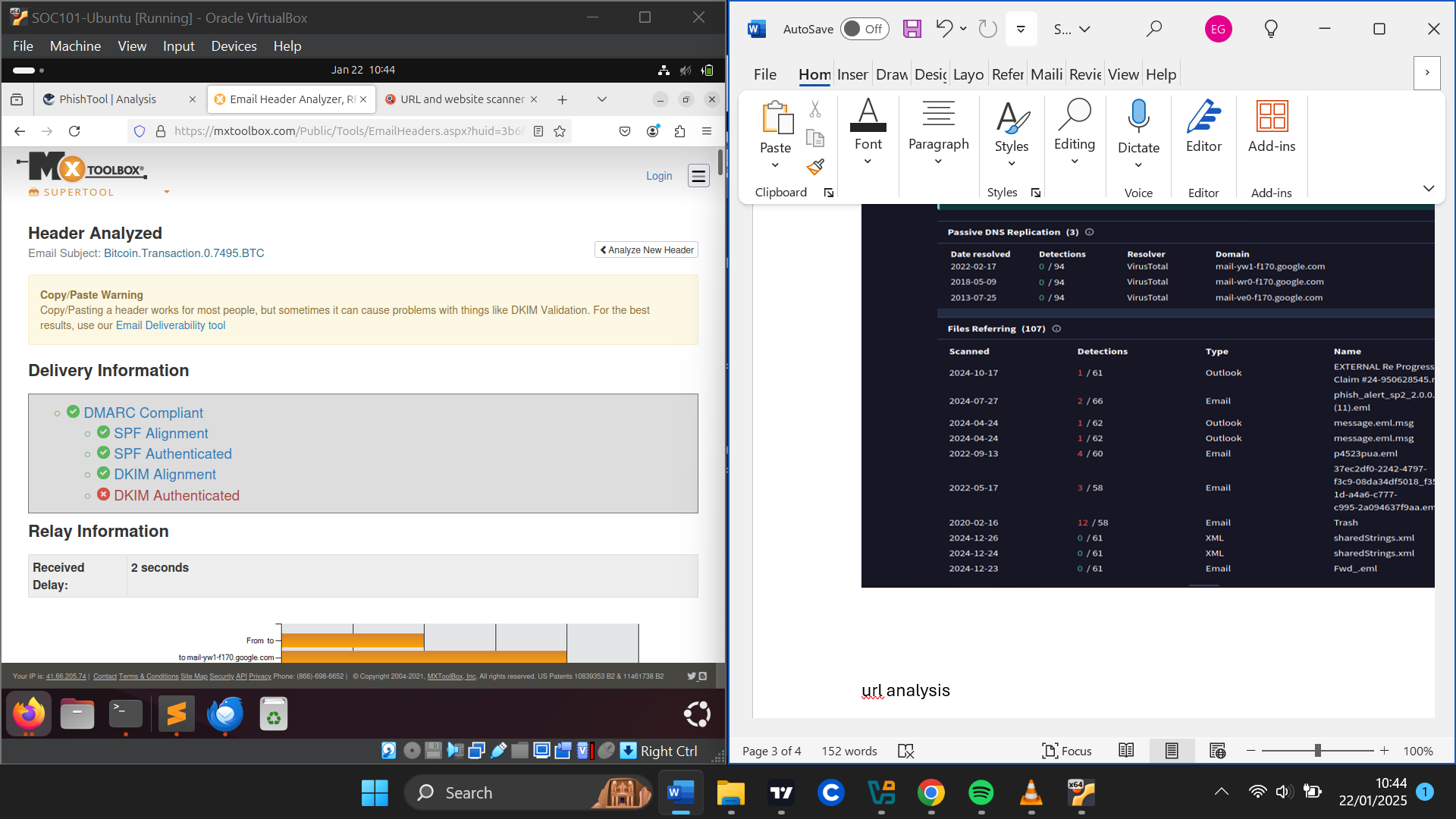
the originating IP of the email (209.85.128.170) resolved to a legitimate google mail server.



