VENNELA G

20BDS0146

INFORMATION SECURITY MANAGEMENT

LAB ASSIGNMENT 1

SLOT L37+L38

Analysis of Network using Wireshark:

Q. Analyse the layered structure of network protocols using a web browsing example.

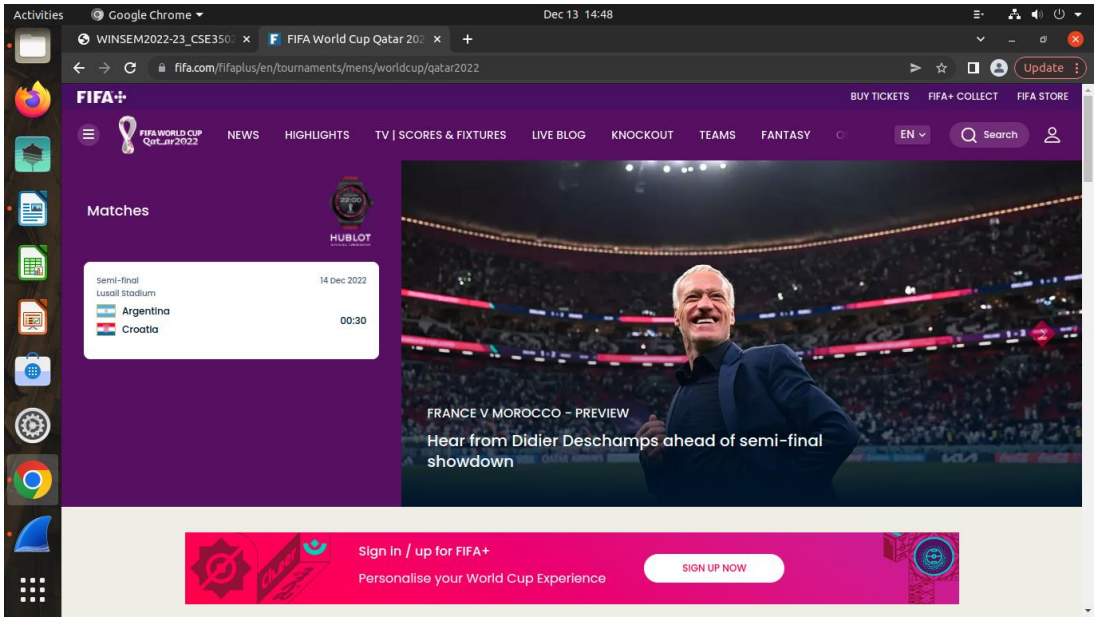
Examine the header structure of the PDUs at the data link, IP, transport, and application layers. In particular, how addresses and port numbers work together to enable end-to- end applications.

Protocols to Examine:
- **Ethernet and IP addressing**
- **DNS Query and Response**
- **TCP three-way handshake, sequence, and ACK numbering**
- **HTTP GET and Response messages**

Protocol Analysis Questions

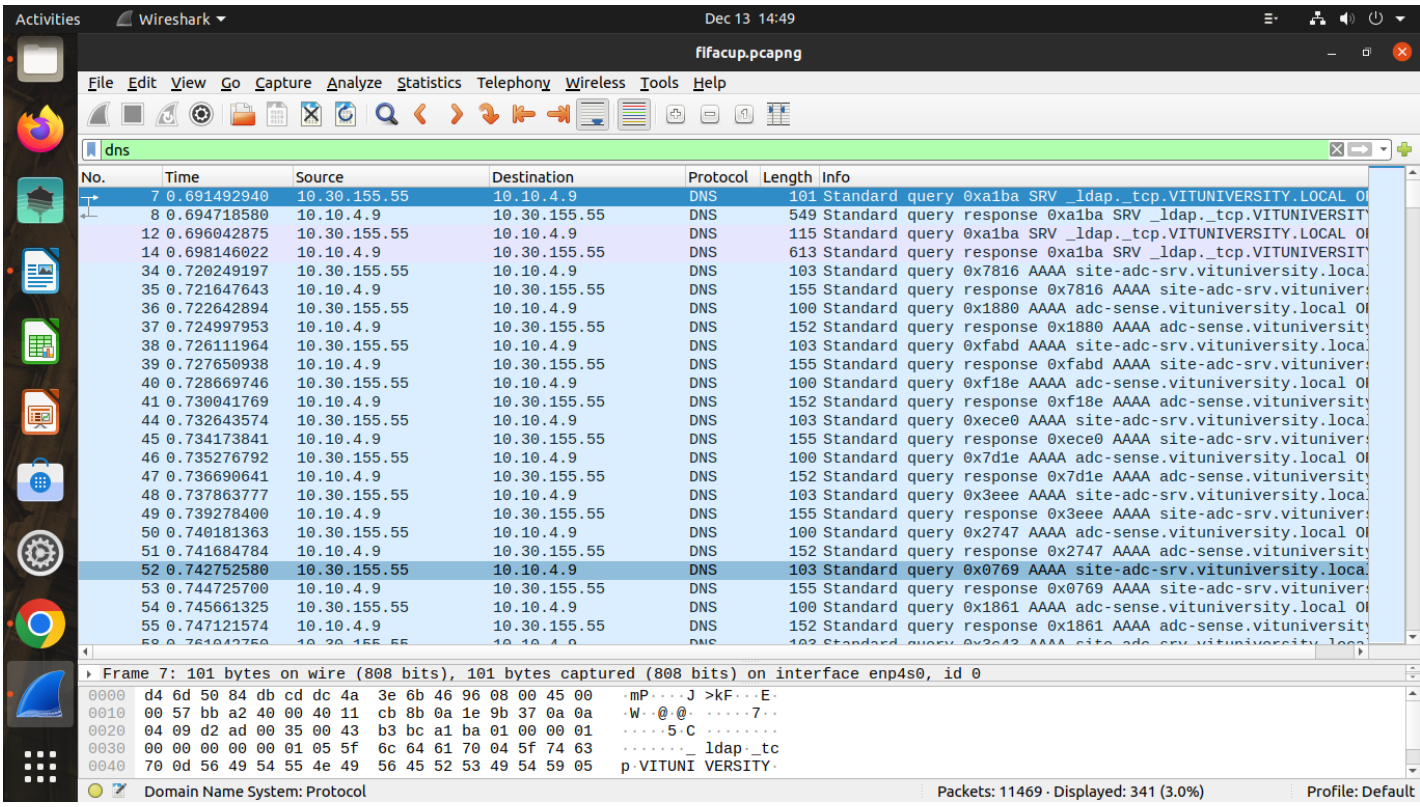
To begin with this, we have captured the packets using Wireshark by visiting the website: fifa.com and the captured file was saved.

