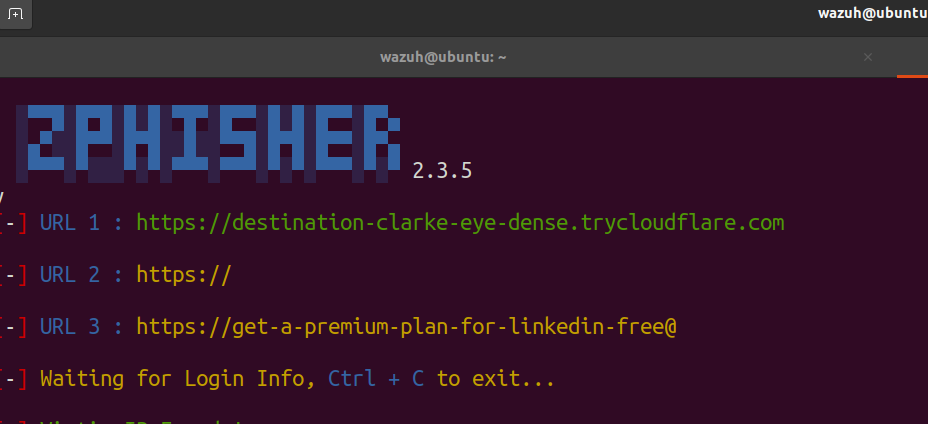
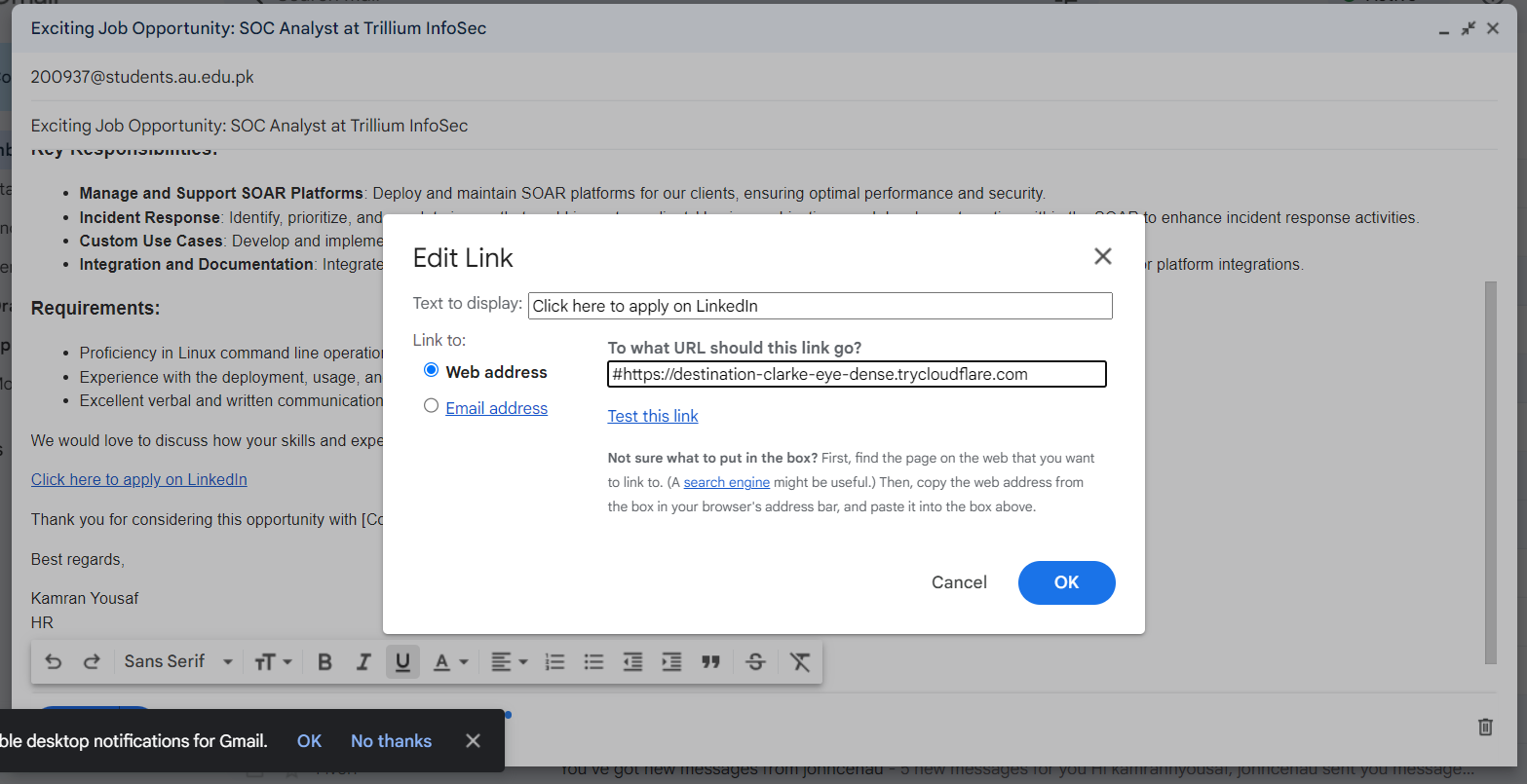