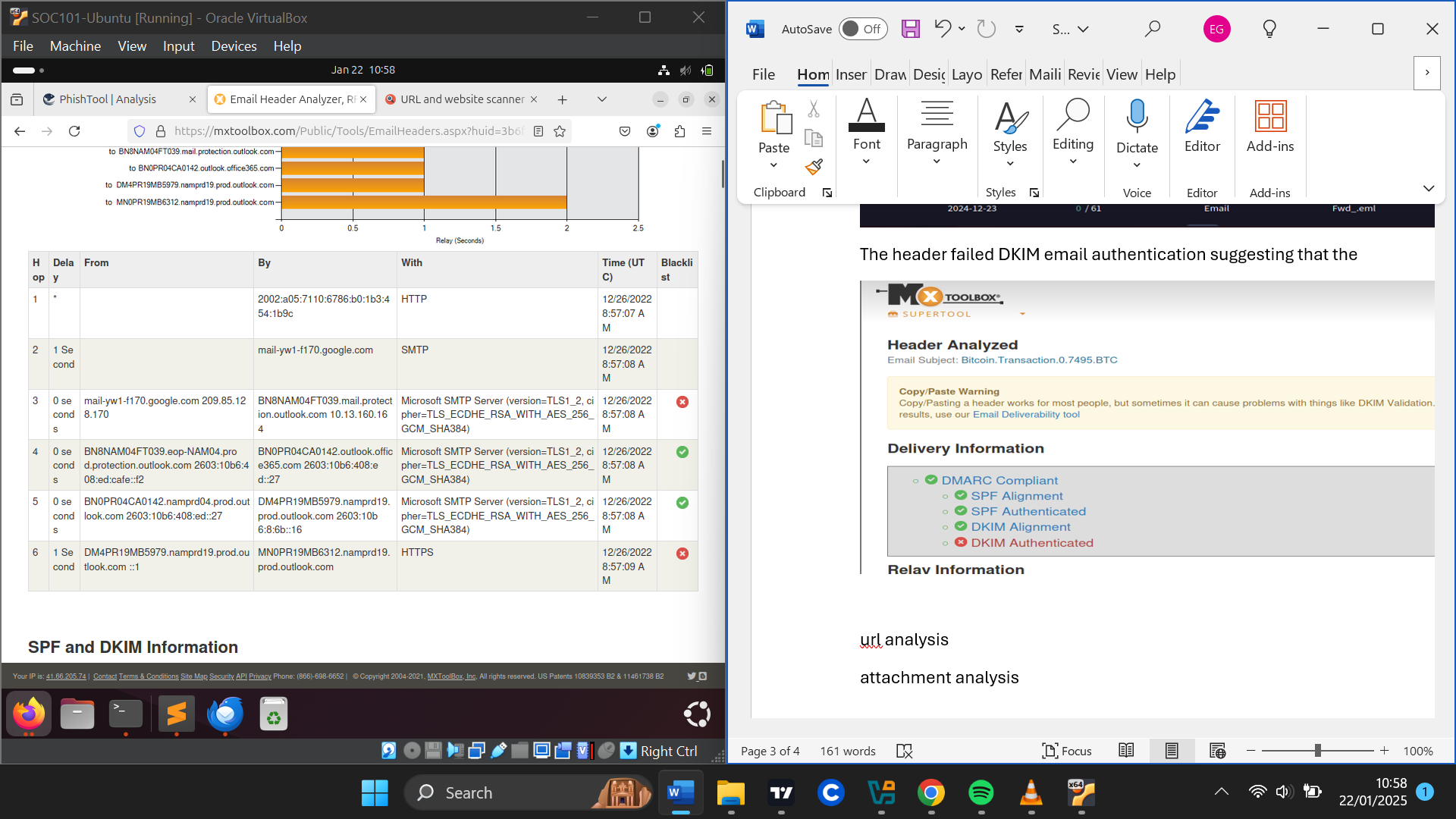
This IP address however being related to a google mail server has had relations with malicious files where the IP address was embedded in them or found in their contents.



The header failed DKIM email authentication suggesting that the email content has been tampered with during transit.