1. Protocols Capture: To ensure if we have captured DNS, TCP, and HTTP packets, we use the filter options from Wireshark as shown below.



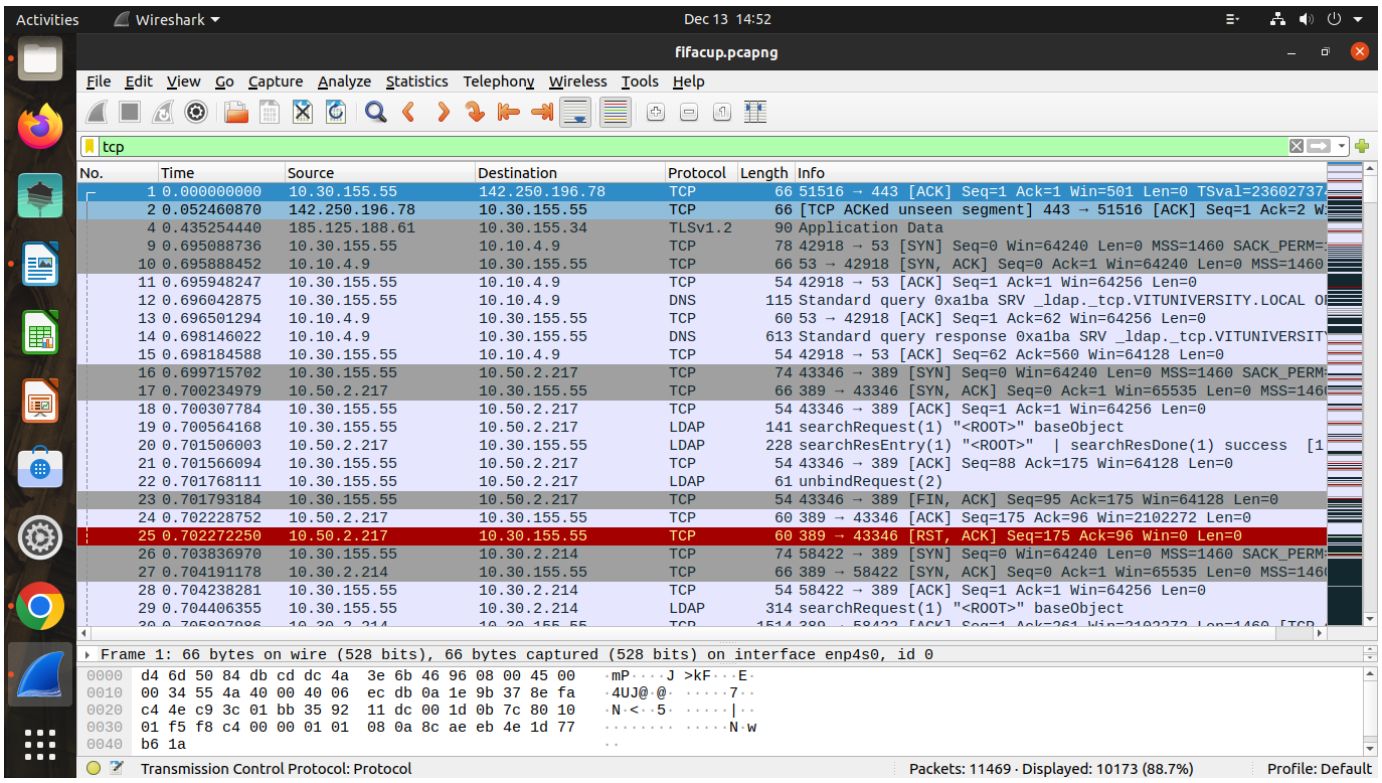
a. DNS packets:

Using DNS filter

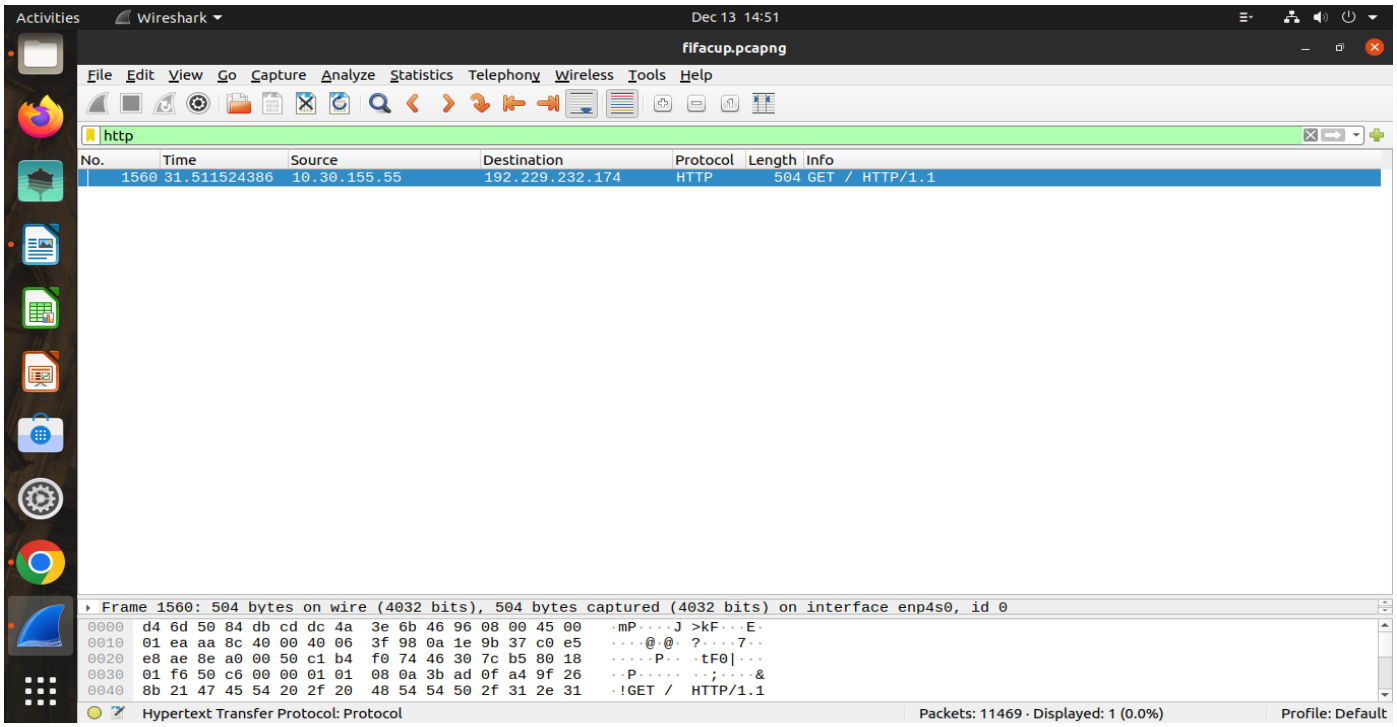


b. TCP packets:

Using TCP filter

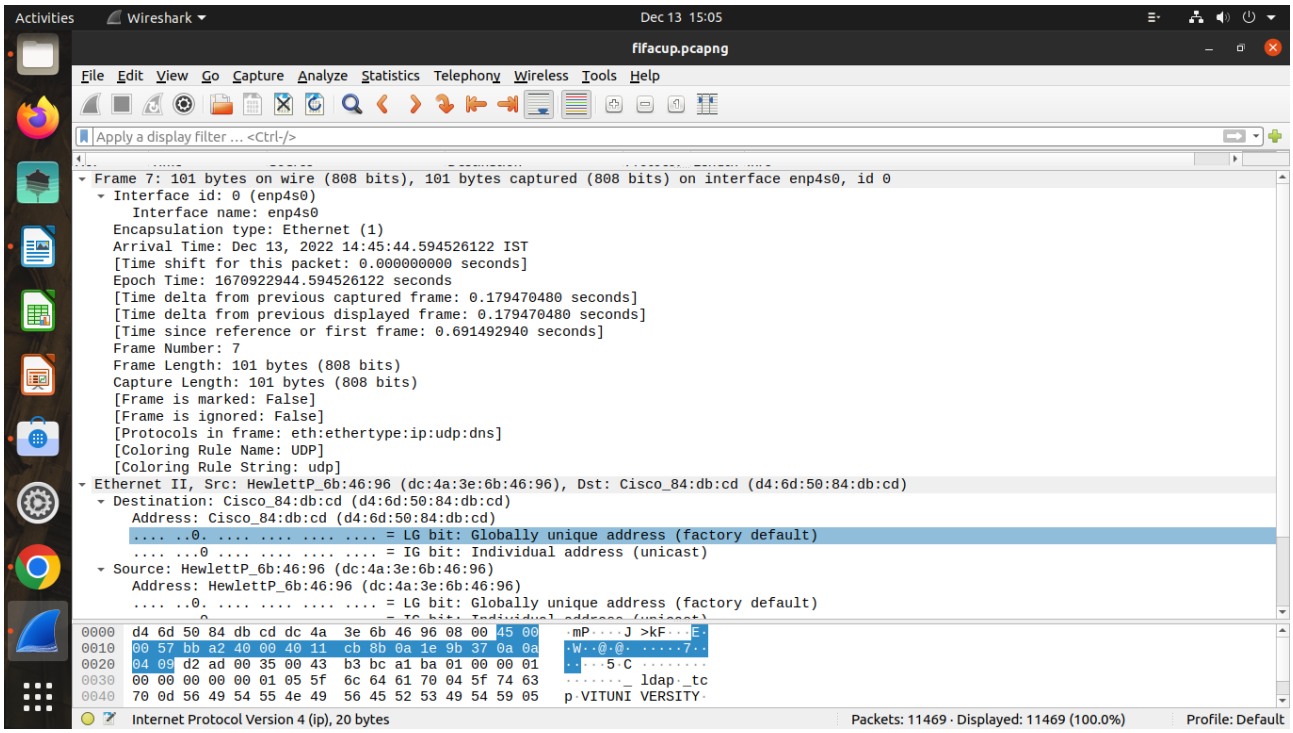


c. HTTP packets:



2. Ethernet frame, IP packet, and UDP datagram:

i. Examine the frame for the first DNS packet sent by the client



b. By examining protocols, we found the client's Ethernet: HewlettP_6b:46:96 (dc:4a:3e:6b:46:96)

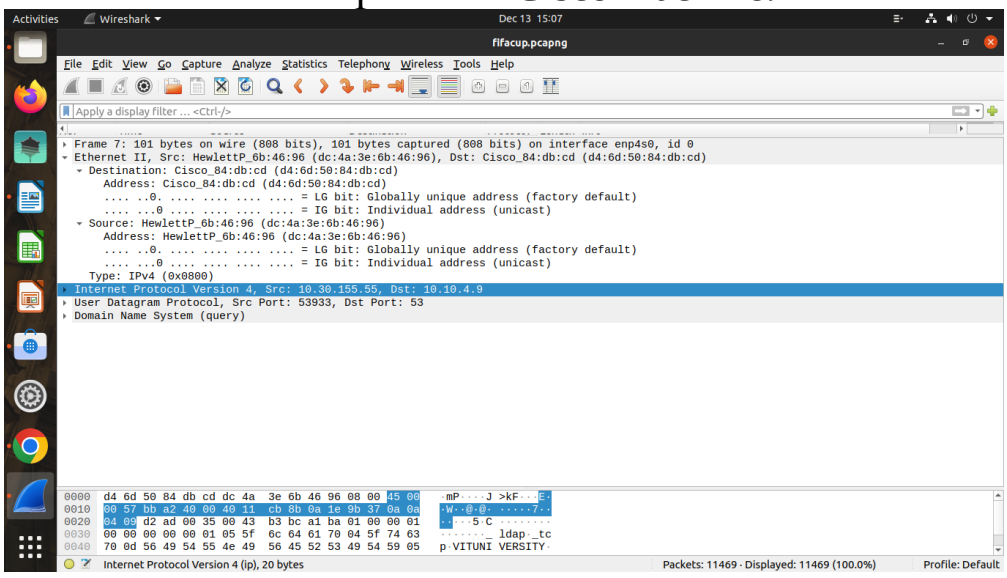
c. Content of type field in Ethernet Frame: IPv4