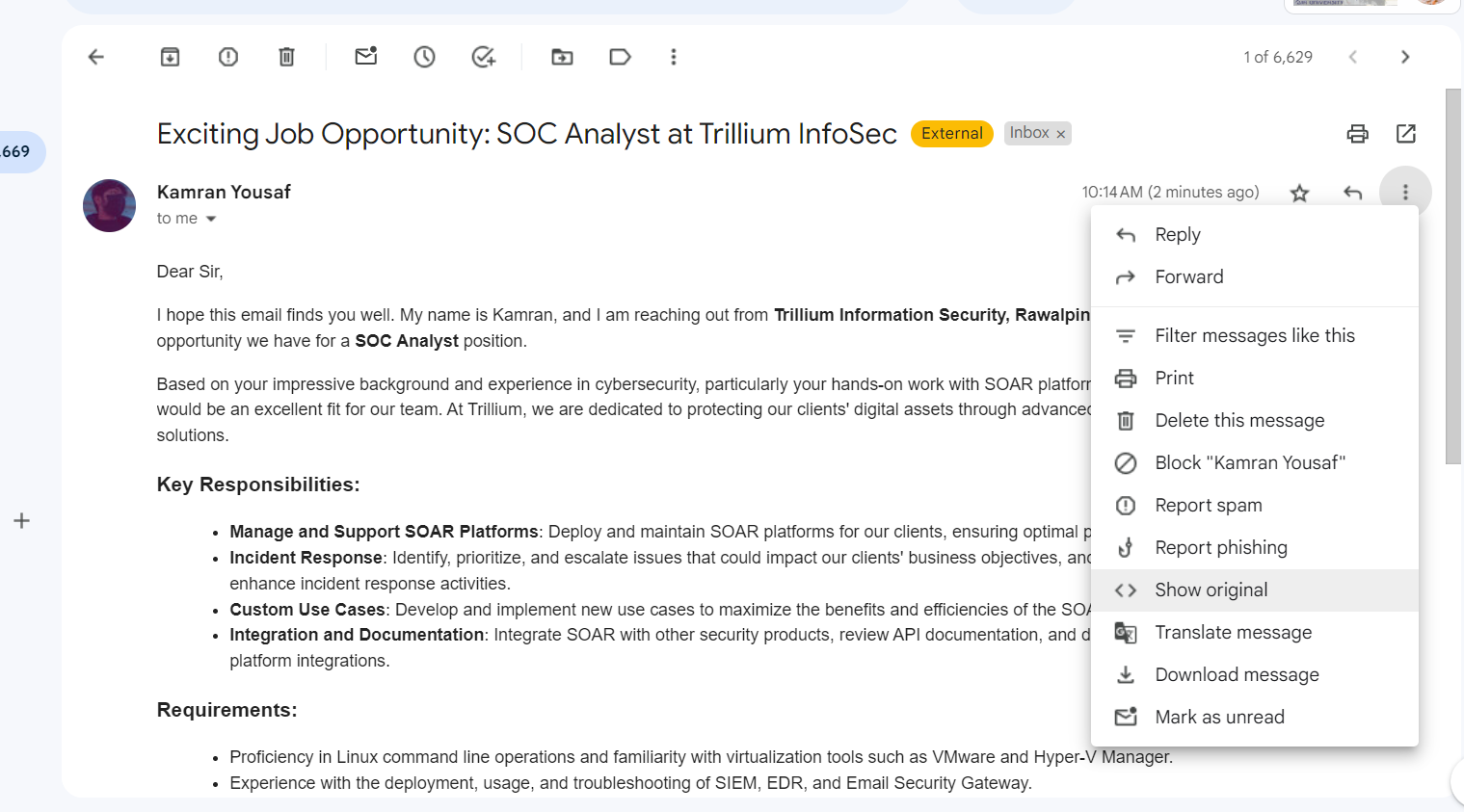
Muhammad Kamran Yousaf  
CodeAlpha   
  
