Cyber Law and Forensics (CS402)

Lab Assignment 6

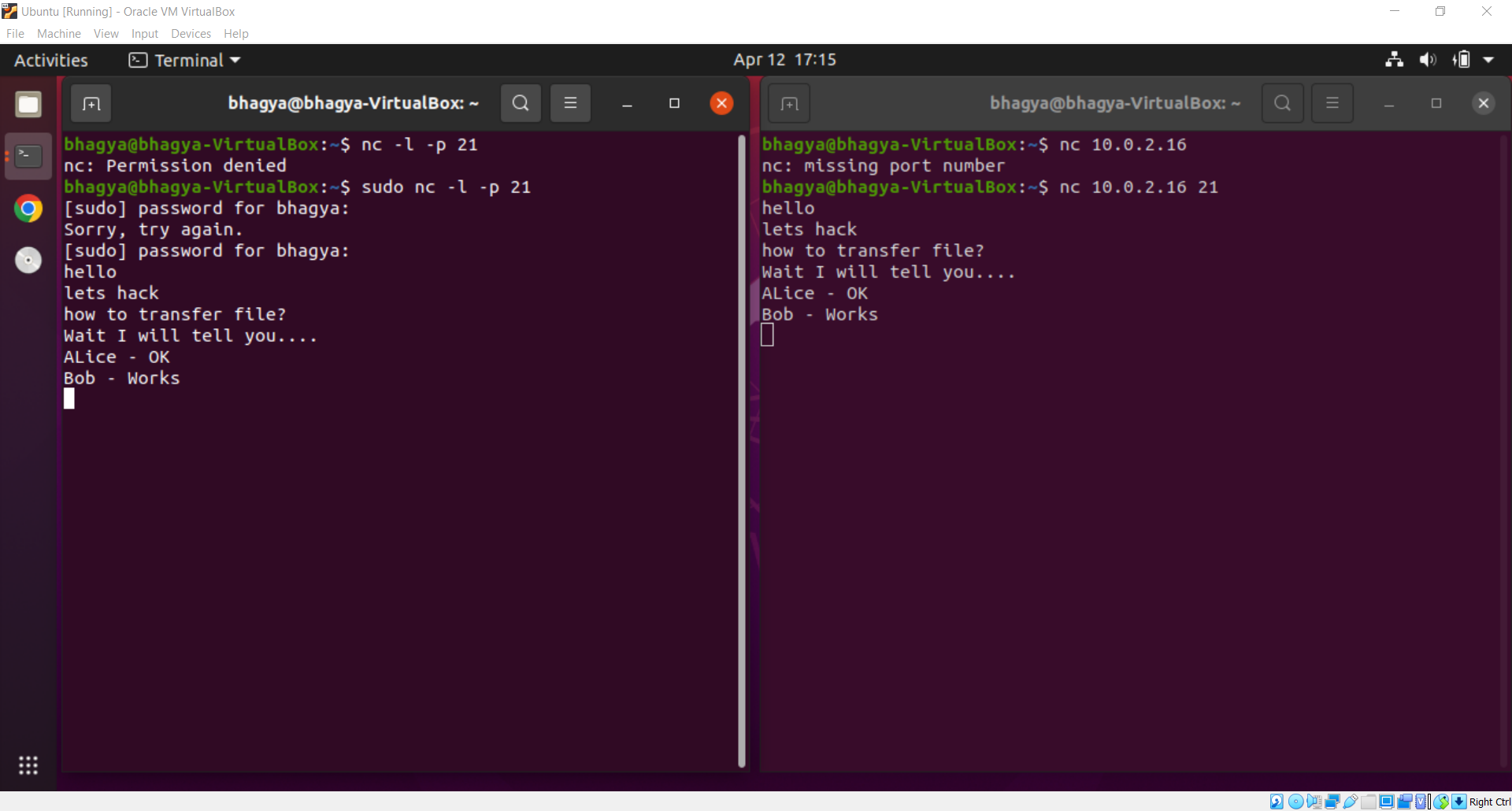
**U19CS012**

A.) Remote data acquisition using Netcat Command

Link 1: <https://www.youtube.com/watch?v=cq9RHDL2yMM>

Link 2: <https://www.youtube.com/watch?v=OcSS34Lw910>

