NETWORKING AND SECURITY

LAB - 2

Submitted by – **Kartik Attri**

Submitted To – **Dr. Shaoquan Jiang**

Student Number – **110091738**

Question 1-

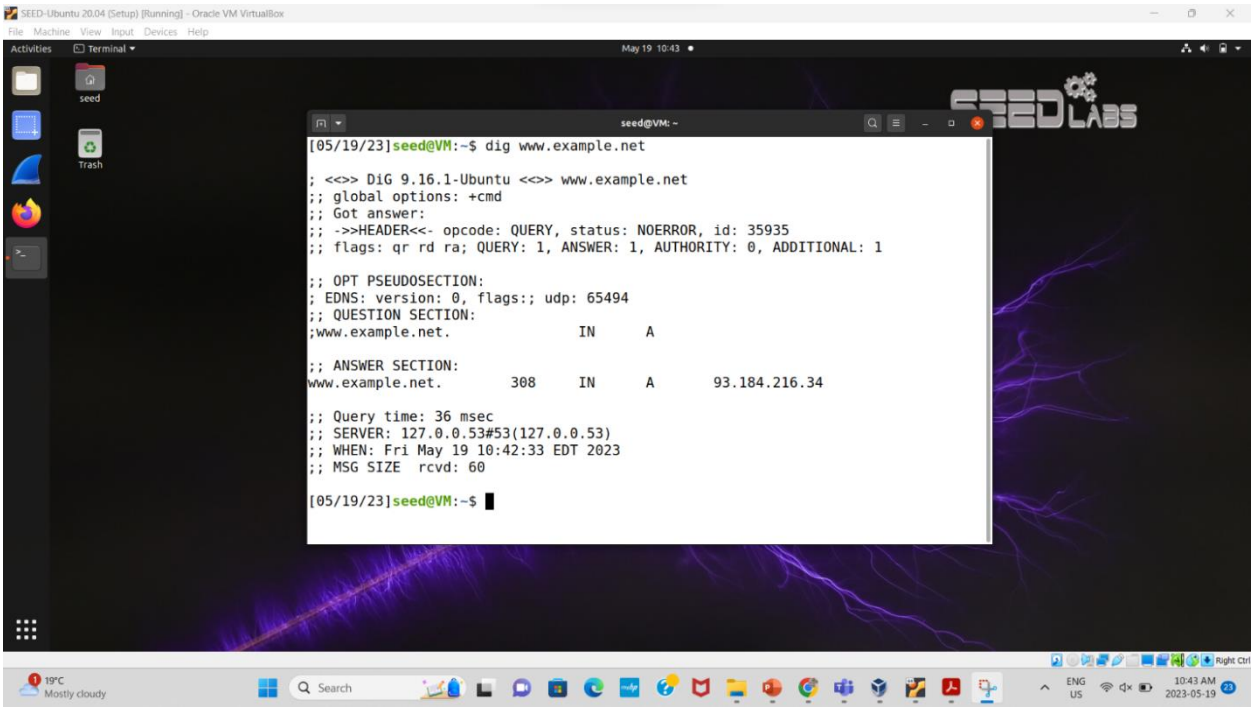
Part A

Command dig is used to find the IP address of a hostname such as www.google.com. To do

this, you can simply run dig www.google.com. This is the result returned by your local DNS server when you run dig command to request it to find out the IP address of www.google.com. Question section is to repeat your question and A stands for the record of IP address. We can see that www.google.com has an IP address 172.217.1.164.

