CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-8

Wireshark Lab: NAT & SMTP

March 10, 2025

Chidurala Tejaswini
(CS22BT012/220010012)

Part-1(Introduction)

In this lab, we'll investigate the behaviour of a NAT router. This lab will be different from our other Wireshark labs, where we've captured a trace file at a single Wireshark measurement point. Because we're interested in capturing packets at *both* the input and output sides of the NAT device, we'll need to capture packets at *two* locations. Also, because many students don't have easy access to a NAT device or to two computers on which to take Wireshark measurements, this isn't a lab that is easily done "live" by a student. So, in this lab, you'll use Wireshark trace files that we've captured for you. This should be a relatively short and easy lab since the concepts behind NAT aren't difficult, but it'll be good nonetheless to observe NAT in action.

NAT Measurement Scenario

In this lab, we'll capture packets containing a simple HTTP GET request message from a client inside a home network to a remote server, and the corresponding HTTP response from that server. Within the home network, the home network router provides a NAT service, Figure 1 shows our Wireshark trace-collection scenario. We'll capture packets in *two* locations, and thus this lab has *two* trace files:

- We'll capture packets being received at the local area network (LAN) side of the NAT router. All devices in this LAN have addresses in 192.168.10/24. This file is named ***nat-inside-wireshark-trace1-1.pcapng*.**
- Because we're also interested in analysing packets being forwarded (and received) by the NAT router on its Internet-facing side, we'll collect a second trace file on the Internet side of the router, as shown in Figure 1. Packets captured by Wireshark at this point that were sent from a host on the right to the server on the left will have undergone NAT translation by the time they reach this second measurement point. This file is named ***nat-outside-wireshark-trace1-1.pcapng*.**

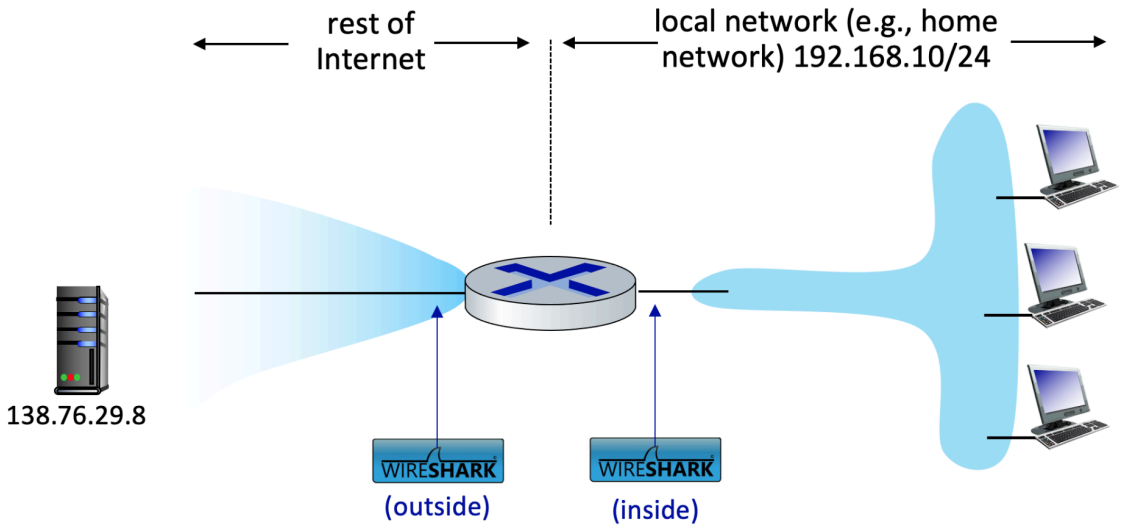
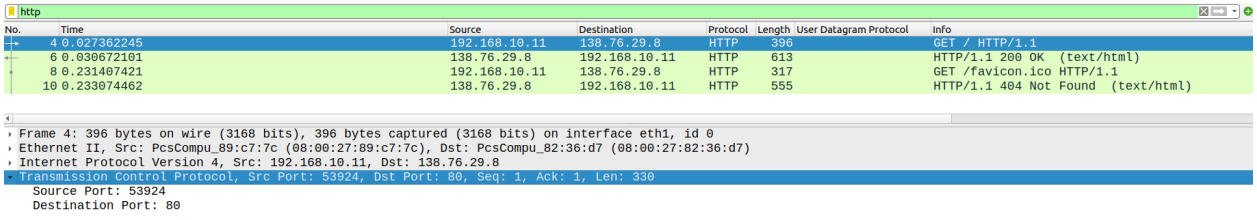


Figure 1: NAT packet capture scenario

Let's first take a look at what's happening on the LAN side of the NAT router. Open the ***nat-inside-wireshark-trace1-1.pcapng*** trace file. In this file, you should see an HTTP GET request addressed to the external web server at IP address 138.76.29.8, as well as the subsequent HTTP response message ("200 OK"). Both of these messages in the trace file were captured on the LAN side of the router.

