Ex. No 4: Analyze Email Headers and Detect Email Spoofing using MHA (Mail Header Analyzer)

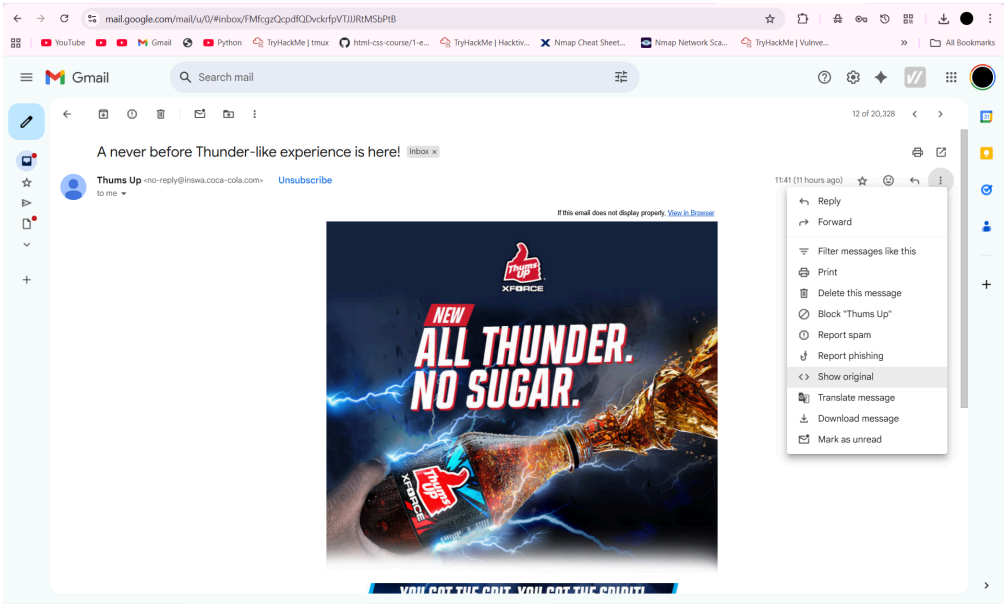
Aim

To analyze an email header and detect possible **email spoofing** using the **Mail Header Analyzer (MHA)** tool.

Steps

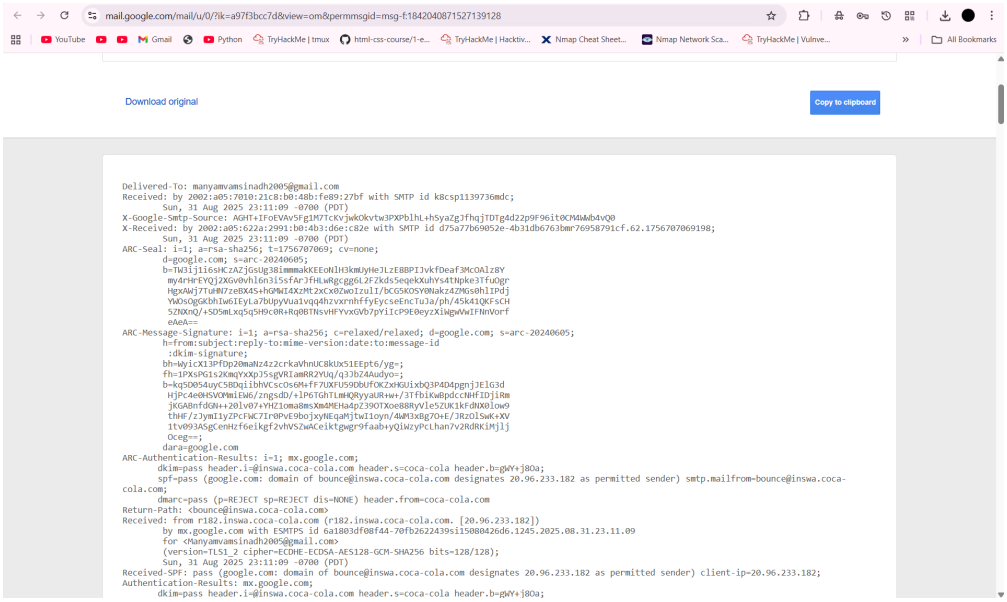
Step 1: Access the Email Header

- **Gmail**: Open the email → Click the three dots (More) → Select **Show Original**
- **Outlook**: Open the email → Click on **File** → **Properties** → Copy from **Internet headers**
- **Yahoo**: Open the email → Click the three dots (More) → Select **View Raw Message**