Link 3: <https://www.youtube.com/watch?v=HehVavsBhgI>

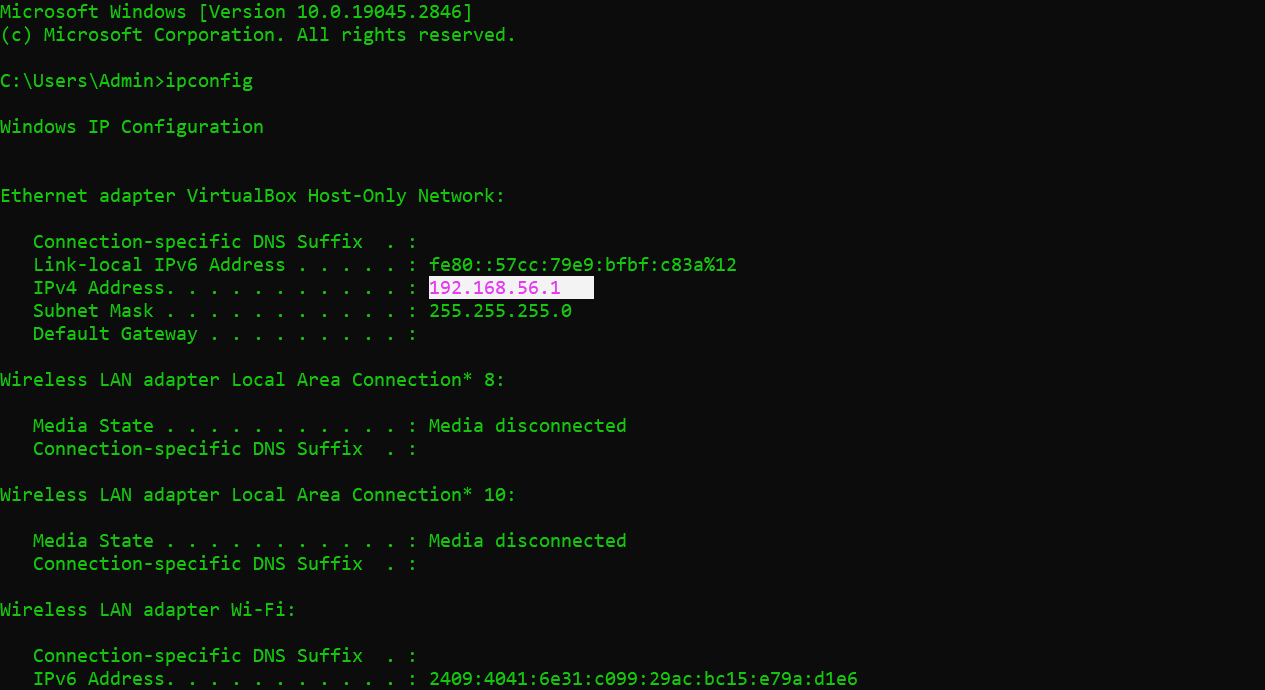


“nc” - netcat

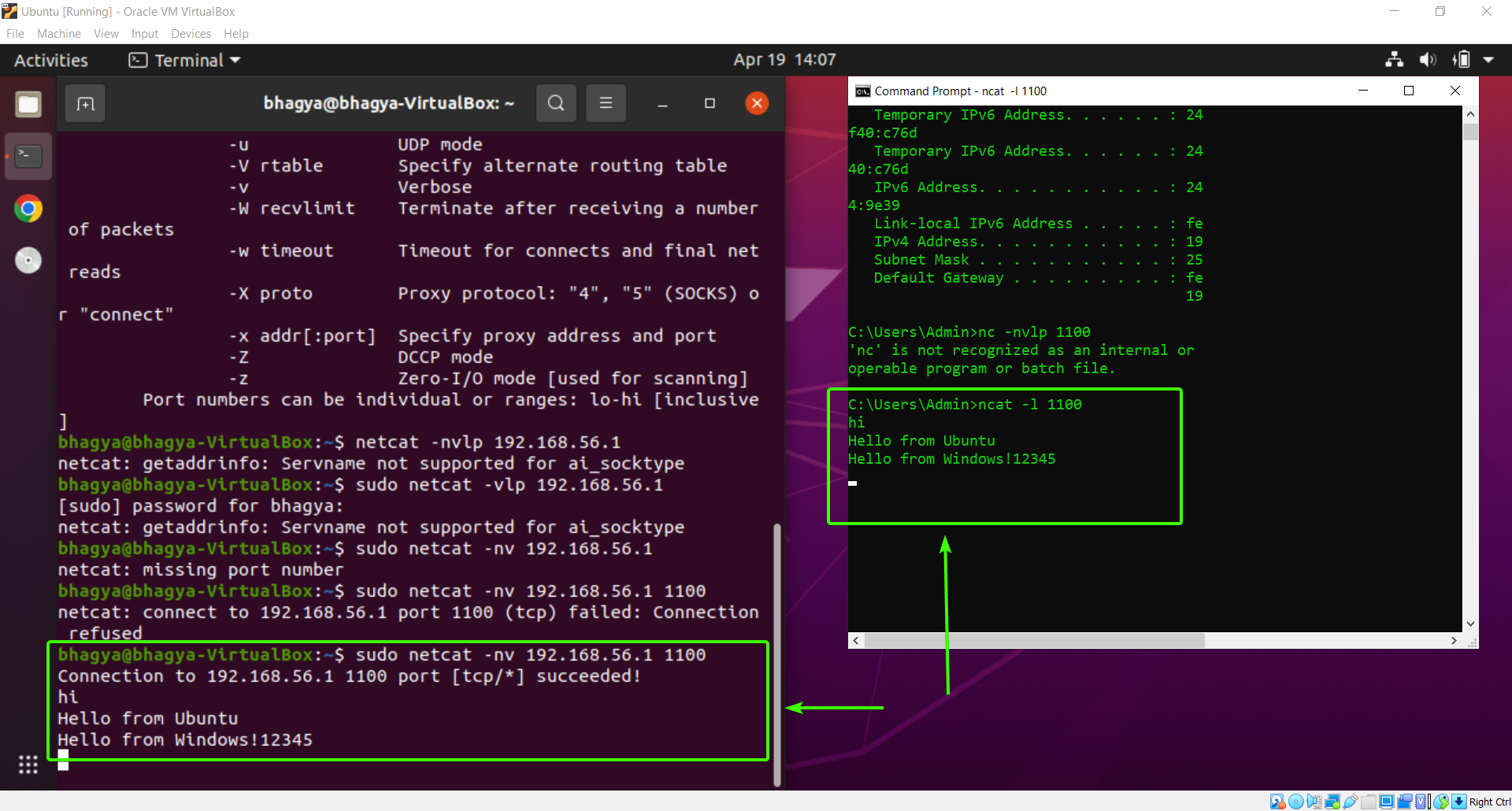
-v = verbose output

-l = listening

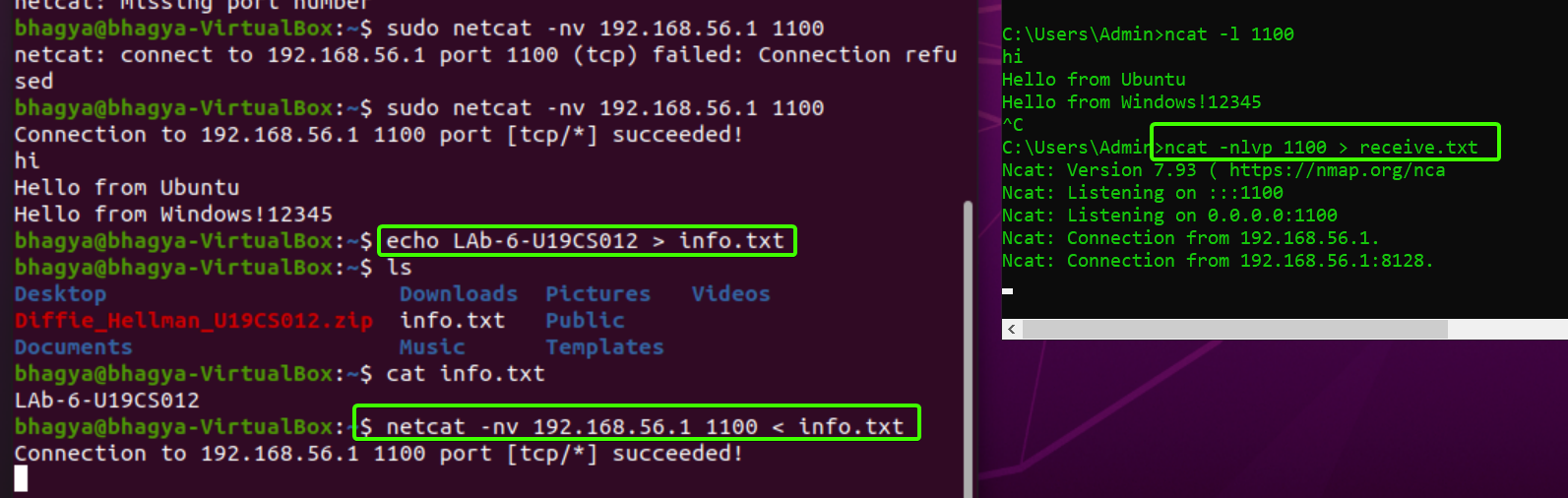
-p = port number