Answer the following questions.

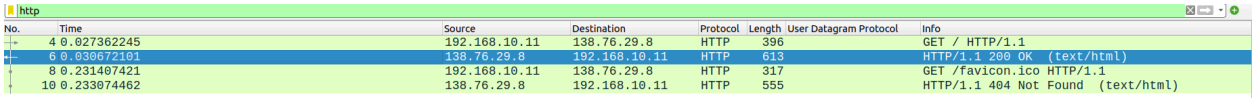
1. **What is the IP address of the client that sends the HTTP GET request in the *nat-inside-wireshark-trace1-1.pcapng* trace? What is the source port number of the TCP segment in this datagram containing the HTTP GET request? What is the destination IP address of this HTTP GET request? What is the destination port number of the TCP segment in this datagram containing the HTTP GET request?**



IP address of the client that sends the HTTP GET request	**192.168.10.11**

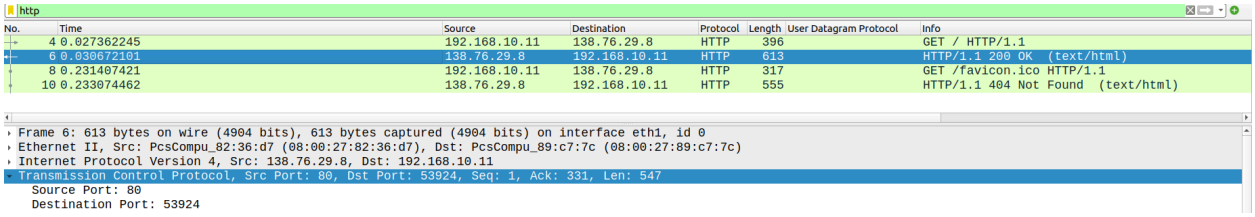
Source port number of the TCP segment in this datagram containing the HTTP GET request	**53924**
Destination IP address of this HTTP GET request	**138.76.29.8**
Destination port number of the TCP segment in this datagram containing the HTTP GET request:	**80**

2. **At what time is the corresponding HTTP 200 OK message from the web server forwarded by the NAT router to the client on the router's LAN side?**



Time : 0.030672101 seconds

3. **What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?**



Source Address	**138.76.29.8**
Destination Address	**192.168.10.11**
Source Port	**80**
Destination Port	**53924**

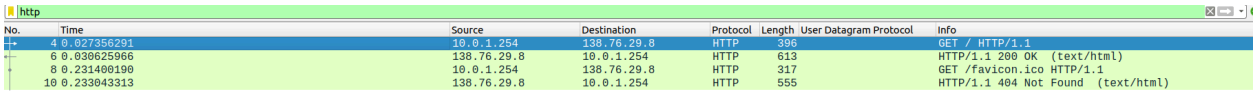
In the following, we'll focus on these two HTTP messages (GET and 200 OK). Our goal below will be to locate these two HTTP messages in the trace file *nat-outside-wireshark-trace1-1.pcapng*, captured on the Internet-side link between the router and

the ISP. Because the captured packets heading towards the server will have already been forwarded through the NAT router, some of the IP addresses and port numbers will have been changed as a result of NAT translation.

Open the trace file *nat-outside-wireshark-trace1-1.pcapng*. Note that the time stamps in this file and the *nat-inside-wireshark-trace1-1.pcapng* files are not necessarily synchronized.

