**Task 2 [Elevate labs]**

## Analyze a Phishing Email Sample

**Aim:**

To develop awareness of phishing tactics and gain practical skills in identifying, analyzing, and evaluating suspicious emails.

**Tools Used:**

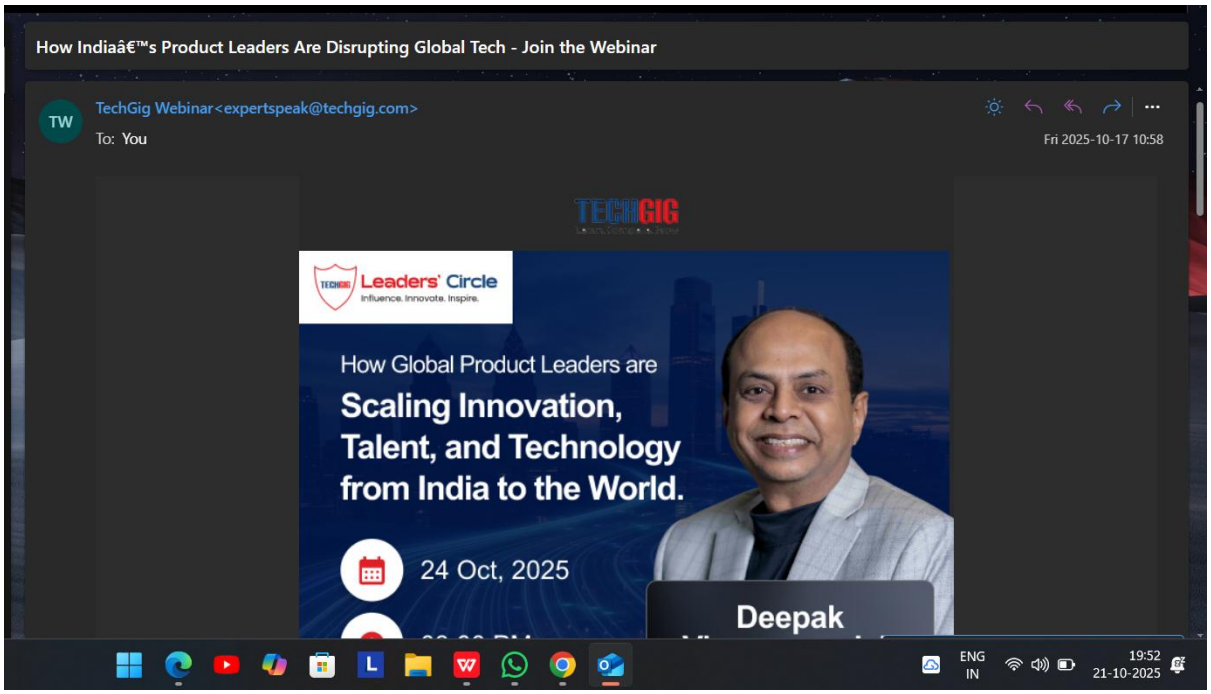
1Email Client – to view and copy raw email headers (Gmail, Outlook, etc.)