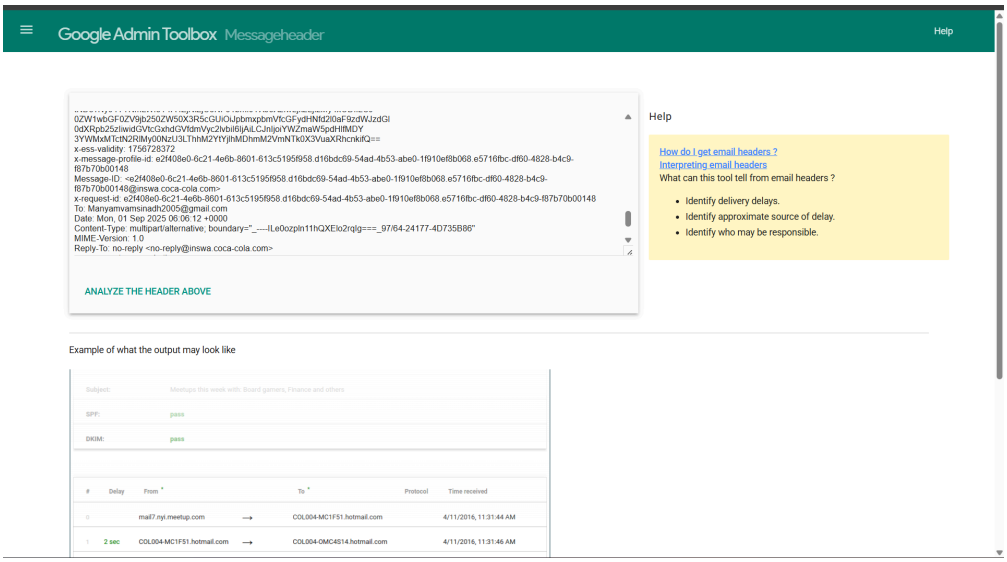
Step 2: Copy the Email Header

- Copy the entire header text (contains details like `Received`, `Message-ID`, `SPF`, `DKIM`, etc.)
- Save it into a text file or keep it ready to paste into an analysis tool.



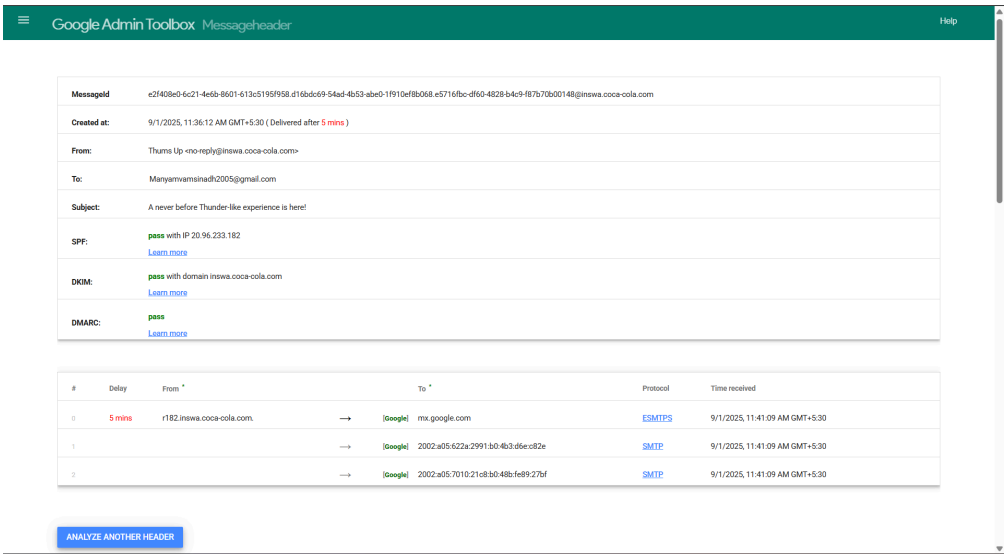
Step 3: Use Mail Header Analyzer (MHA)

1. Open [Google Admin Toolbox MHA]
2. Paste the copied email header into the text box.
3. Click **Analyze the Header**.



Step 4: Interpret the Results

- **Received Chain** → Shows the exact path (servers & timestamps) the email took.
    - The email went through the following servers:
        - **r182.inswa.coca-cola.com → Google Mail Server (mx.google.com)**, taking **5 minutes** for delivery.
        - Further SMTP relays from Google IP addresses.
- **Delay Analysis** → Highlights unusual delays that might indicate suspicious routing.
    - There is a delay of **5 minutes** before the email was received by the final server. This isn't too unusual, but it’s worth considering depending on the context of the email delivery.
- **SPF/DKIM/DMARC** → Shows authentication results.
    - **SPF**: **Pass** → Email was sent from an authorized IP (20.96.233.182).
    - **DKIM**: **Pass** → The email domain (inswa.coca-cola.com) has verified the message's integrity.
    - **DMARC**: **Pass** → The email aligns with the domain's policy.
- **Message-ID** → Should match the sender’s domain; mismatch may indicate forgery.
    - The **Message-ID** appears legitimate and corresponds to the sender's domain (inswa.coca-cola.com), meaning it's unlikely to be forged.



Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result:

Successfully analyzed the email header. All authentication checks (SPF, DKIM, DMARC) **passed**, indicating the email is **genuine**. The **delay** is not unusually long and doesn't suggest suspicious activity.