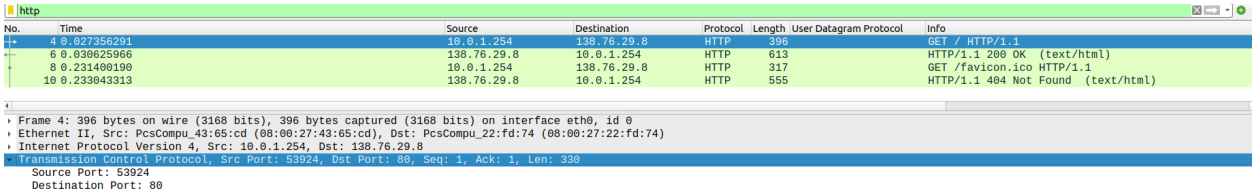
In the *nat-outside-wireshark-trace1-1.pcapng* trace file, find the HTTP GET message that corresponds to the HTTP GET message that was sent from the client to the 138.76.29.8 server at time t=0.027362245, where t=0.027362245 is the time at which this message was sent, as recorded in the *nat-inside-wireshark-trace1-1.pcapng* trace file.

4. **At what time does this HTTP GET message appear in the *nat-outside-wireshark-trace1-1.pcapng* trace file?**



Time : 0.027356291 seconds

5. **What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP GET (as recorded in the *nat-outside-wireshark-trace1-1.pcapng* trace file)?**



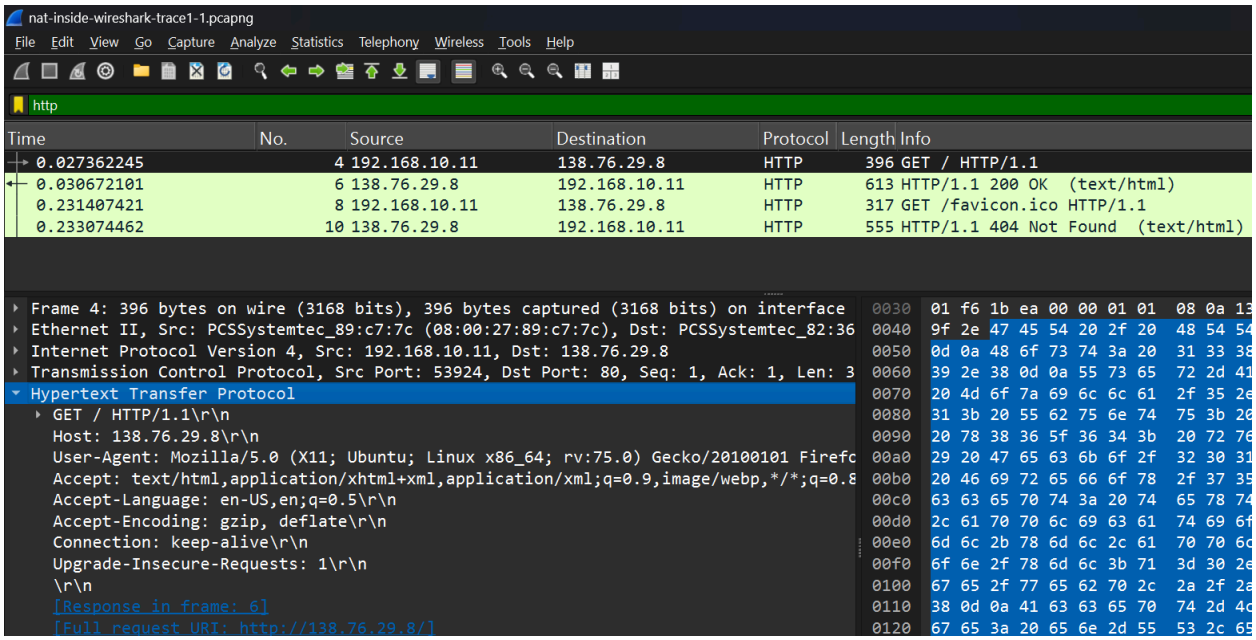
Source Address	**10.0.1.254**
Destination Address	**138.76.29.8**
Source Port	**53924**
Destination Port	**80**