2.VirusTotal – to safely scan URLs and attachments

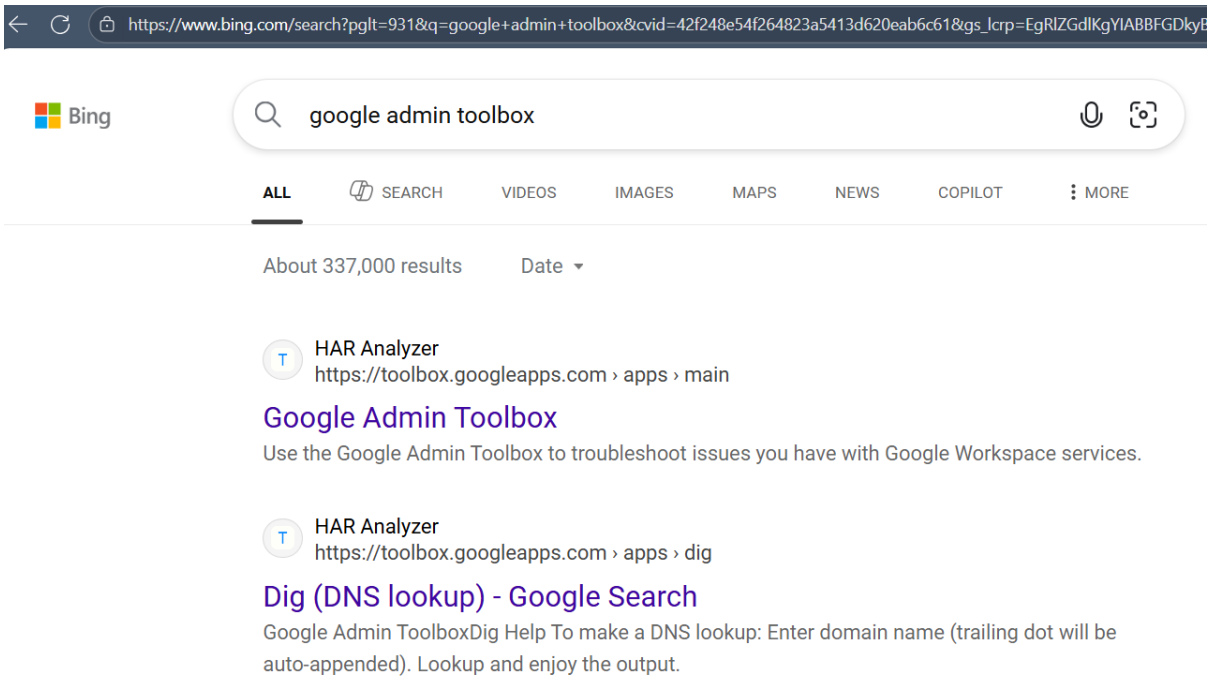
3.URLScan.io – to inspect suspicious links in a sandboxed environment

4.Text Editor / Spreadsheet – to document findings, phishing traits, and URLs

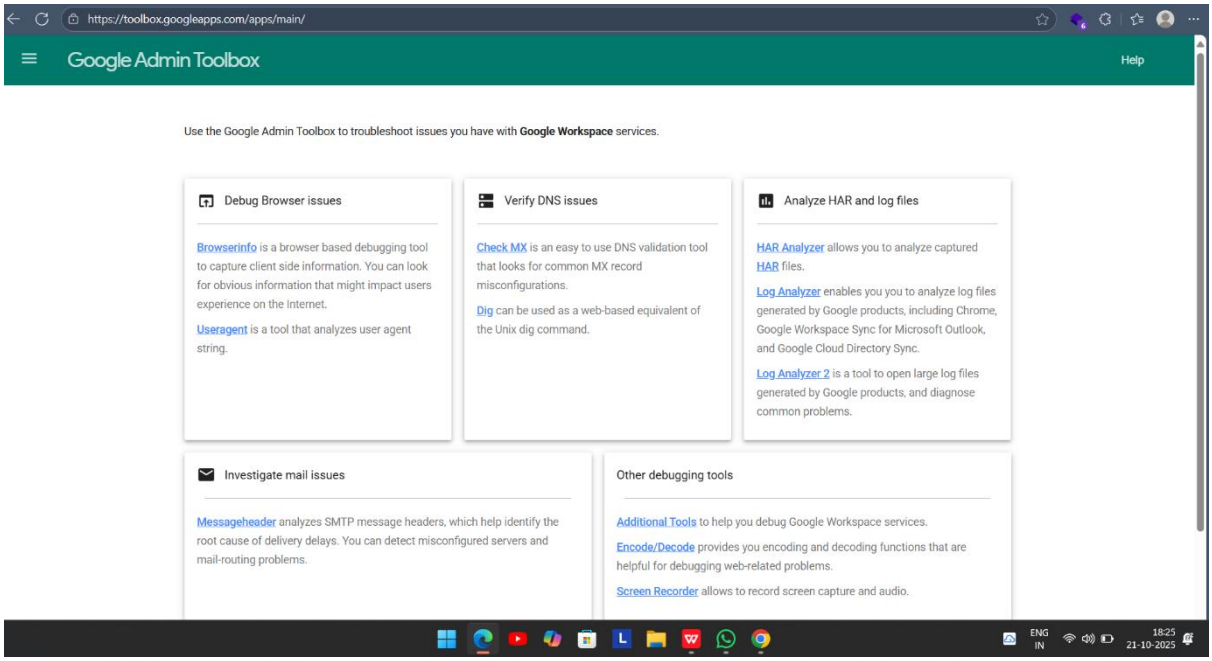
1.Obtained a sample phishing email. i took the spam one.