The senders’ Ip address also appeared to be blacklisted indicating it to be suspicious or malicious



**URL analysis**

-

**Attachment analysis**

A screenshot of a computer

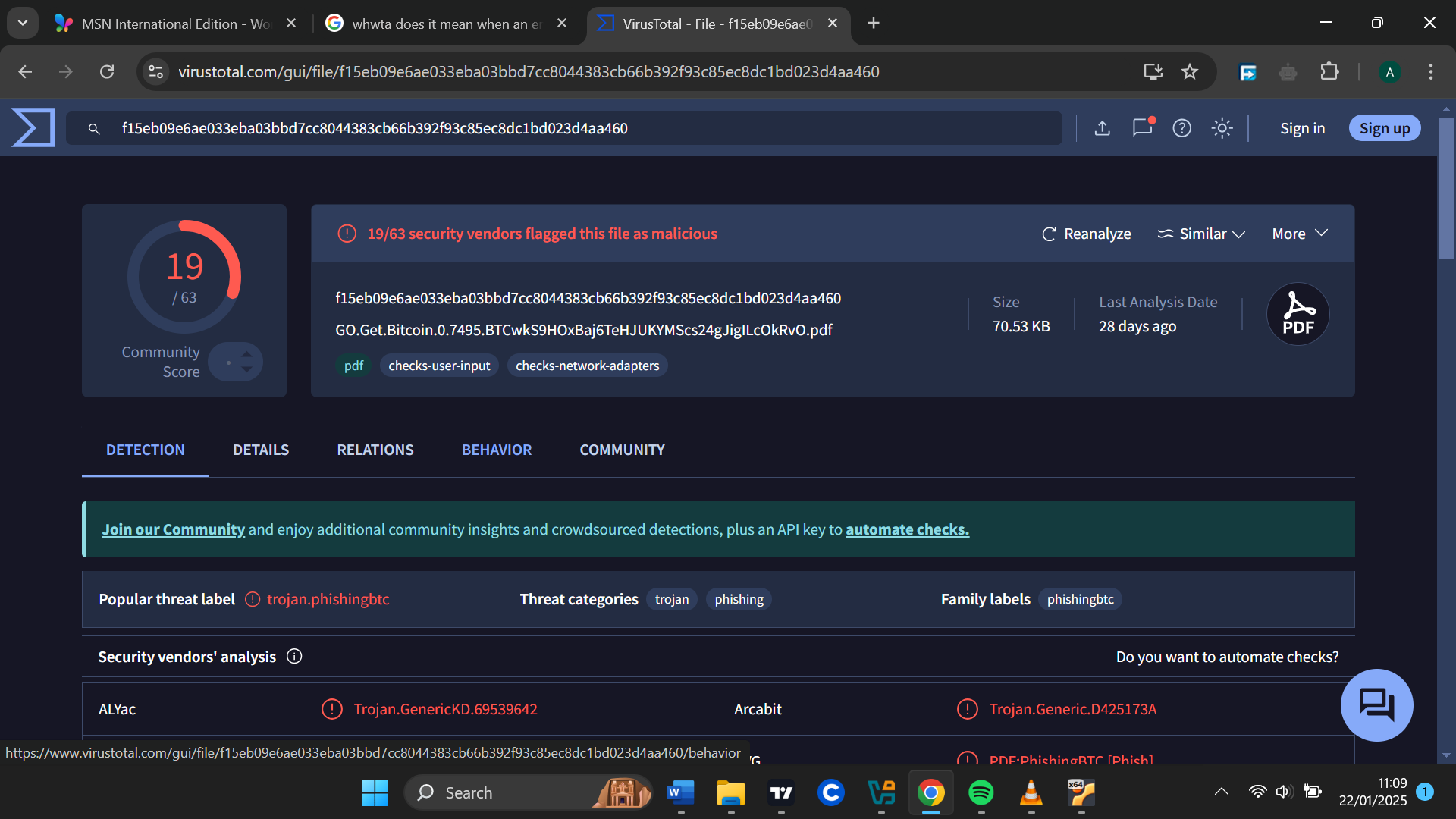
Description automatically generated

The email contained a pdf file “GO.Get.Bitcoin.0.7495.BTCwkS9HOxBaj6TeHJUKYMScs24gJigILcOkRvO.pdf”.

It claims that there has been an amount of 0.7495.BTC that has accumulated into the user’s account.

There is some sort of indication of urgency stating that the main thing the recipient has to do is make time to withdraw the allotted amount of $11736 else the account will be blocked in about two days from when the email was sent.

After running the file hash in virustotal, the file appeared to be malicious with 19 vendors flagging it as malicious.