Task 02:  
Stimulation of a phishing attack  
  
Solved:

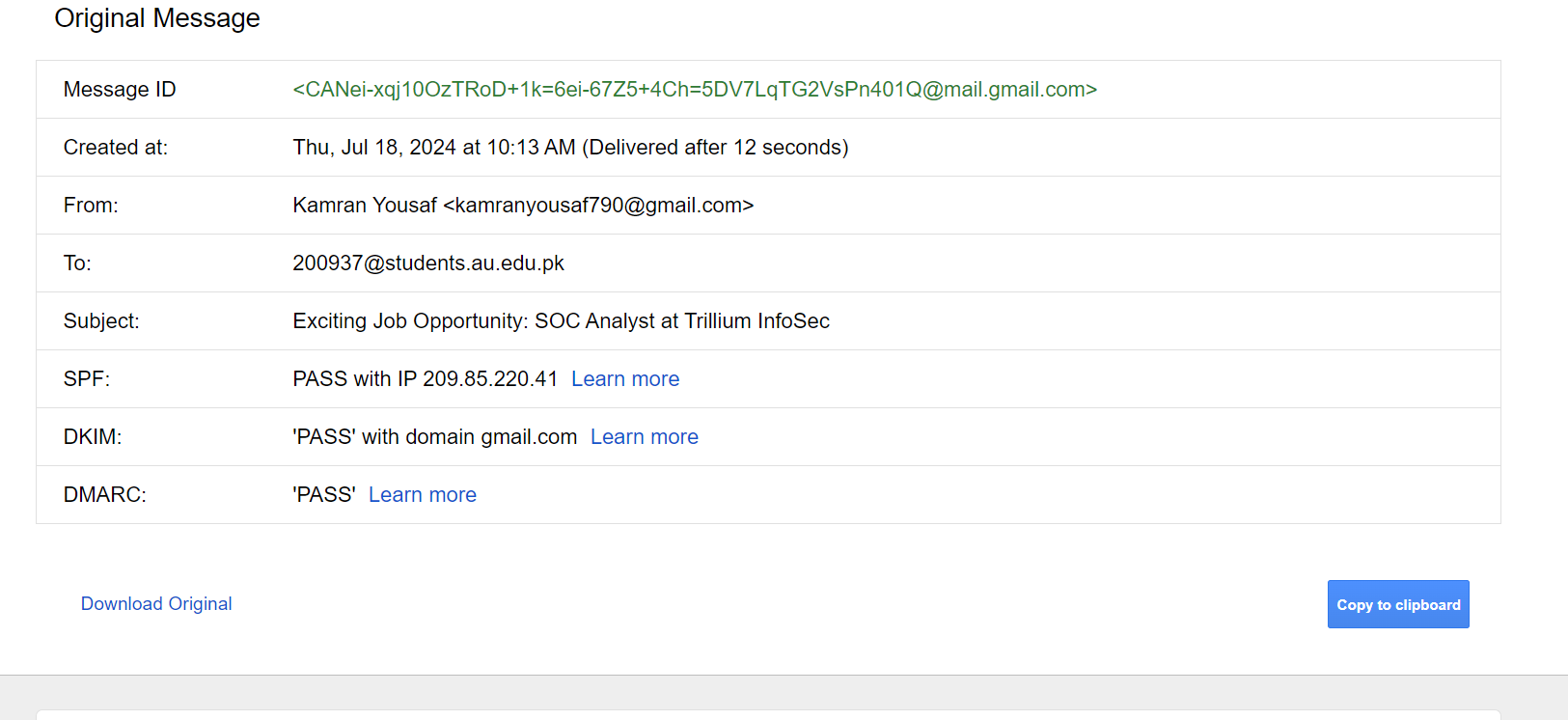
For this firstly we need to craft a malicious phishing email which can be sent to the target. I installed Zphisher to generate a malicious link to be added in the email.  


Then the email is written to send to our Victim  
  


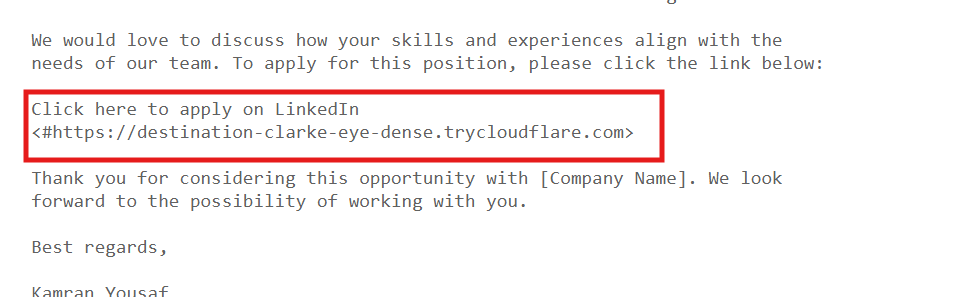
Once the email is received, click on the three dots and click show original, to see the email headers