Answer-

Ip address of www.example.net = 93.184.216.34



Part B

run Wireshark on your VM, then $ dig www.example.net and stop wireshark. Look at the

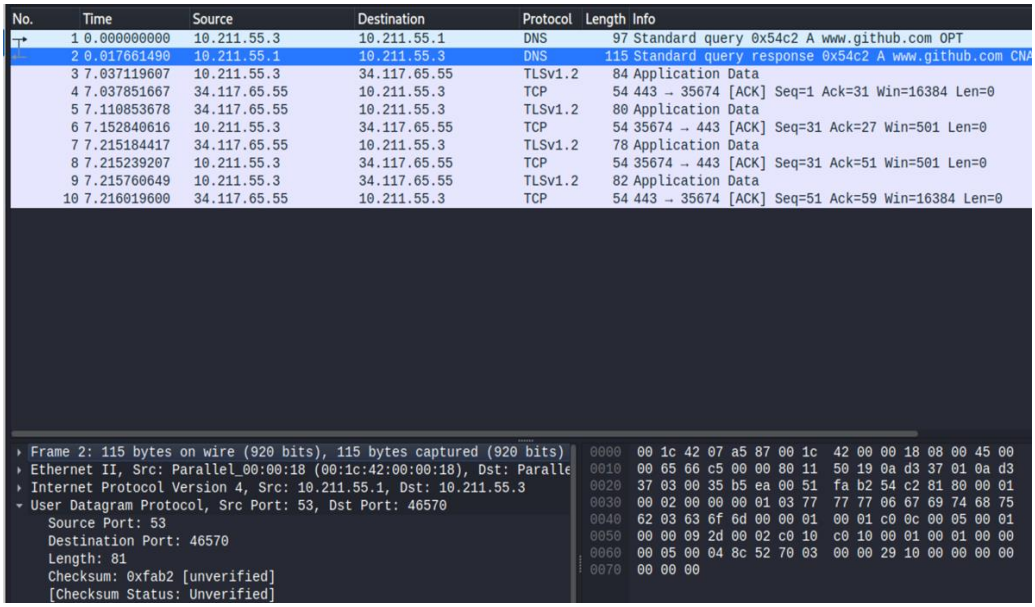
DNS request packet (using filter DNS to find it easily), confirm that the transport layer protocol

is UDP. What are the values of this UDP header (you need to first check the header fields

learned in class)?

Note: You might need to clear the DNS cache, using $ sudo systemd-resolve - - flush-caches

Answer-



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.211.55.3	10.211.55.1	DNS	97	Standard query 0x54c2 A www.github.com OPT
2	0.017661490	10.211.55.1	10.211.55.3	DNS	115	Standard query response 0x54c2 A www.github.com CNA
3	7.037119607	10.211.55.3	34.117.65.55	TLSv1.2	84	Application Data
4	7.037851667	34.117.65.55	10.211.55.3	TCP	54	443 → 35674 [ACK] Seq=1 Ack=31 Win=16384 Len=0
5	7.110853678	34.117.65.55	10.211.55.3	TLSv1.2	80	Application Data
6	7.152840616	10.211.55.3	34.117.65.55	TCP	54	35674 → 443 [ACK] Seq=31 Ack=27 Win=501 Len=0
7	7.215184417	34.117.65.55	10.211.55.3	TLSv1.2	78	Application Data
8	7.215239207	10.211.55.3	34.117.65.55	TCP	54	35674 → 443 [ACK] Seq=31 Ack=51 Win=501 Len=0
9	7.215760649	10.211.55.3	34.117.65.55	TLSv1.2	82	Application Data
10	7.216019600	34.117.65.55	10.211.55.3	TCP	54	443 → 35674 [ACK] Seq=51 Ack=59 Win=16384 Len=0

```
Frame 2: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Paralle
Internet Protocol Version 4, Src: 10.211.55.1, Dst: 10.211.55.3
User Datagram Protocol, Src Port: 53, Dst Port: 46570
    Source Port: 53
    Destination Port: 46570
    Length: 81
    Checksum: 0xfab2 [unverified]
    [Checksum Status: Unverified]
```

```
0000  00 1c 42 07 a5 87 00 1c  42 00 00 18 08 00 45 00
0010  00 65 66 c5 00 00 80 11  50 19 0a d3 37 01 0a d3
0020  37 03 00 35 b5 ea 00 51  fa b2 54 c2 81 80 00 01
0030  00 02 00 00 00 01 03 77  77 77 06 67 69 74 68 75
0040  62 03 63 6f 6d 00 00 01  00 01 c0 0c 00 05 00 01
0050  00 00 09 2d 00 02 c0 10  c0 10 00 01 00 01 00 00
0060  00 05 00 04 8c 52 70 03  00 00 29 10 00 00 00 00
0070  00 00 00
```