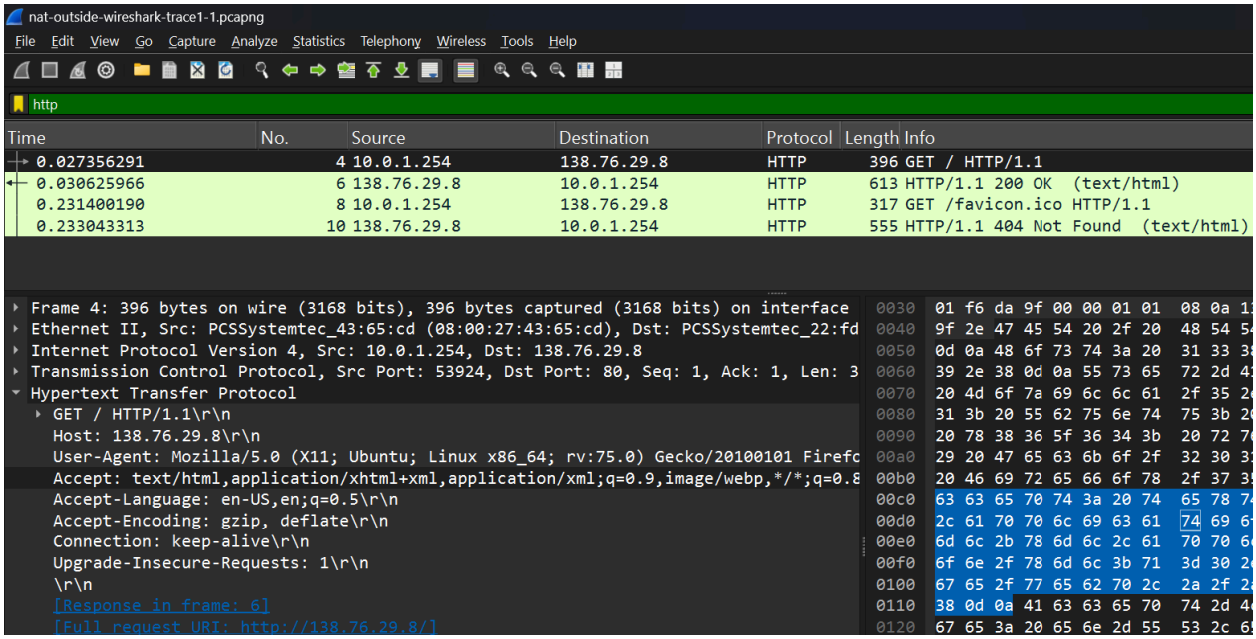
6. **Which of these four fields is different from your answer to question 1 above?**

Source Address

7. **Are any fields in the HTTP GET message changed?**

   In the HTTP GET message, no fields are changed



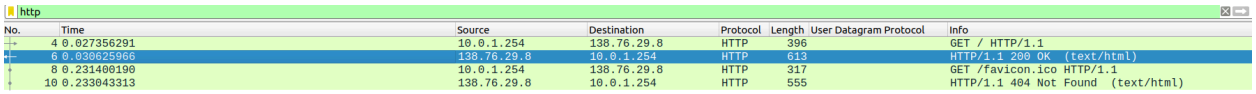


8. **Which of the following fields in the IP datagram carrying the HTTP GET are changed from the datagram received on the local area network (inside) to the corresponding datagram forwarded on the Internet side (outside) of the NAT router: Version, Header Length, Flags, Checksum, Source Address, TTL?**

   Checksum, Source Address, TTL fields are changed.

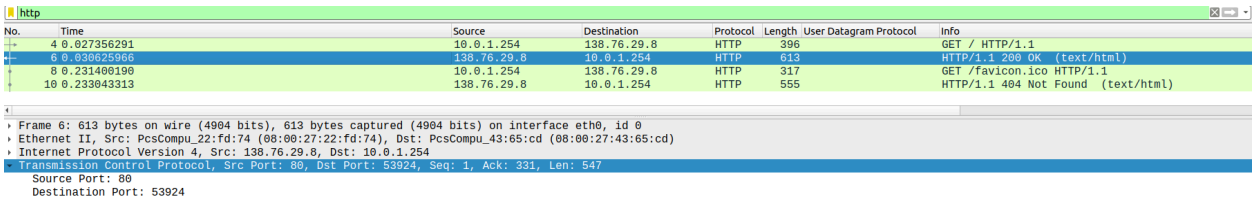
Let's continue to look at the *nat-outside-wireshark-trace1-1.pcapng* trace file. Find the HTTP reply containing the "200 OK" message that was received in response to the HTTP GET request you just examined in questions 4-8 above.