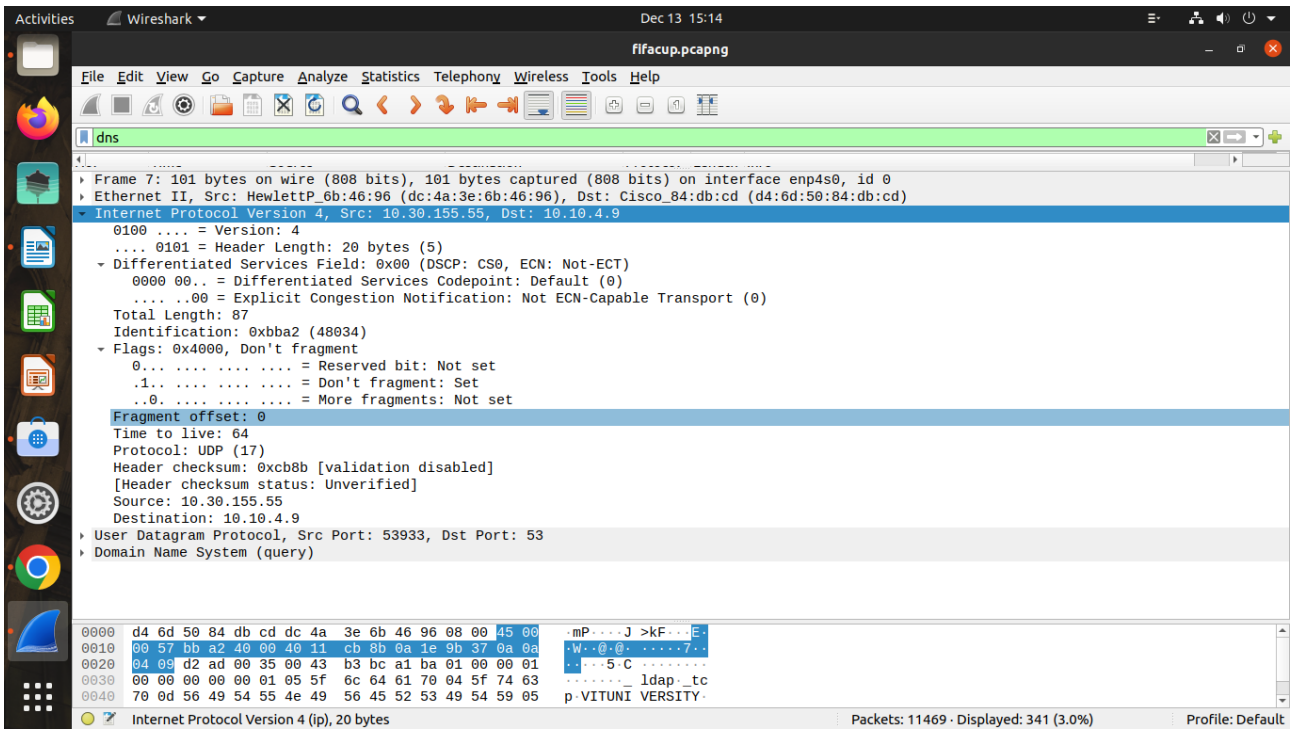
d. Destination:

i. Ethernet: Cisco_84:db:cd (d4:6d:50:84:db:cd)

ii. IP: 10.10.4.9

Destination's Ethernet corresponds to Cisco machine.



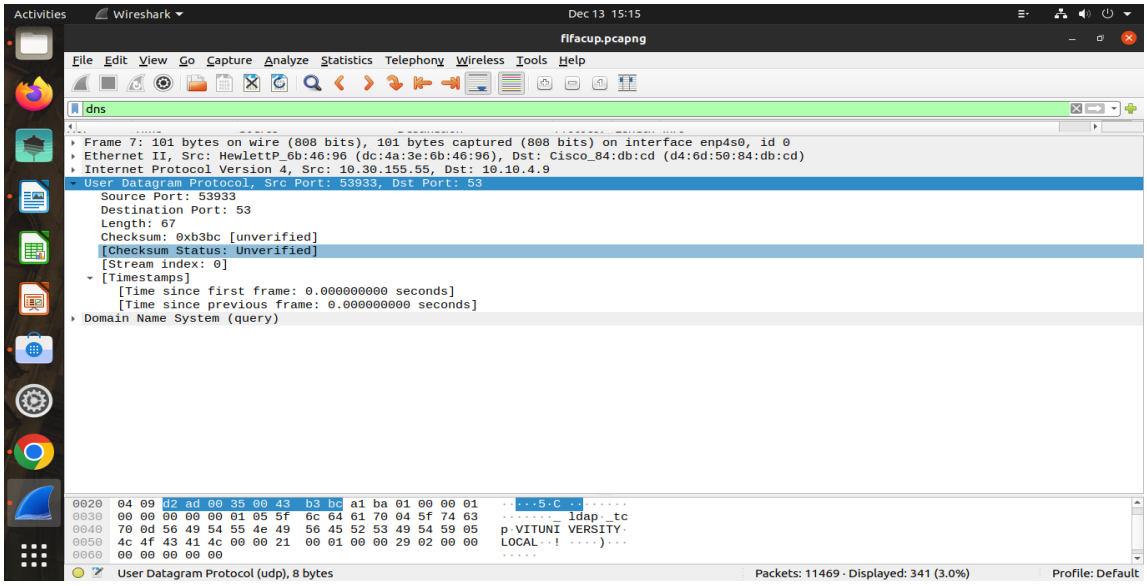


ii. Examine the IP header for the first DNS packet sent by the client

a. Header Length = 20 bytes and Total Length = 87
b. Protocol Type field = UDP (User Datagram Protocol) (17)
Type of protocol in payload = UD