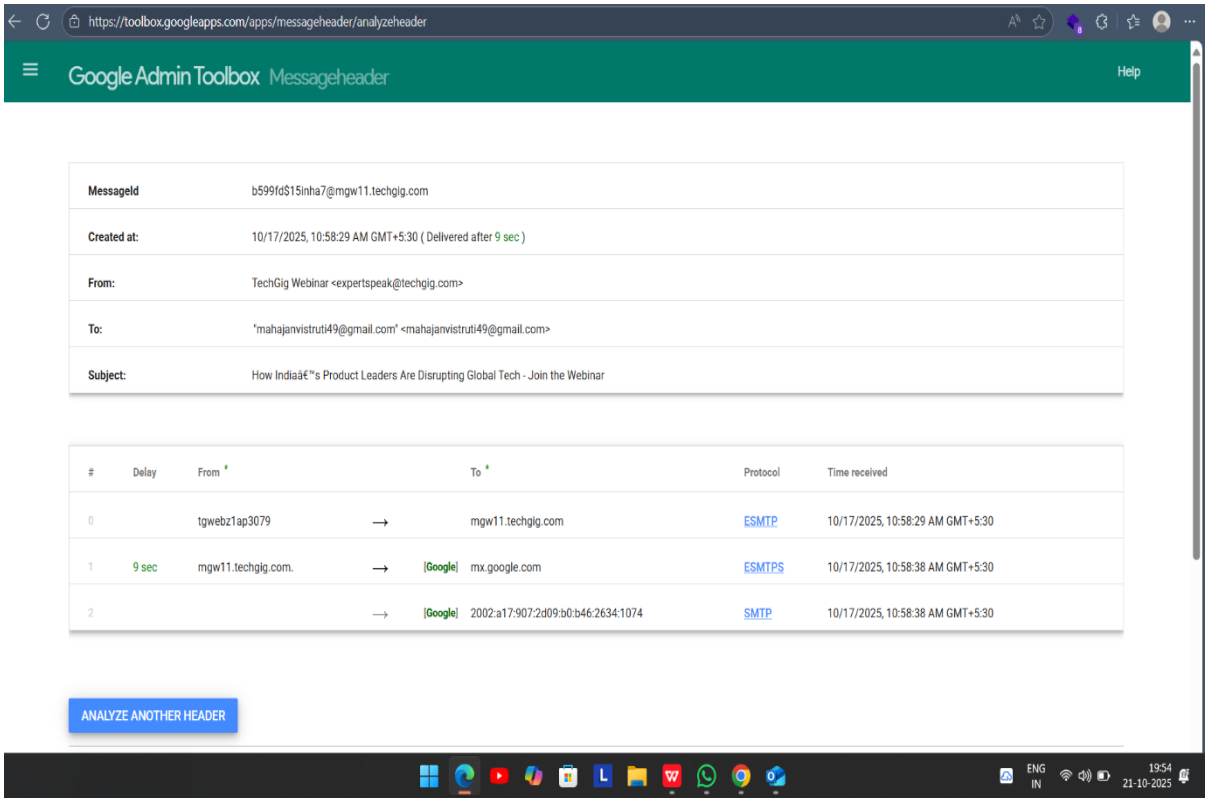
2.open the tool to analyse the header and fine if it is suspicious or not.