9. **At what time does this message appear in the *nat-outside-wireshark-trace1-1.pcapng* trace file?**



Time: 0.030625966 seconds

10. **What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP reply ("200 OK") message (as recorded in the *nat-outside-wireshark-trace1-1.pcapng* trace file)?**



Source Address	**138.76.29.8**
Destination Address	**10.0.1.254**
Source Port	**80**
Destination Port	**53924**

Lastly, let's consider what happens when the NAT router receives this datagram that you examined in questions 9 and 10, performs NAT translation, and finally forwards that datagram to the destination host on the LAN side. Based on your answers to questions 1 through 10 above and your knowledge of how NAT works, you should be able to answer the following question without actually looking at the *nat-inside-wireshark-trace1-1.pcapng* trace file:

11. **What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying the HTTP reply ("200 OK") that is forwarded from the router to the destination host in the right of Figure 1?**

To ensure you understand NAT, you should now use Wireshark to peek into the *nat-inside-wireshark-trace1-1.pcapng* trace file and look at the HTTP reply ("200 OK").

Do your answers to question 11 above match what you see in the *nat-inside-wireshark-trace1-1.pcapng* trace file?

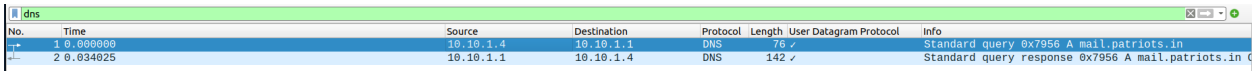
Source Address	**138.76.29.8**
Destination Address	**192.168.10.11**
Source Port	**80**
Destination Port	**53924**

Yes, the answers to question 11 get matched to what we see in the nat-inside-wireshark-trace1-1.pcapng trace file.

Part-2: SMTP

Answer the following questions referring to `Assignment_8_smtp_trace.pcap` file

1. **What is the IP address of the client, and DNS resolver?**



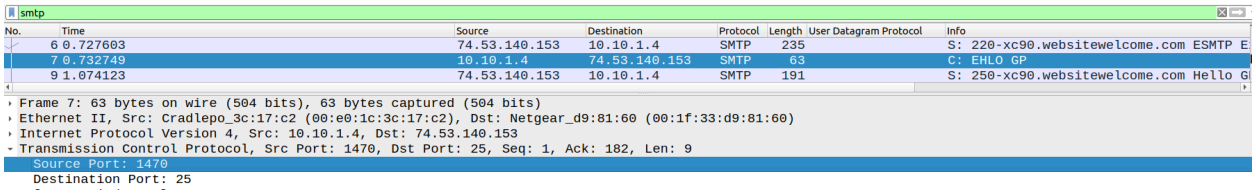
IP address of the client : 10.10.1.4
DNS resolver: 10.10.1.1

2. **Mention the domain name, and IP address of the mail server to which the client is requesting to send an email.**

```
mail.patriots.in: type CNAME, class IN, cname patriots.in
    Name: mail.patriots.in
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 10827 (3 hours, 27 seconds)
    Data length: 2
    CNAME: patriots.in
patriots.in: type A, class IN, addr 74.53.140.153
```

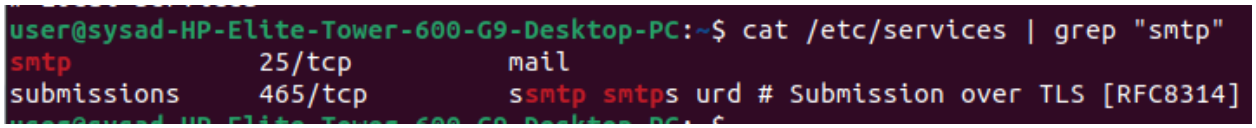
Domain name: mail.patriots.in
IP address of the mail server to which the client is requesting to send an email →74.53.140.153

3. **What is the source and destination port number of the SMTP connection between the client and the mail server? Does the destination port number match with the standard port of SMTP in `/etc/services/`?**