Values in UDP header-:

Source port: 53

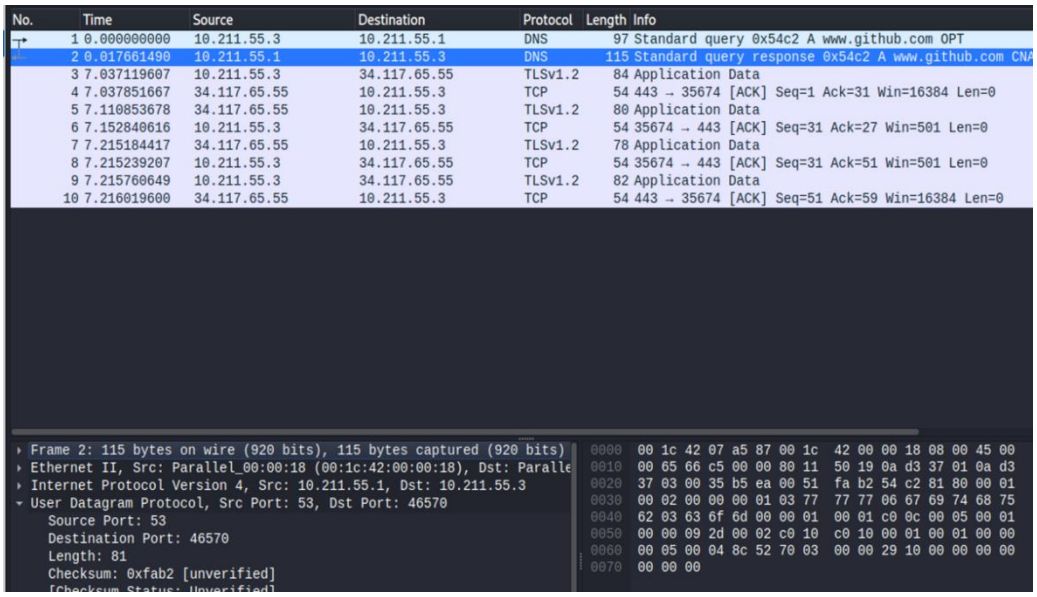
Destination Port: 46570

Length: 81

Part C

In the DNS request packet in step b, the destination IP is your local DNS server's IP. What is this value? As said, DNS is serviced by UDP and has no connection setup before sending DNS request. You can confirm this by checking that there is no any packet in Wireshark exchanged between your VM and local DNS server, prior to the DNS request packet (show the screen shot of the window of Wireshark for the list of packets).

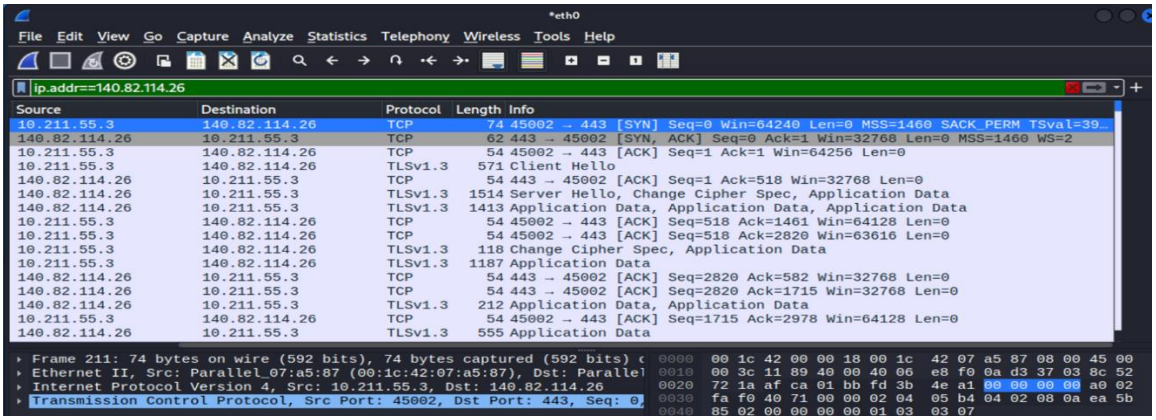
Answer- As in below screenshot we can see that there is no exchange of packets which confirm that's it's UDP ,