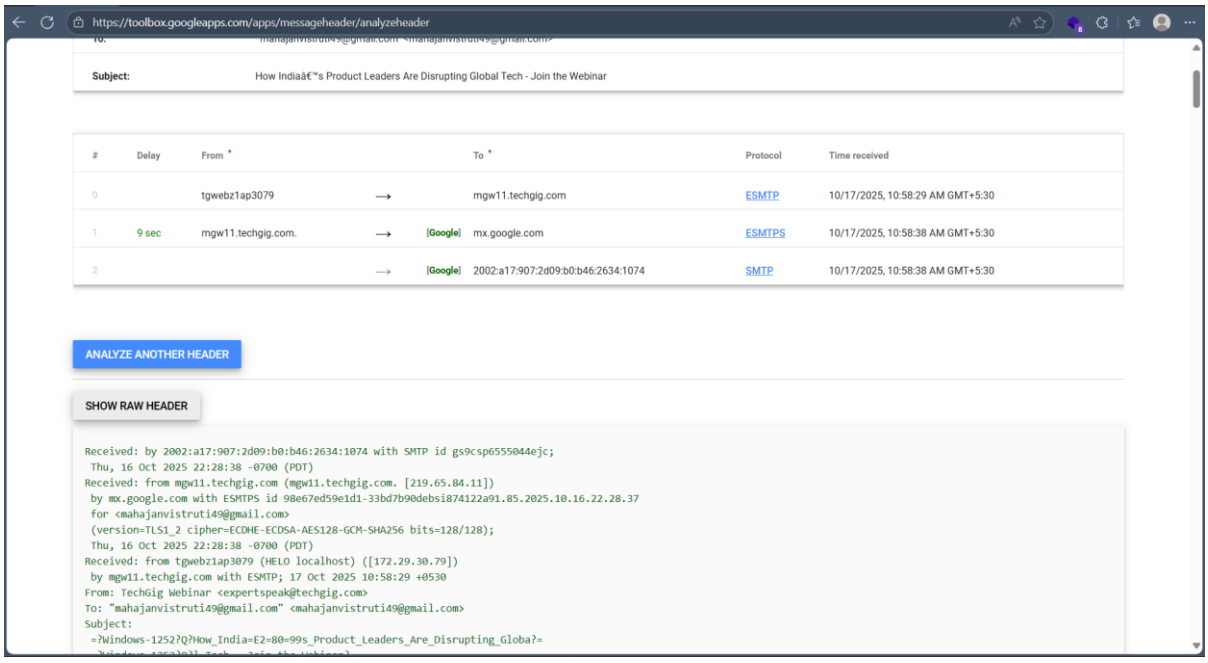

3.Go to the investigate mail issues to analyse the email.