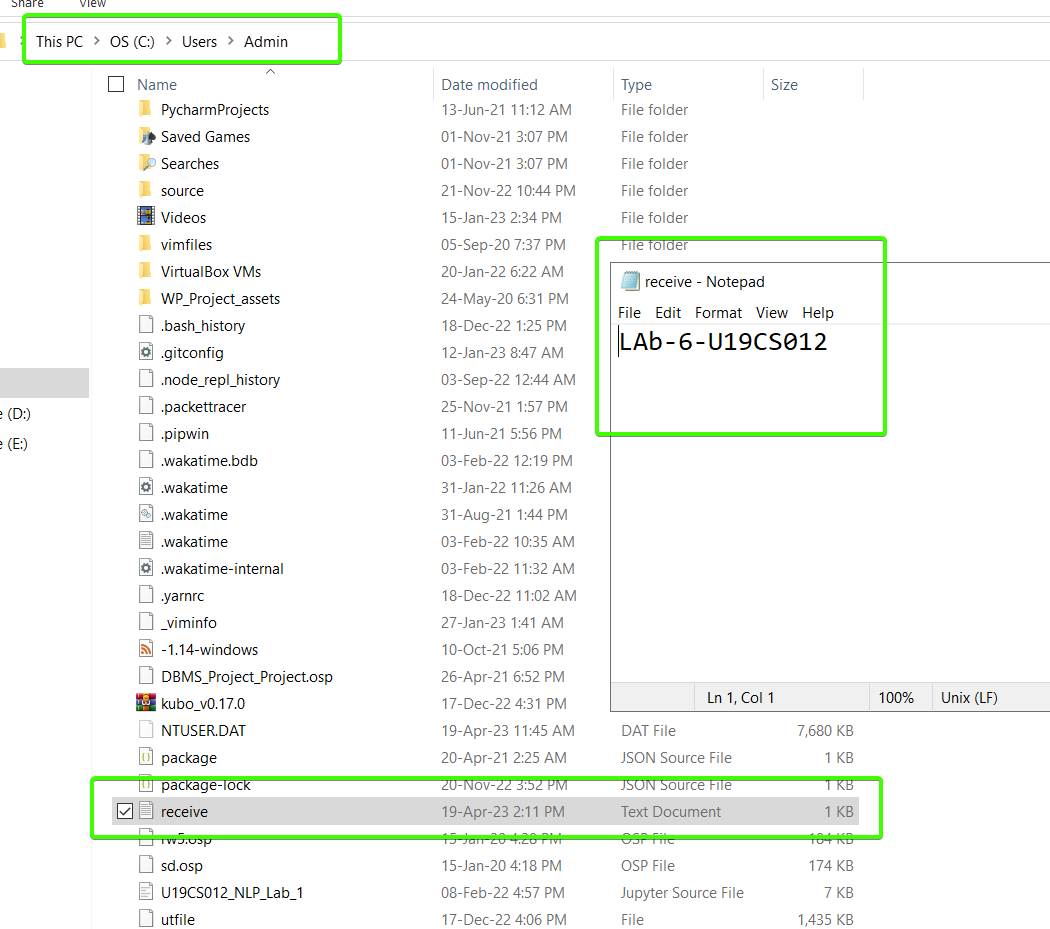
Get the IP Address of Windows Machine using “ipconfig”.



Once we have checked that message Transfer is Possible and Correct, Lets do the same for File Transfer.



We make a File “info.txt” with Text “Lab-6-U19CS012” and save it. Afterwards, We listen to Port 1100 and send the output to “receive.txt” File. Using netcat command we Successfully Transfer the File.



As you can see in above image, that the File is received!

B.) Identify whether the email is a **fake mail** or **legitimate email**?