iii. Examine the UDP header of the first DNS packet sent by the client

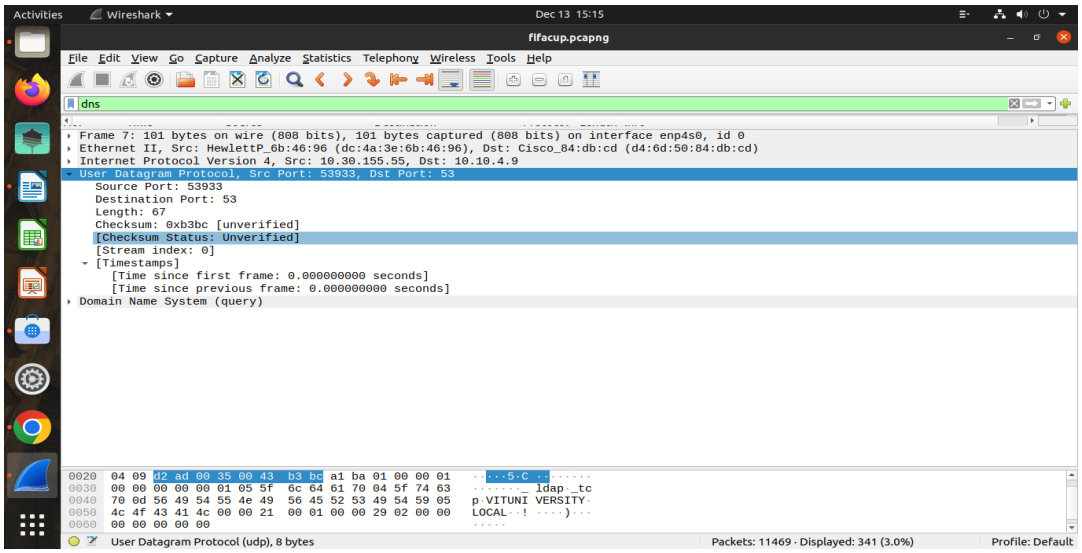
a.



Client Port = 53933
Server Port = 53

HTTP as an application layer protocol in payload.

b. If we see the DNS packets, we can conclude that Header Length of IP remains constant for any of the DNS packet sent. Below image is the second DNS packet sent by the client.



3. DNS

Examine the DNS query message in the DNS packet sent by the client.

a. What field indicates whether the message is query or a response?

If Queries field is only present in DNS packet, then we can say the message is query and if there is Queries along with Answers field then we can say that message is a response message.

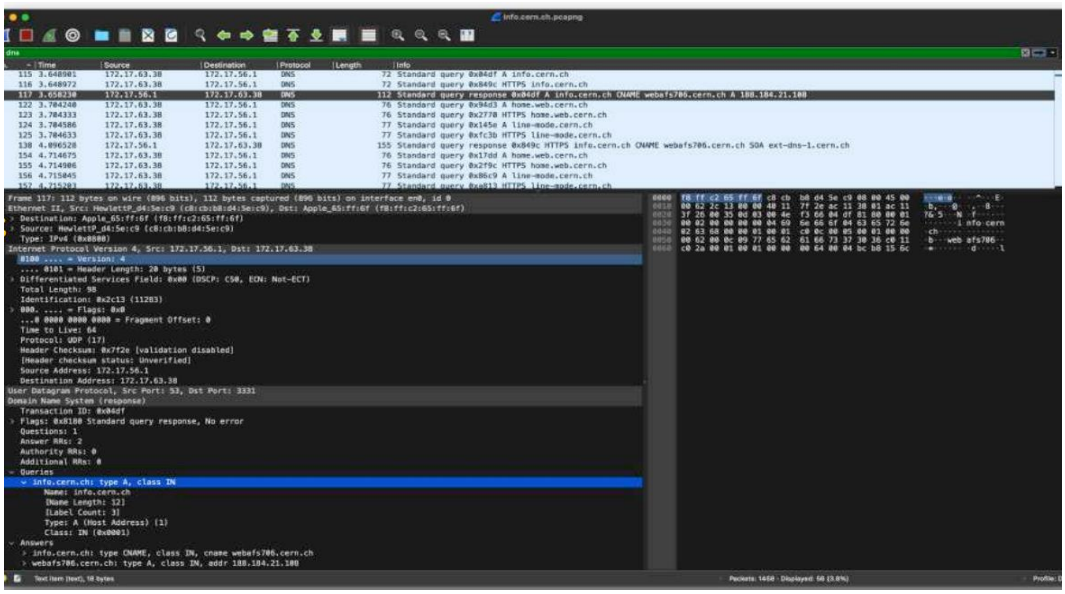
b. What information is carried in the body of the query?

Information such as Domain Name, Name Length, Type and Class is present in the body of the query.

c. What is the query transaction ID?

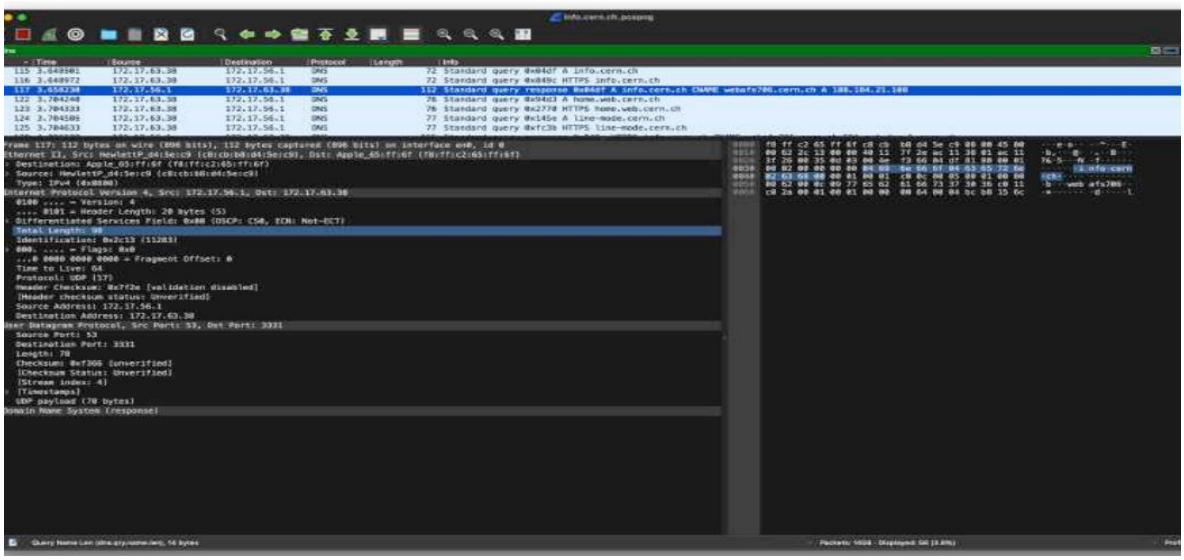
The query transaction ID is a 16-bits random value chosen by the client. When a client sends a question to a DNS server, it remembers the question and its identifier. When a server returns an answer, it returns in the Transaction ID field the identifier chosen by the client. With this client can match the received answer with the question that it sent.