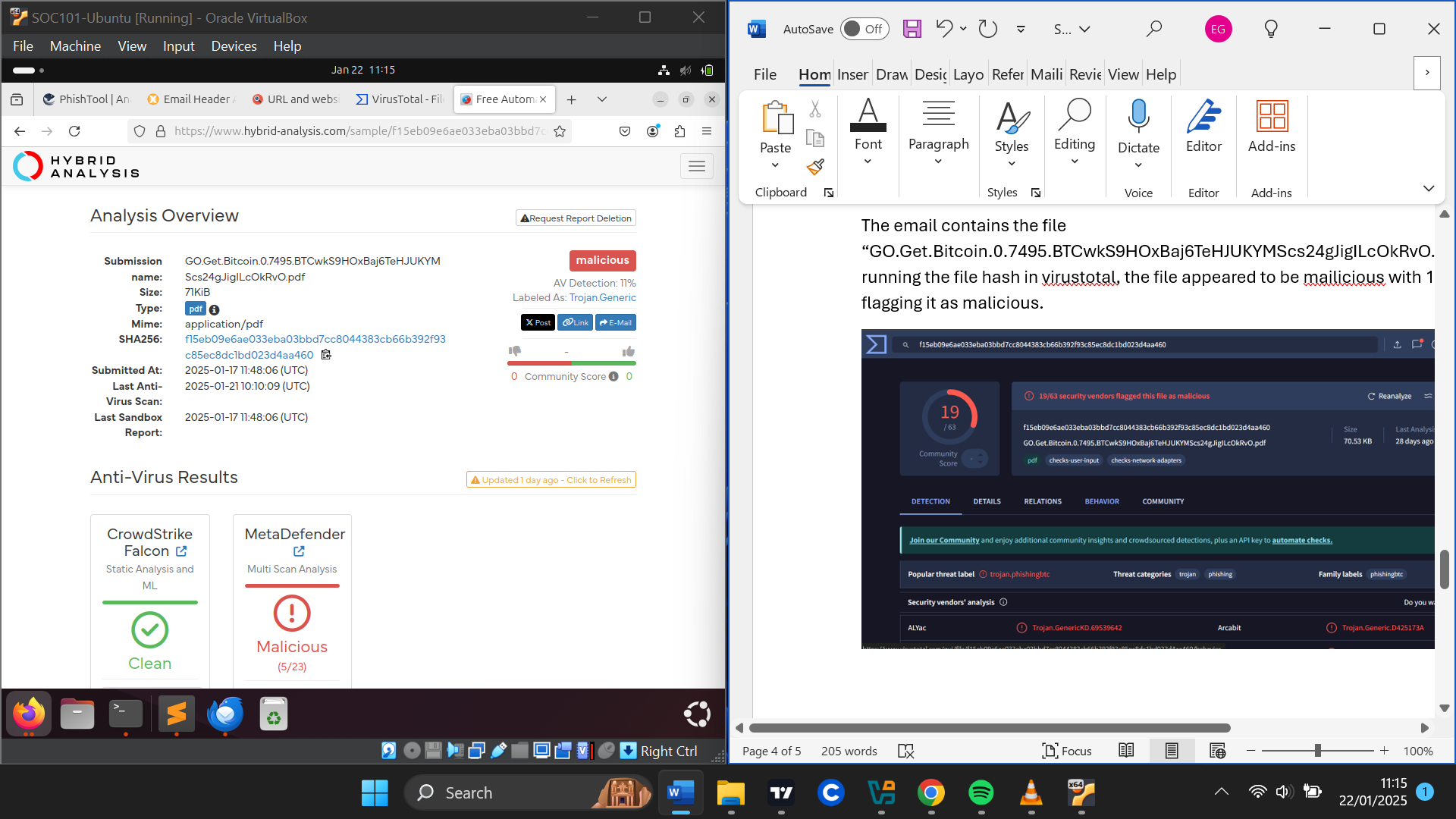


The pdf appeared to contain an embedded URL (“hxxps[://]bit[.]ly/3v0Vpm2”) when we ran our pdf-parser.py on the file.