Question 2-

Run Wireshark and then access www.example.net using Firefox (you might need to clear the browser history). Then stop the Wireshark. Check your list of packets in Wireshark window, filtered by the ip address of www.example.net. You can see that before the HTTP request to www.example.net, there is a connection stage with three packets: SYN packet, SYN-ACK packet and ACK packet. This is to provide the connection setup between your VM and www.example.net. Confirm this. Also, confirm that the transport layer protocol in these packets (check one of them is good enough) is TCP. When the message exchange starts, you can see ACK packet. This is to confirm the receipt of a packet. Find out such a packet. This is to find a packet with flags bit A=1. This provides an evidence that TCP is a reliable protocol. This is different from the UDP protocol. ACK packet might or might not contain the application data. Verify the ACK packet you consider (any of them is ok) to see if it contains application data.

Answer 2-



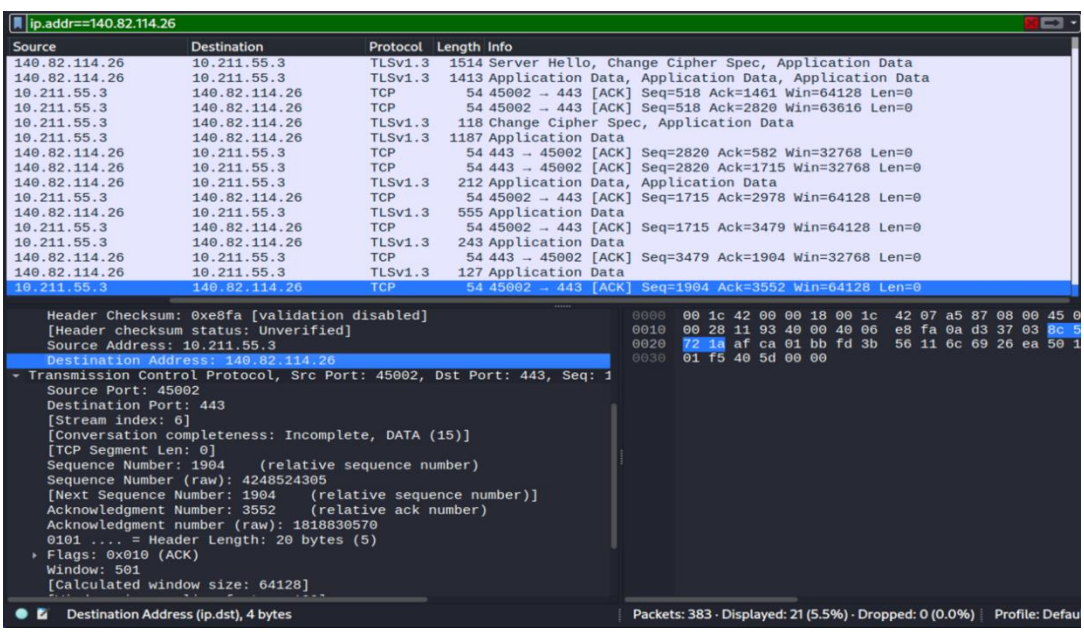
Question 3-

Run Wireshark and access www.example.net and then close your webpage and stop your Wireshark. Answer the following questions: -

Part A

Find out the first packet from your VM to www.example.net (you should know the ip address of www.examplenet now). This should be the SYN-packet (i.e., the first packet of the 3-way handshake protocol). What is source port # and destination port #? Confirm that they are in the TCP header in the Wireshark packet window. What is source IP and destination IP? Confirm that they are in the ip header in the Wireshark packet window?