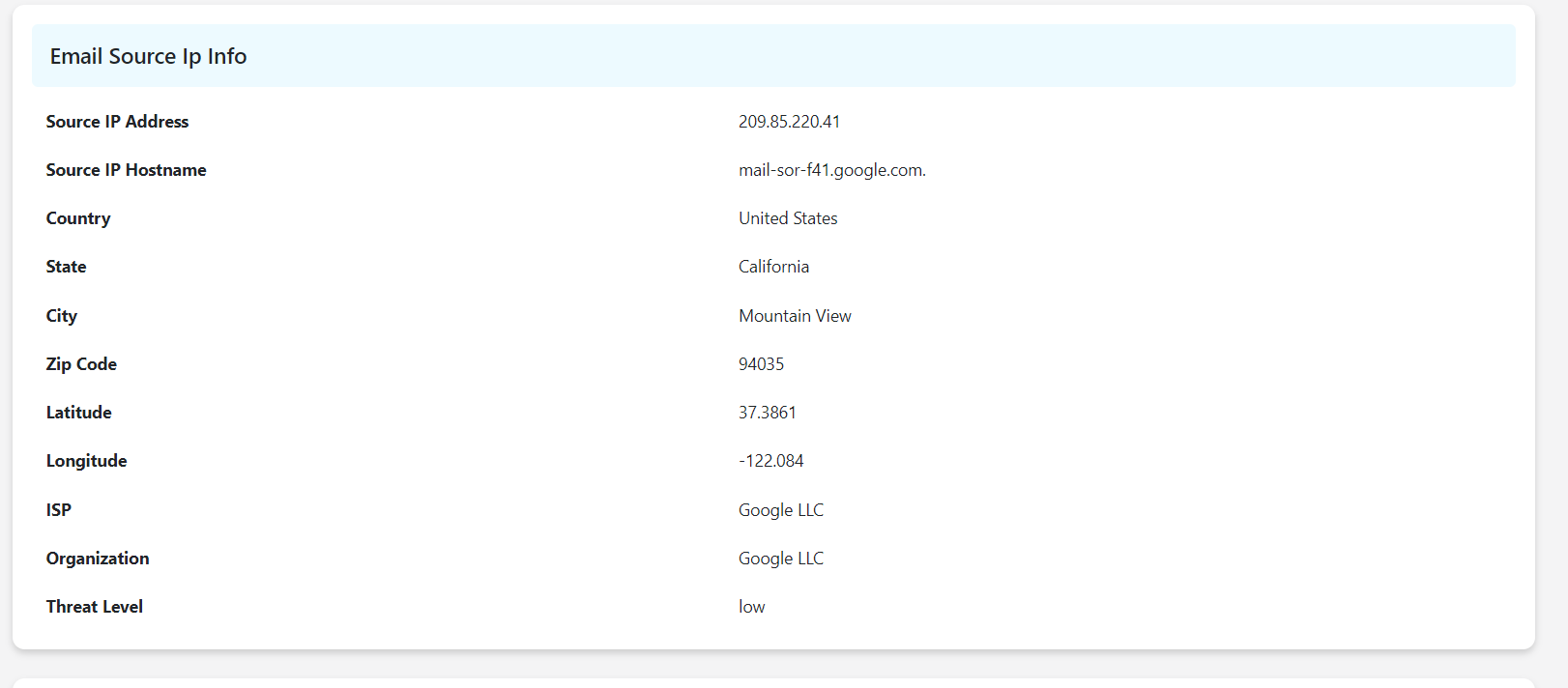


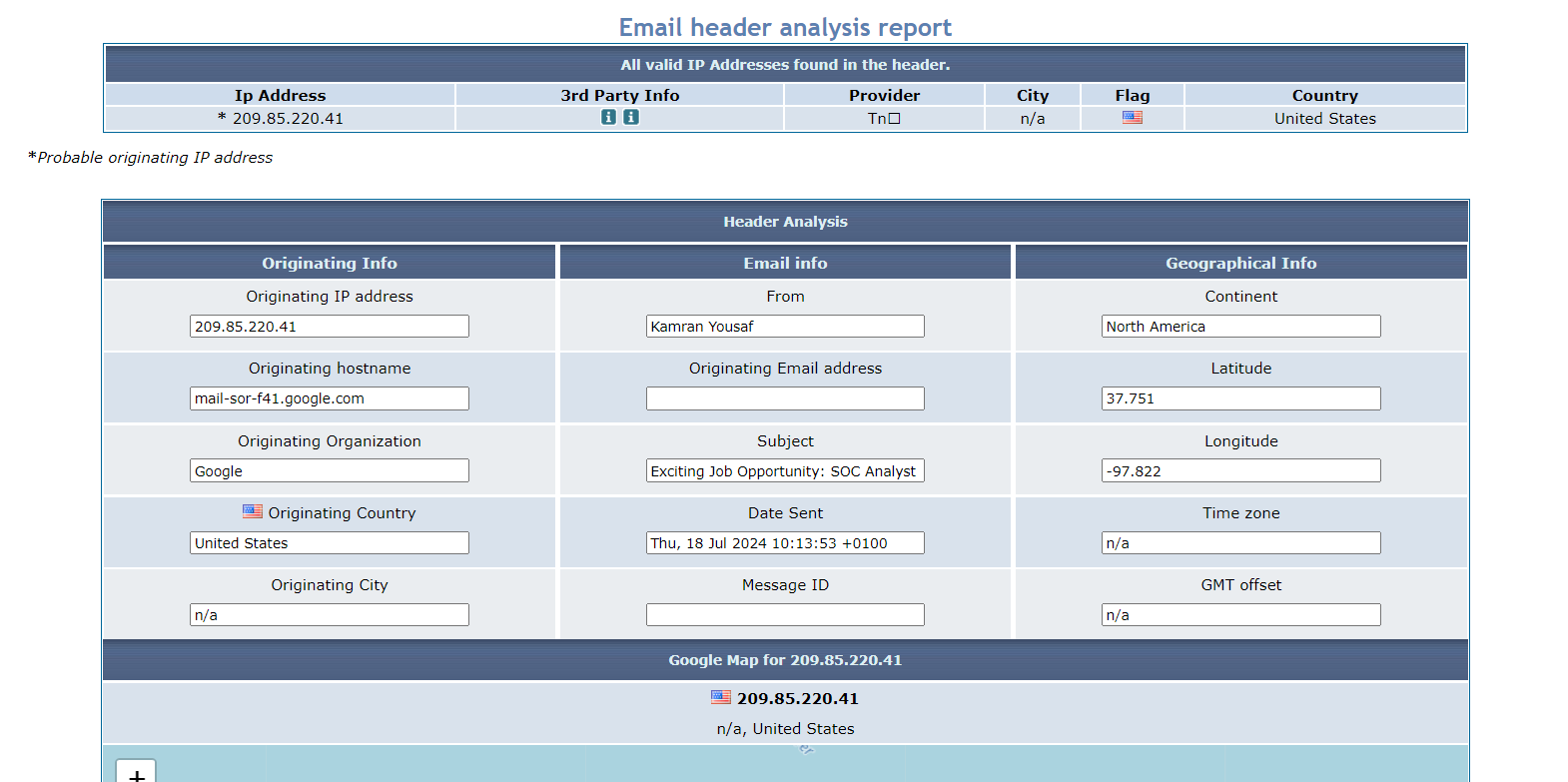
Once opened we can see a screen like that, here we can see few details about the sender and some authentication checks as well. Below these there is the header data which can give a lot of potential information



As we can see here all the authentication checks SPF, DKIM, DMARC are pass in the above email because the google considers the sender email [kamranyousaf@gmail.com](mailto:kamranyousaf@gmail.com) as a permitted email  


It shows the address of sender and the receiver but it is not in conventional IP format, we can use a email Header analyzer tool to extract such information further from the given header. If this email was sent from a forged or fake domain it should have been Failed the SPF, DKIM, DMARC check   
  
it is also an indication of a phishing email as the URL is leading to cloudflare server instead of Linkedin.  
Lets put this header in a header analyzer to see further details



We can see the source IP from this header, also as this mail was sent from Gmail client so the details of location etc are also mentioned and even the location is of the google’s head office because the email was using Gmail Client. To cross verify the originating ip address I used another tool IPtrackeronline to check for it and the results defined by it are same as mentioned above   


The main reason for this mail to be identified as phishing is because

* The email sender pretends to be from a company but instead of using company’s email they are using gmail address which is quite strange for a job offer.
* The email contains a directive to click and apply via linkedin, but the url below that is not of linkedin instead it routes to a cloudflare server where a fake linkedin page is being hosted
* This specific email passes the authentication checks (SPF,DMARC,DKIM) because it was sent from a permitted source, if it would have been sent from a suspicious impersonating domain then the checks might have failed, indicating phishing attempt