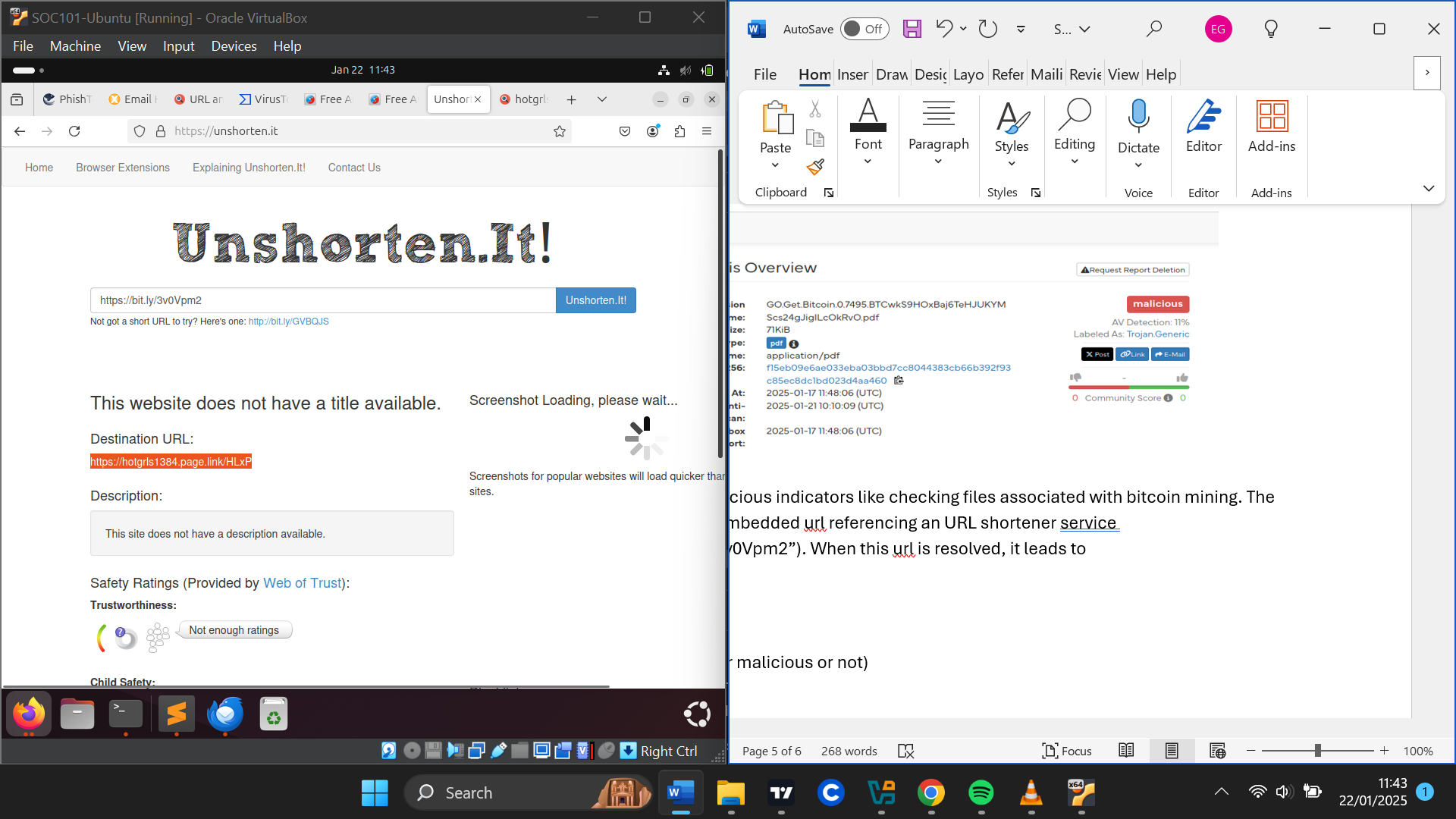
A screenshot of a computer

AI-generated content may be incorrect.