Answer –

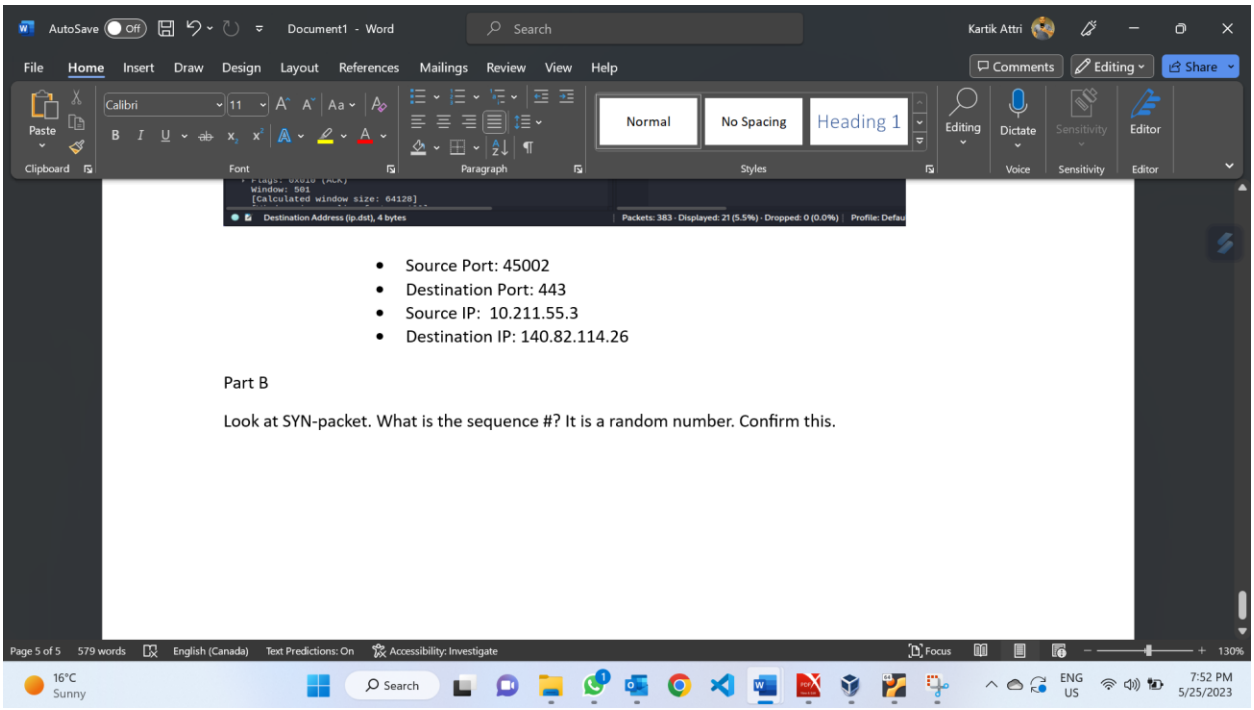


- Source Port: 45002
- Destination Port: 443
- Source IP: 10.211.55.3
- Destination IP: 140.82.114.26

Part B

Look at SYN-packet. What is the sequence #? It is a random number. Confirm this?