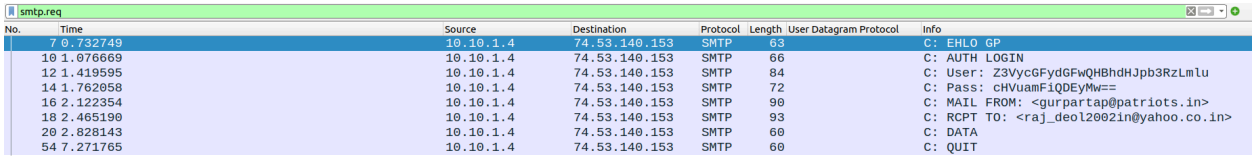
Source port: 1470

Destination port: 25



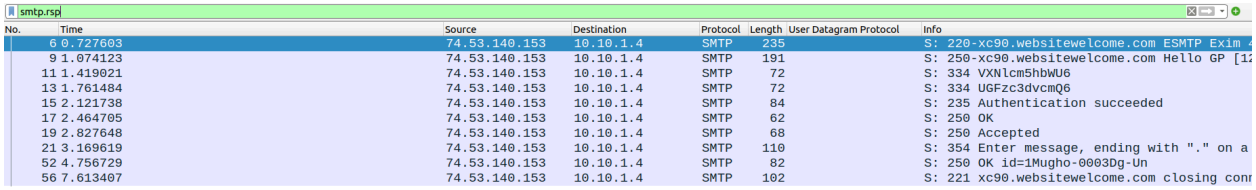
Yes, the destination port number matches the standard port of SMTP in /etc/services/ which is 25.

4. **Enumerate all SMTP commands sent by the client to the mail server, starting from the service ready response from the mail server until the connection is closed.**



- EHLO GP
- AUTH LOGIN
- User:
- Pass:
- MAIL
- RCPT
- DATA
- QUIT

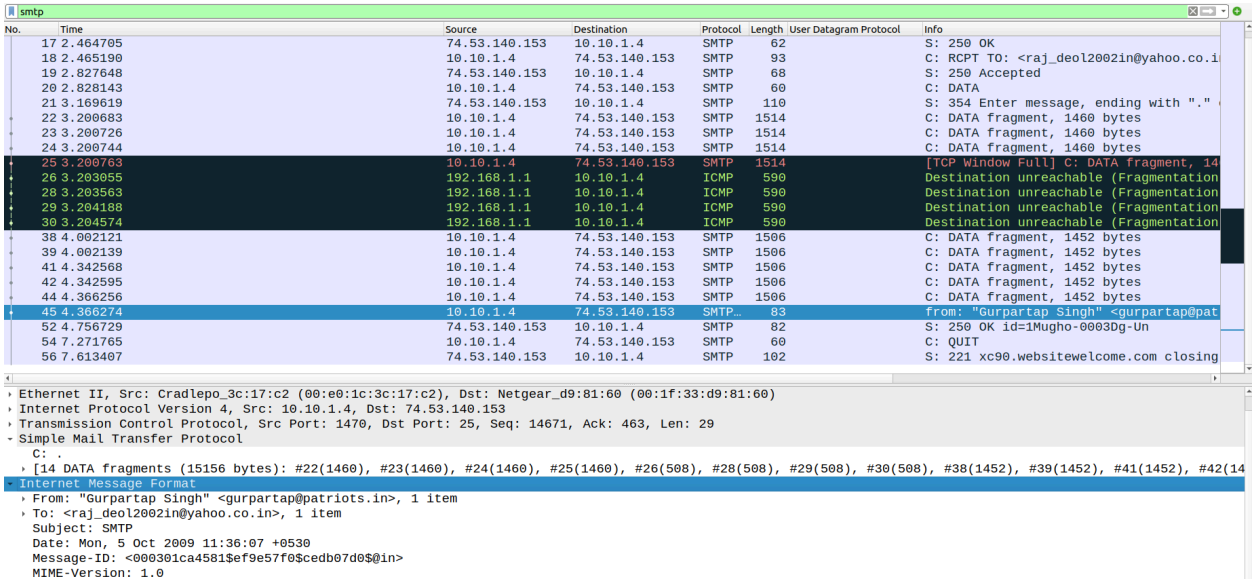
5. **Mention the different response codes that the mail server sends to the client for each of the SMTP commands. [Hint: Refer to section 3.2.2 in paper]**