d. Identify the fields that carry the type and class of the query.
Ans: The Queries field in DNS carries the type and class of the query.
Consider the packet that carries the DNS response to the above query.
a. What should the Ethernet and IP addresses for this packet be? Verify that these addresses are as expected.
In case of source, the Ethernet and IP addresses for this packet should be the server's system addresses. And in case of destination, client's system Ethernet and IP addresses should be there. The below shown screenshot verifies that:



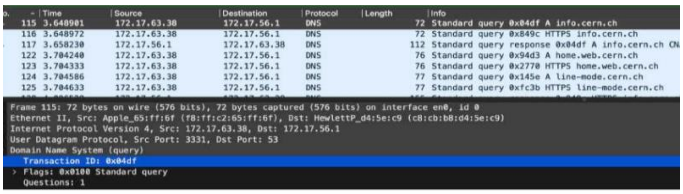
Ethernet:
Source: Cisco_84:db:cd (d4:6d:50:84:db:cd)
Destination: HewlettP_6b:46:96 (dc:4a:3e:6b:46:96)
IP:
Source: 10.10.4.9
Destination: 10.30.155.55

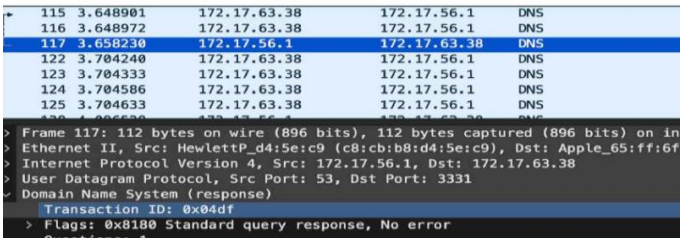
b. What is the size of the IP packet and UDP datagram that carry the response? Is it longer than the query?
The size of the IP packet and UDP datagram that carry the response varies from the query.
Response:



IP packet length: 87 bytes
UDP datagram packet length: 67 bytes.
Yes, the IP packet and UDP datagram for the response has longer length than that of query.

c. Confirm that the transaction ID in the response message is correct.
The transaction ID for the response is 0x04df and that of query is also same. Hence, it is correct.

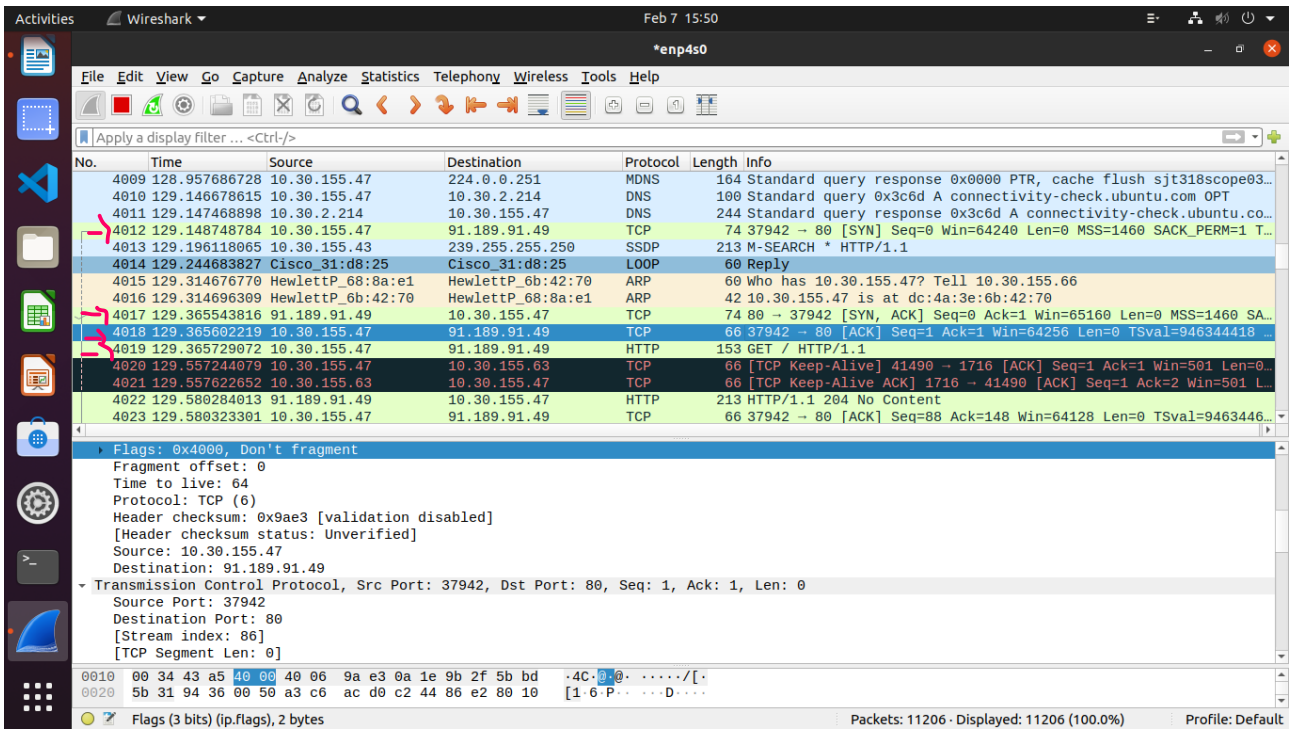




d. How many answers are provided in the response message? Compare the answers and their time-to-live values.
There are two answers in the response message.
Fifa.com- 98 sec (1min, 38 sec)
Fifaplustournaments.com- 100 sec (1min, 40 sec)