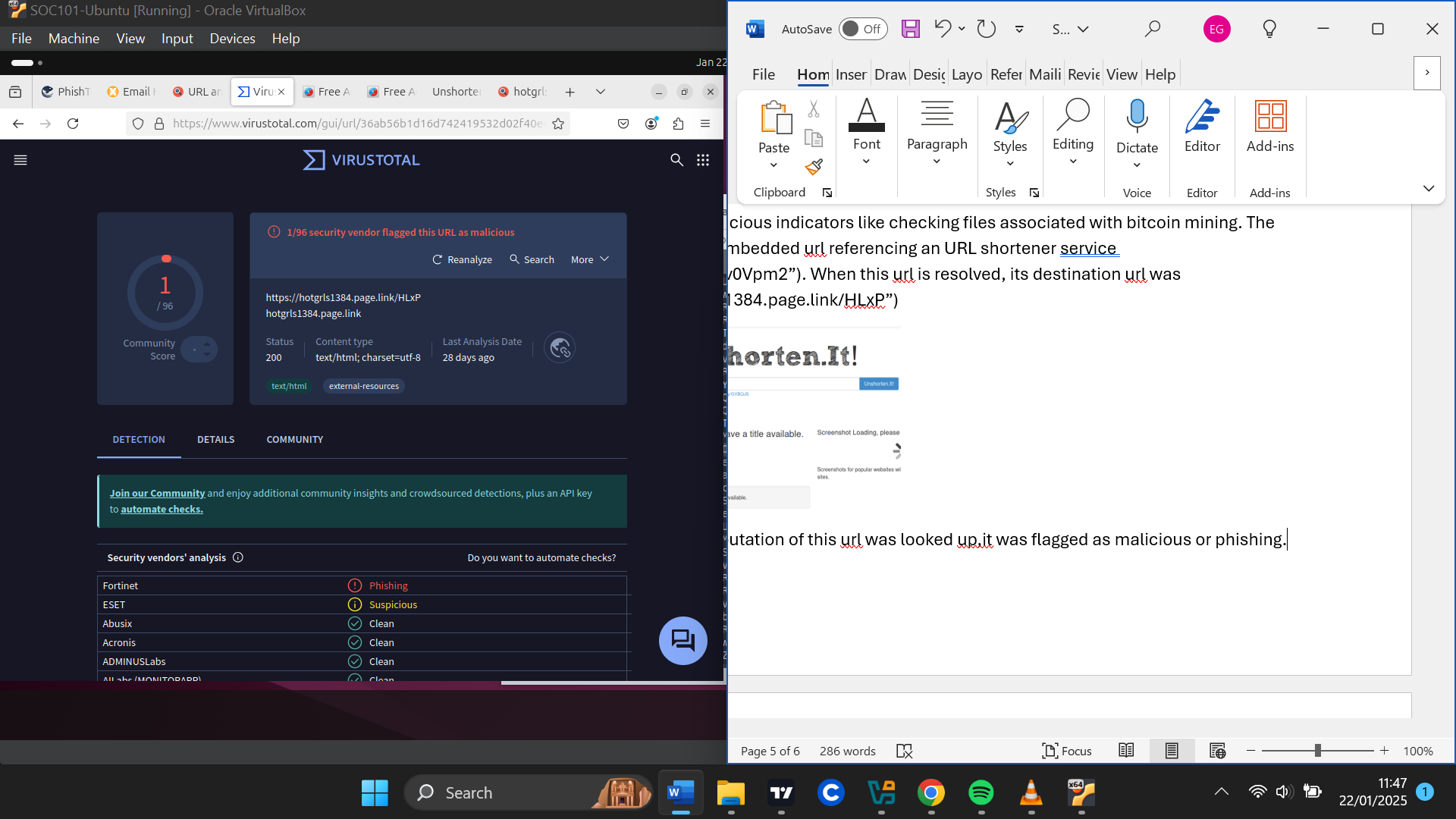
Hybrid analysis also confirms this pdf to be malicious and categorizes it as a trojan



The pdf had suspicious indicators like checking files associated with bitcoin mining. The pdf also had an embedded URL referencing a URL shortener service (“hxxps[://]bit[.]ly/3v0Vpm2”) When this URL was resolved, its destination URL was (“hxxps[://]hotgirls1384[.]page[.]link/HLxP”)



And when the reputation of the destination URL was looked up, it was flagged as malicious or phishing. This showed the attacker leveraged the use of URL shortening to disguise this malicious URL.



VERDICT

Due to the sender Ip address being suspicious even though related to google and failing DKIM authentication tests which is an indication of spoofing.

Additionally, after analyzing the pdf attachment file it was flagged as malicious(trojan) and the embedded URL in the pdf file was also flagged as malicious (phishing).

As a result, this email has been determined as malicious.

DEFENSE ACTIONS

To prevent the email sender from sender further mails, I have blocked the email sender “dorothyleejux3@gmail.com” on the email gateway.

I have also blocked any email originating from the suspicious sender IP address since it has relations with malicious domains.

To ensure users never visit the malicious URL embedded in the pdf, I have blocked the URL (“hxxps[://]hotgirls1384[.]page[.]link/HLxP”)