SMTP Response Code	Meaning	Description

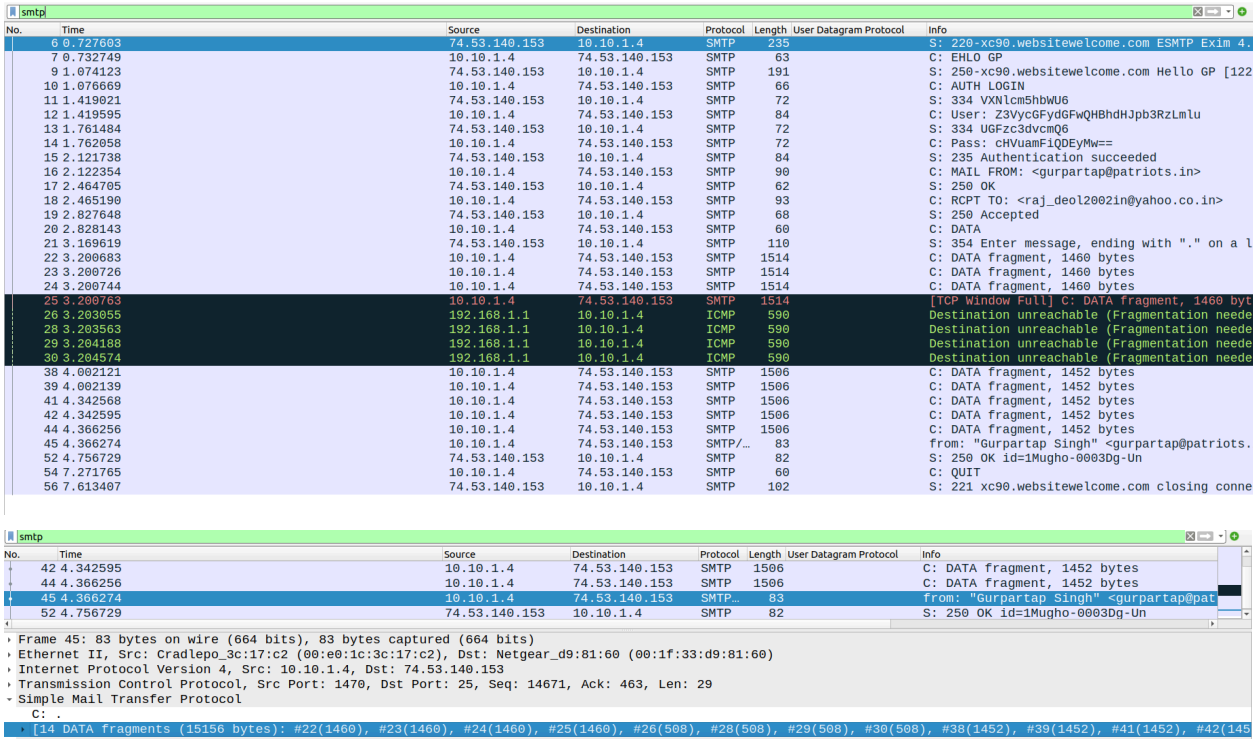
220	Server Ready	Indicates that the mail server is ready to accept connections. Sent as the first response when a client connects to the SMTP server. Typically followed by the client sending EHLO.
250	Command Successful	Confirms that the previous command was successfully processed. For EHLO, it indicates successful execution (e.g., `250-xc90.websitewelcome.com Hello GP [122.162.143.157]`).
334	Authentication Required	Server requests authentication credentials from the client. The response `"334 VXNlcm5hbWU6"` (Base64-encoded) translates to `"Username:"` and `"334 UGFzc3dvcmQ6"` translates to `"Password:"`.
235	Authentication Succeeded	Indicates that the client has successfully authenticated with the mail server, meaning the provided username and password were correct.
250 OK	Sender Accepted	After `MAIL FROM`, confirms that the sender's email address is accepted.
250 Accepted	Recipient Accepted	A variation of `250 OK`, confirming that the recipient's address is valid after the `RCPT TO` command.
354	Ready for Email Content	After the `DATA` command, signals the client to start sending the email body, including headers (e.g., `Subject, From, To`) and the message content. Ends with a single period (`.`) on a line by itself.
250 OK id=xyz	Email Queued for Delivery	Confirms that the email message has been successfully received and queued for delivery. The message ID (e.g., `id=1Mugho-0003Dg-Un`) helps track the email in the server queue.
221	Closing Connection	Indicates that the server is gracefully closing the connection after the client has sent the `QUIT` command. Both client and server terminate communication at this stage.