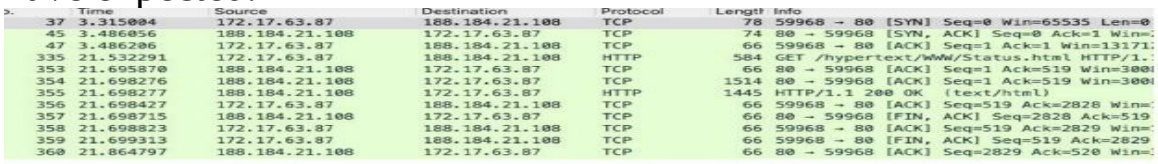
4. TCP three-way handshake

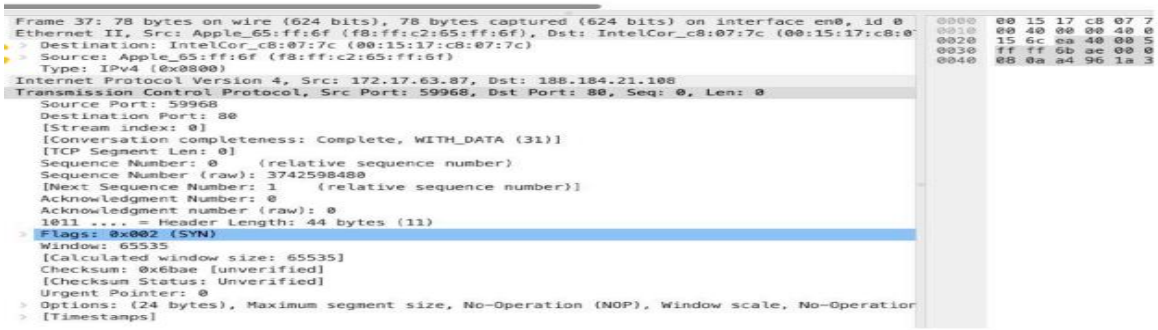
• *Identify the frame that carries the first TCP segment in the three-way handshake that sets up the connection between the http client and server.*



a. What source Ethernet and IP addresses do you expect in this segment? What protocol and type fields do you expect in the first segment? Confirm that these addresses are as expected.

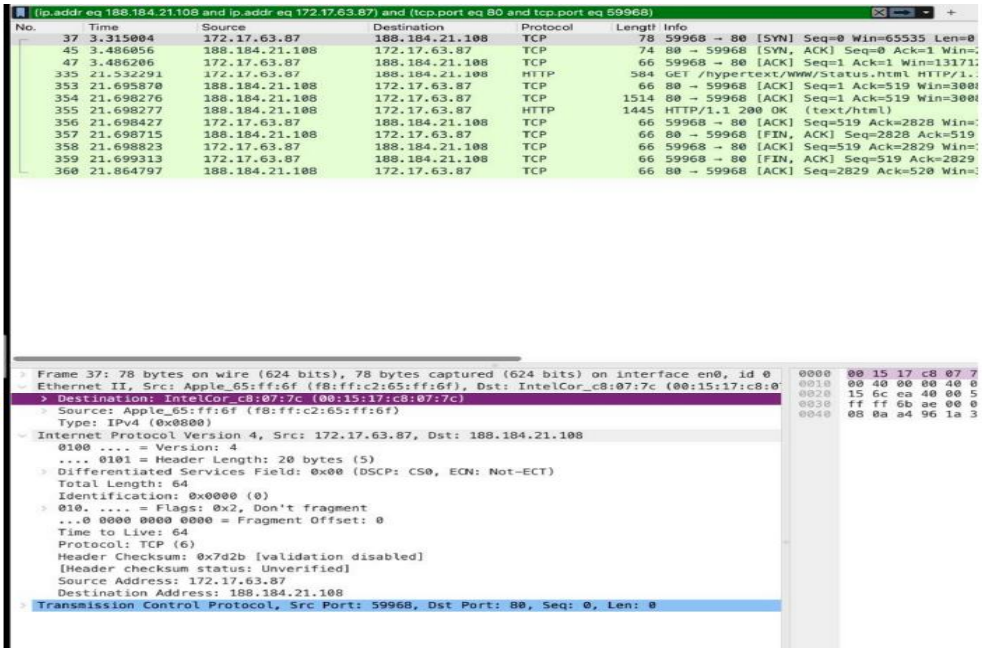
The client's ethernet and IP address would be there. There would be IP and TCP protocol present in segment. The following image verifies what we have expected.





b. *Explain the values in the destination Ethernet and IP addresses in the first segment? To what machines these addresses correspond?*

The destination system has the name (IntelCor_c8:07:7c) with mac address as (00:15:17:c8:07:7c) and IP address as 188.184.21.108

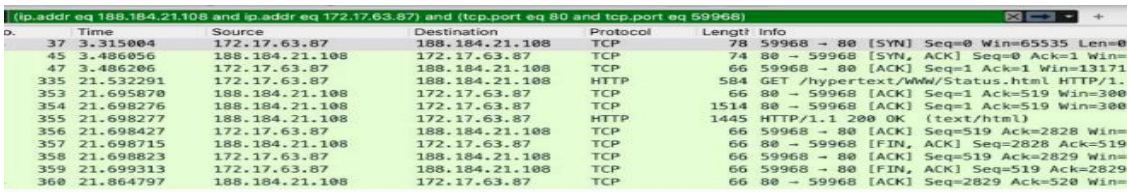


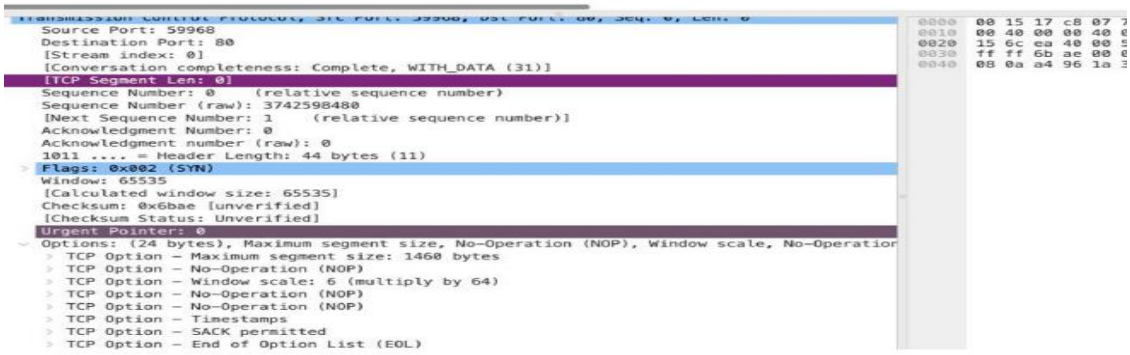
c. Identify the ephemeral port number used by the client and confirm that the well-known port number is the correct value for HTTP.

The ephemeral port number used by client is 59968. The well-known port number for HTTP is from 0 – 1023.

d. What is the length of the TCP segment?

The TCP segment length is zero.