Answer - Sequence #: 4248522402

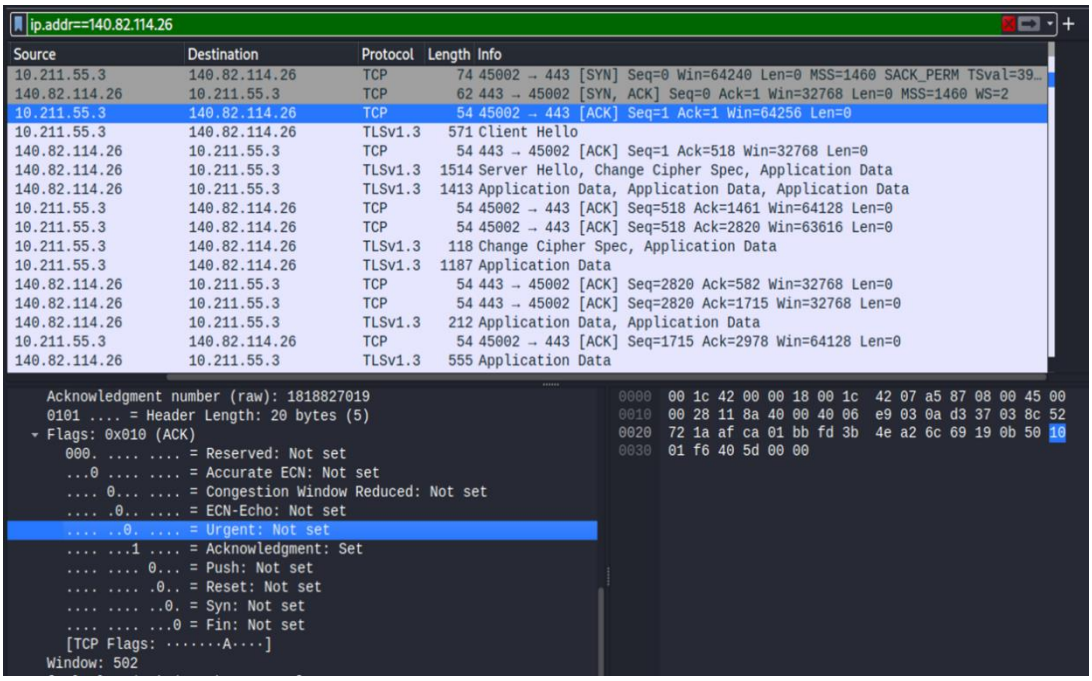


Part C

Find out in the TCP header the flag bits U|A|P|R|S|F in the SYN-ACK packet

Answer –

Flag A = 1

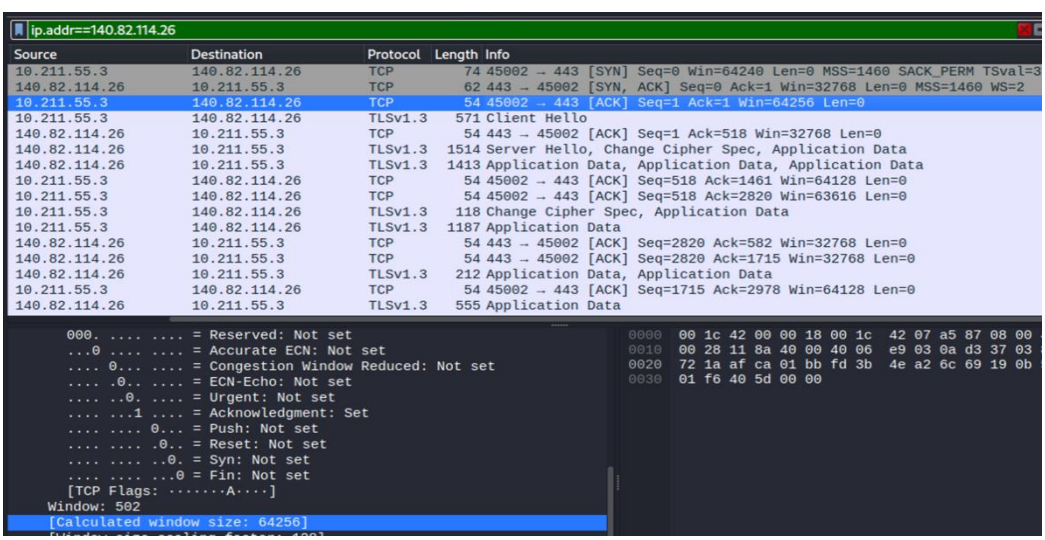


Part D

The receive window field is to tell its partner the current **receive-buffer** size it has. Find out the window size of SYN-ACK packet and that of http response packet. Are they equal?