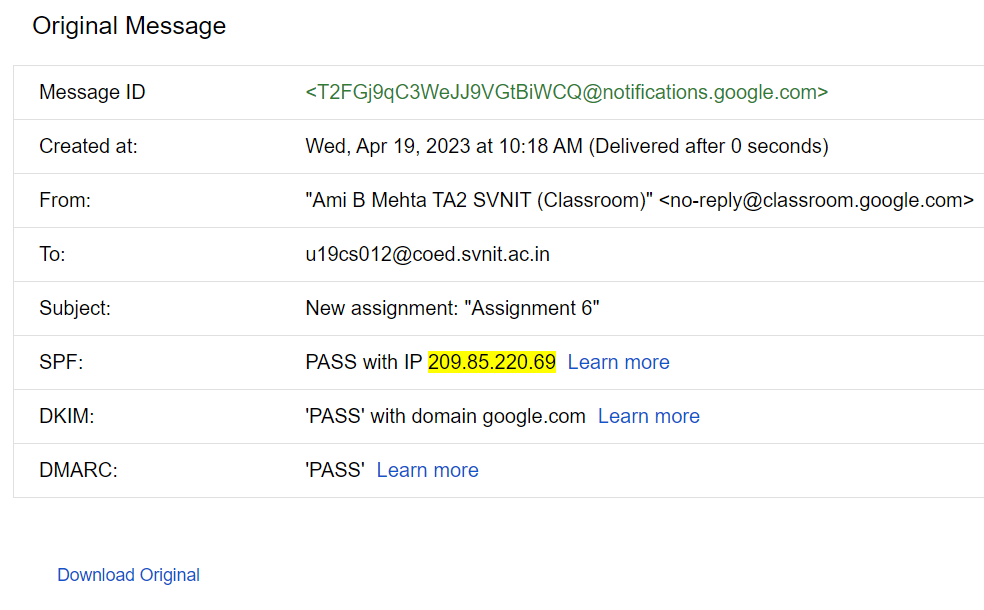
* Email Evidence is in Email itself (Header)!
* Tracing -> Examination of an Email Header to determine its **point of origin**
* Header – Info regarding the Sender, Receiver and the Route the Email took to the Destination

**Retrieving email headers**

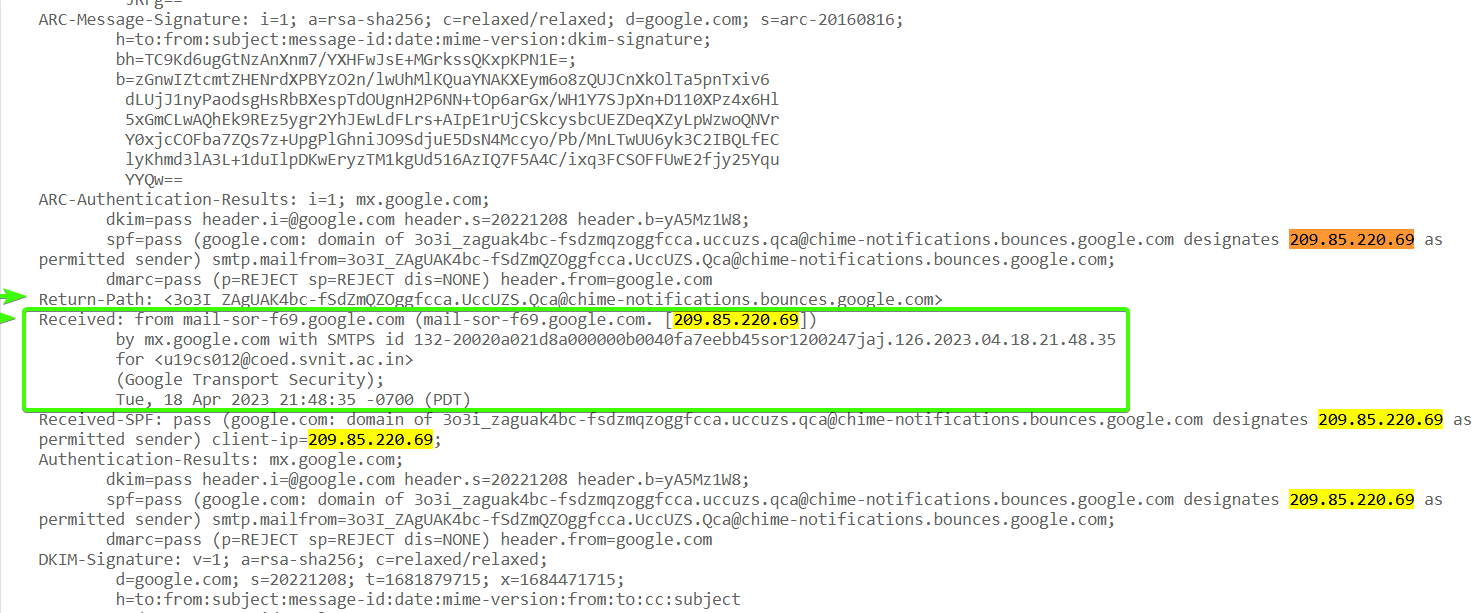
* + Office 365: Open email, click on the three dots at the top right, select 'View message details.
  + Gmail: Open email, click on the three dots at the top right, select 'Show original'. The header will appear on the bottom part of the screen
  + Yahoo: Open email, click on the three dots at the bottom, select 'View raw message.
  + Outlook: Open email, navigate to the horizontal menu at the top and click on 'File', click on 'Properties' in the 'Info' section, the header is in the 'Internet headers' box