6. **Complete the entries of the 'Internet Message Format' in the table based on the observed reassembled data frame.**



Field Name	Value
FROM	“Gurpartap Singh”<gurpartap@patriots.in>
TO	raj_deol2002in@yahoo.co.in
Subject	SMTP
Date	Mon, 5 Oct 2009 11:36:07 +0530
Message ID	<000301ca4581$ef9e57f0$cedb07d0$@in>
MIME version	1.0

7. **What is the total size of the data transmitted from the client to the mail server? Mention the total number of data fragments and their byte size.**



smtp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
6	0.727603	74.53.140.153	10.10.1.4	SMTP	235		S: 220-xc90.websitewelcome.com ESMTP Exim 4.
7	0.732749	10.10.1.4	74.53.140.153	SMTP	63		C: EHLO GP
9	1.074123	74.53.140.153	10.10.1.4	SMTP	191		S: 250-xc90.websitewelcome.com Hello GP [122
10	1.076669	10.10.1.4	74.53.140.153	SMTP	66		C: AUTH LOGIN
11	1.419021	74.53.140.153	10.10.1.4	SMTP	72		S: 334 VXNlcm5hbWU6
12	1.419595	10.10.1.4	74.53.140.153	SMTP	84		C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72		S: 334 UGFzc3dvcmQ6
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72		C: Pass: cHVuamFiQDEyMw==
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84		S: 235 Authentication succeeded
16	2.122354	10.10.1.4	74.53.140.153	SMTP	90		C: MAIL FROM: <gurpartap@patriots.in>
17	2.464705	74.53.140.153	10.10.1.4	SMTP	62		S: 250 OK
18	2.465190	10.10.1.4	74.53.140.153	SMTP	93		C: RCPT TO: <raj_deol2002in@yahoo.co.in>
19	2.827648	74.53.140.153	10.10.1.4	SMTP	68		S: 250 Accepted
20	2.828143	10.10.1.4	74.53.140.153	SMTP	60		C: DATA
21	3.169619	74.53.140.153	10.10.1.4	SMTP	110		S: 354 Enter message, ending with "." on a l
22	3.200683	10.10.1.4	74.53.140.153	SMTP	1514		C: DATA fragment, 1460 bytes
23	3.200726	10.10.1.4	74.53.140.153	SMTP	1514		C: DATA fragment, 1460 bytes
24	3.200744	10.10.1.4	74.53.140.153	SMTP	1514		C: DATA fragment, 1460 bytes
25	3.200763	10.10.1.4	74.53.140.153	SMTP	1514		[TCP Window Full] C: DATA fragment, 1460 byt
26	3.203055	192.168.1.1	10.10.1.4	ICMP	590		Destination unreachable (Fragmentation neede
28	3.203563	192.168.1.1	10.10.1.4	ICMP	590		Destination unreachable (Fragmentation neede
29	3.204188	192.168.1.1	10.10.1.4	ICMP	590		Destination unreachable (Fragmentation neede
30	3.204574	192.168.1.1	10.10.1.4	ICMP	590		Destination unreachable (Fragmentation neede
38	4.002121	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
39	4.002139	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
41	4.342568	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
42	4.342595	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
44	4.366256	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
45	4.366274	10.10.1.4	74.53.140.153	SMTP/…	83		from: "Gurpartap Singh" <gurpartap@patriots.
52	4.756729	74.53.140.153	10.10.1.4	SMTP	82		S: 250 OK id=1Mugho-0003Dg-Un
54	7.271765	10.10.1.4	74.53.140.153	SMTP	60		C: QUIT
56	7.613407	74.53.140.153	10.10.1.4	SMTP	102		S: 221 xc90.websitewelcome.com closing conne

smtp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
42	4.342595	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
44	4.366256	10.10.1.4	74.53.140.153	SMTP	1506		C: DATA fragment, 1452 bytes
45	4.366274	10.10.1.4	74.53.140.153	SMTP…	83		from: "Gurpartap Singh" <gurpartap@pat
52	4.756729	74.53.140.153	10.10.1.4	SMTP	82		S: 250 OK id=1Mugho-0003Dg-Un

```
Frame 45: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
Ethernet II, Src: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60)
Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 14671, Ack: 463, Len: 29
Simple Mail Transfer Protocol
    C: .
  [14 DATA fragments (15156 bytes): #22(1460), #23(1460), #24(1460), #25(1460), #26(508), #28(508), #29(508), #30(508), #38(1452), #39(1452), #41(1452), #42(145
```

[14 DATA fragments (15156 bytes): #22(1460), #23(1460), #24(1460), #25(1460), #26(508), #28(508), #29(508), #30(508), #38(1452), #39(1452), #41(1452), #42(1452), #44(1452), #45(24)]

Total number of data fragments: 14

Byte sizes of fragments:

1460 (×4)+508 (×4)+ 1452 (×4)+24 (×1)=5840+2032+5808+24=15156 bytes

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).