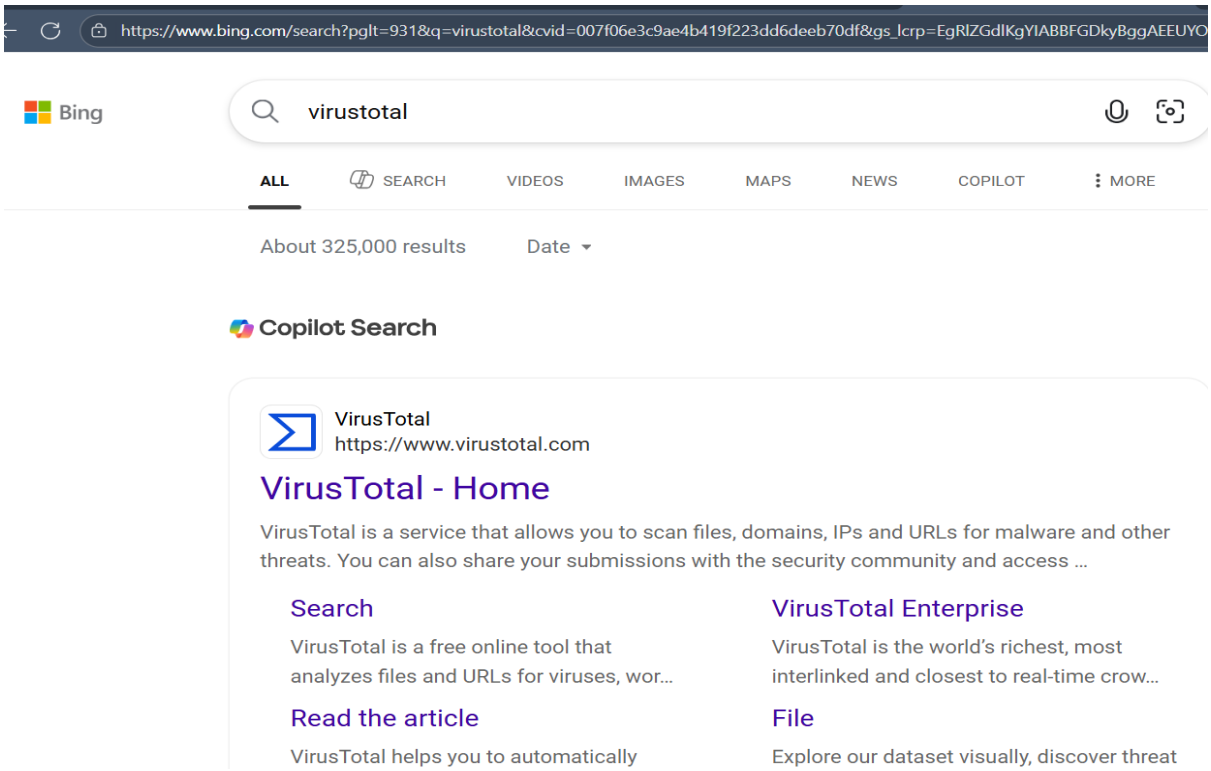
4.paste the header

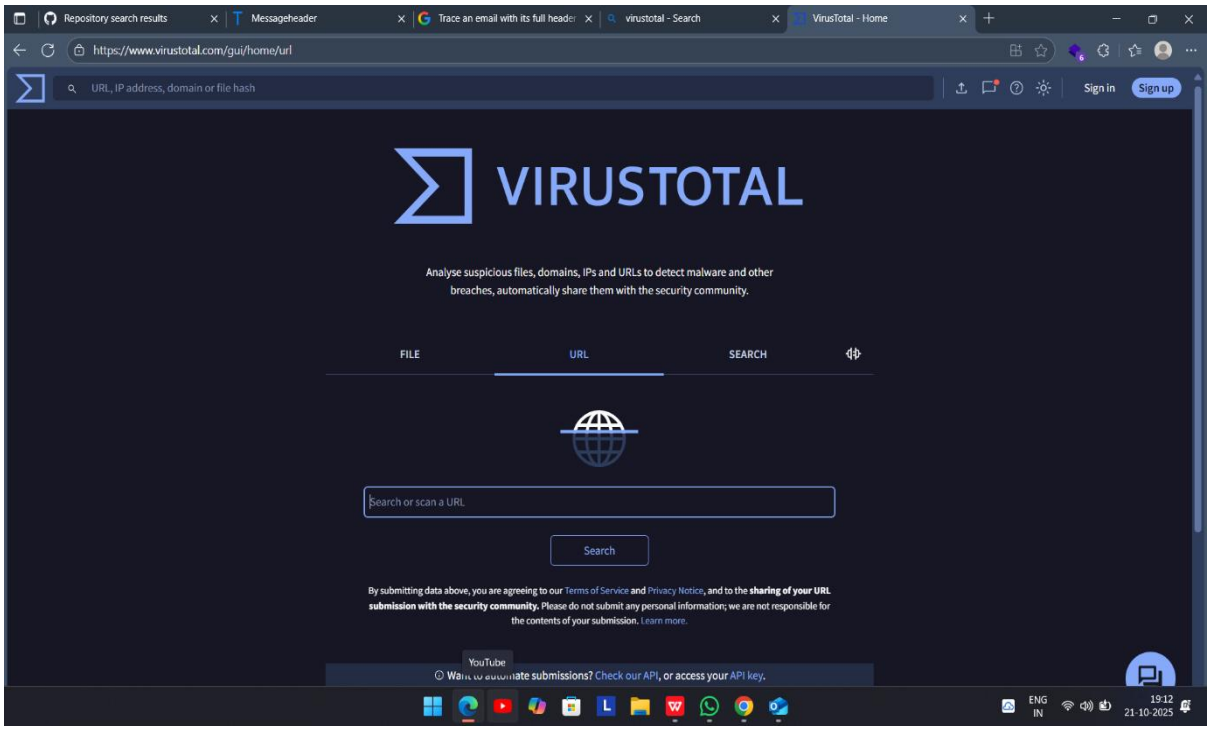



5.The result



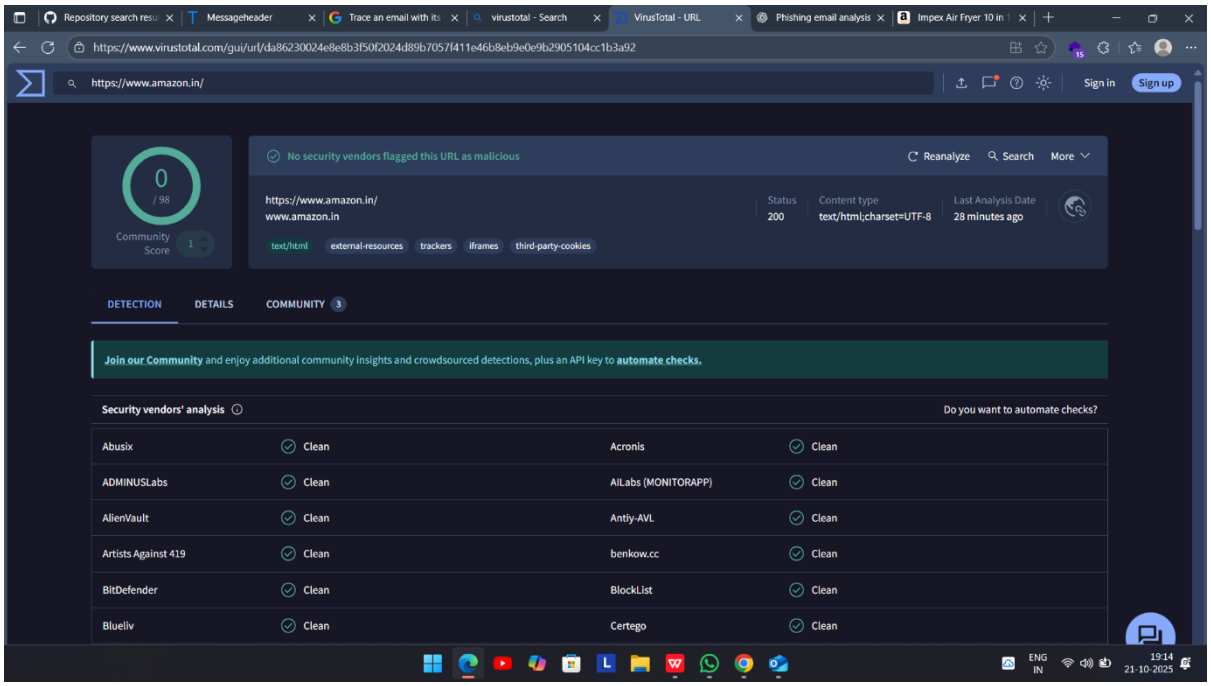
6.For the URLs I have used the virustotal tool.



7.I have used the amazon one for example.


8.The result




## conclusion:

The analysis revealed phishing indicators such as spoofed sender addresses, failed SPF/DKIM/DMARC checks, mismatched or suspicious URLs, urgent language, and spelling/grammar errors. This exercise helped build practical skills for detecting email threats and understanding how phishing attacks operate.