Answer –

Window Size: 64256
Http Window size: 64256

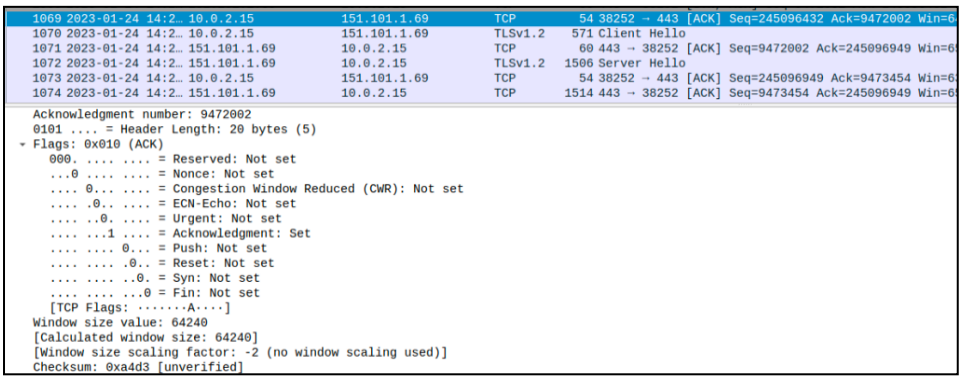


Part E

Find out the sequence # of http request packet and its payload size (the **segment len** is the payload size). The next sequence # is the sum of these two numbers. Verify that this is indeed the sequence # of the next packet sent by your VM (I used Different MAchine)?

Answer – Sequence Number: + TCP Segment len = next Sequence number

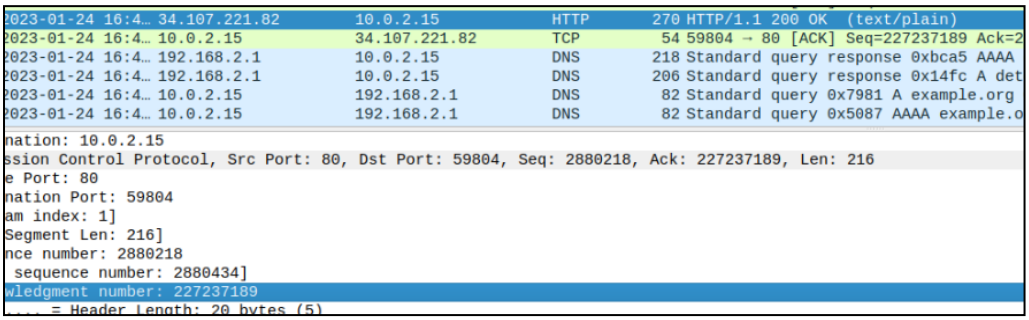
227236893 + 296
227237189



Part F

Find out the acknowledgement # in http response packet. Is this the same as the next sequence # you calculated above for the request packet? Explain why?

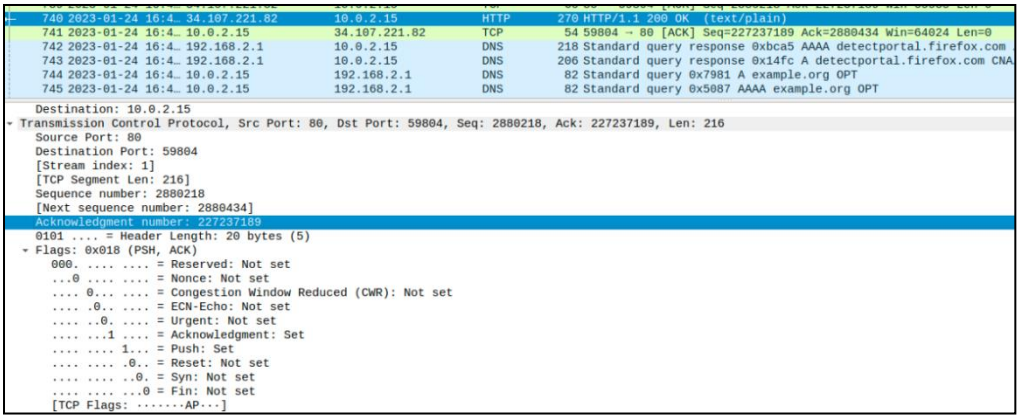
Answer -



Part G

What is the flags bits U|A|P|R|S|F in the http response packet?

Answer -



Part H

Find out the packet your VM requests to terminate the TCP connection. This packet will be sent when you close the webpage. What is the flags bit U|A|P|R|S|F in this packet?

Answer -