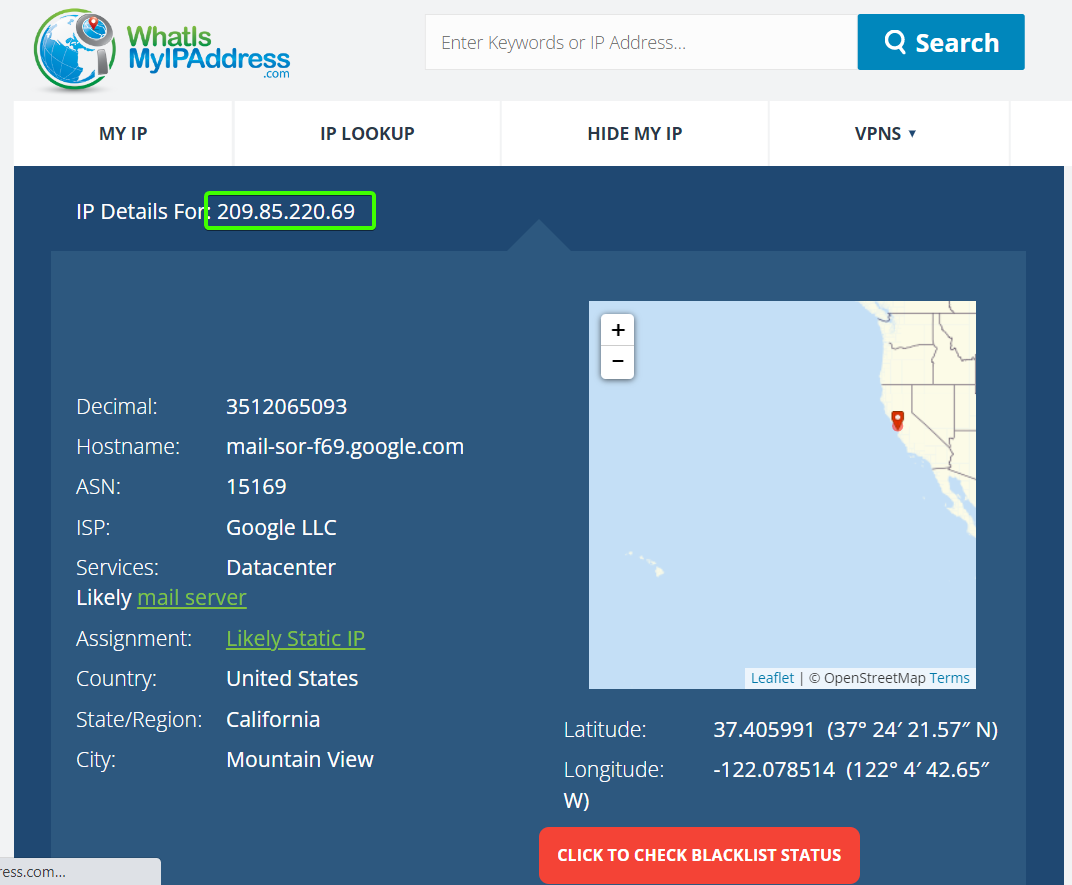
Select all and copy/paste into a text editor like Notepad (may need to enter line breaks)

**Why**? When you Forward the Phishing Email, It moves the Header Information.



* SPF, DKIM and DMARC authentication





Overall, Just check the **Received from** in Email Header and Cross Verify the IP Address, to check whether the Email is Legitimate or Not.

**SUBMITTED BY**:

U19CS012

BHAGYA VINOD RANA