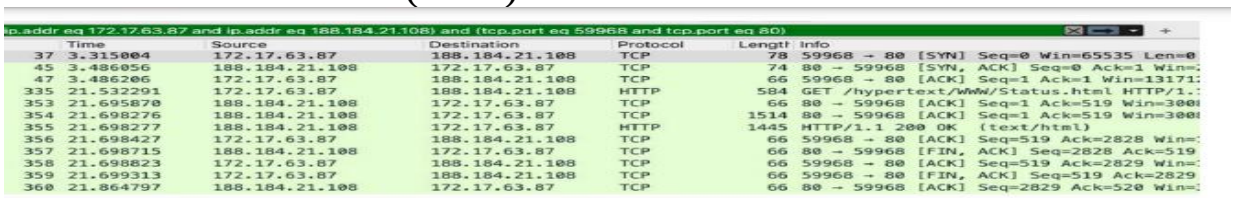


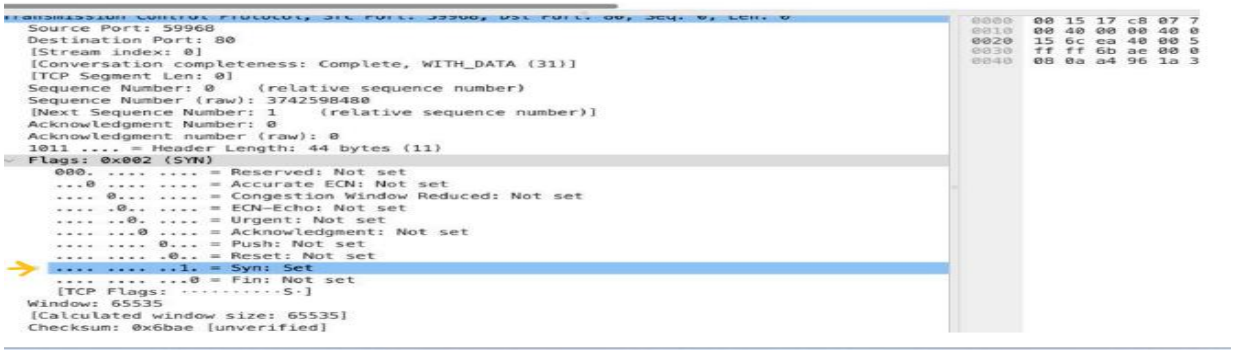
e. *What is the initial sequence number for the segments from the client to the server? What is the initial window size? What is the maximum segment size?*

The initial sequence number for the segments from the client to the server is 0. Initial window size = 65535 Maximum segment size = 1460 bytes

f. Find the hex character that contains the SYN flag bit.

Hex character = 0x002 (SYN)





• **Identify the frame that carries the second segment in the three-way handshake.**

a. How much time elapsed between the capture of the first and second segments?

The total of 18 sec (approx.) is elapsed between the first and second segment.

b. Before examining the captured packets, specify the values for the following fields in this frame:

• *Source and destination addresses and type field in Ethernet frame.*

Source: Apple_65:ff:6f (f8:ff:c2:65:ff:6f) Destination: IntelCor_c8:07:7c (00:15:17:c8:07:7c) Type: IPv4 (0x0800)

• *Source and destination IP addresses and port numbers in IP packet.*

Source Address: 172.17.63.87 Destination Address: 188.184.21.108

Source Port number = 59968 Destination Port number = 80

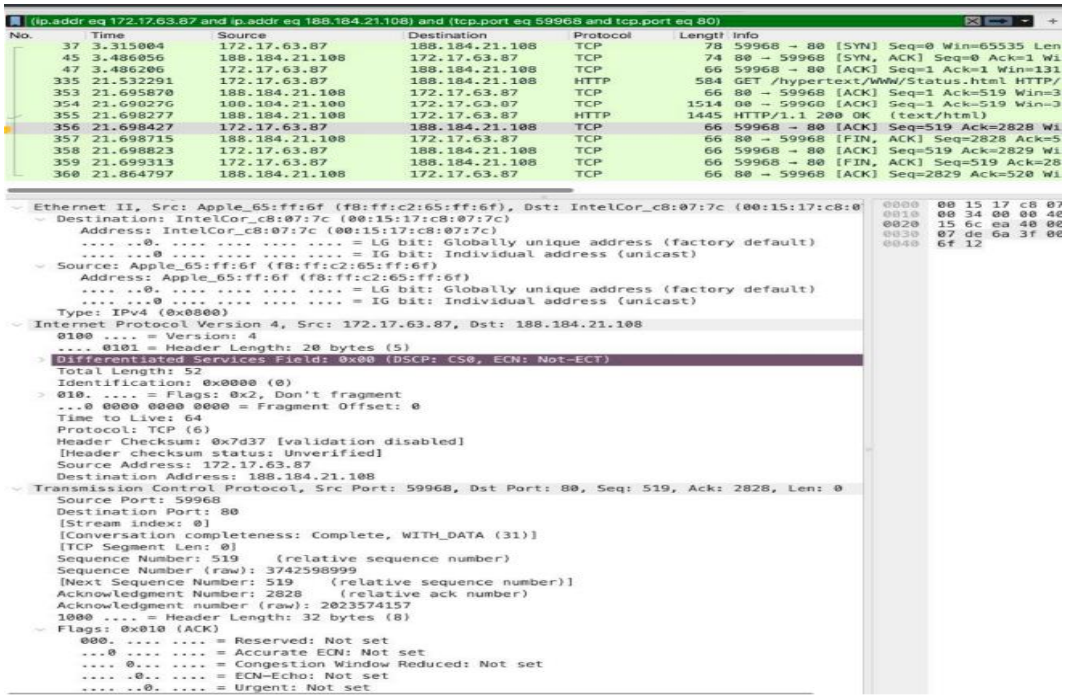
• *Acknowledgement number in TCP segment.*

Acknowledgment Number: 2828 (relative ack number)

• *Values of flag bits.*

In flag bits, Acknowledgment bit is only set

• *Confirm that the frame contains the expected values.*



c. What is the length of the TCP segment?

The length of TCP segment is zero

d. What is the initial sequence number for the connection from the server to the client? What is the maximum segment size?

Initial sequence number from server to client: 2828 (relative sequence number) Maximum segment size = 1460 bytes

5. HTTP GET

• **Identify the frame that carries the HTTP "GET" message.**

a. Confirm that the sequence and acknowledgement values in the TCP header are as Expected

Sequence Number = 1 Acknowledgment Number = 1

b. Examine the flag bits in the TCP header. Can you explain why the two flag bits are set?

The Acknowledgment (ACK) and Push (PSH) in flags bits are set. When ACK bit is set, it contains the value of the next sequence number the sender of the packet is expecting to receive. When PSH bit is set, it is

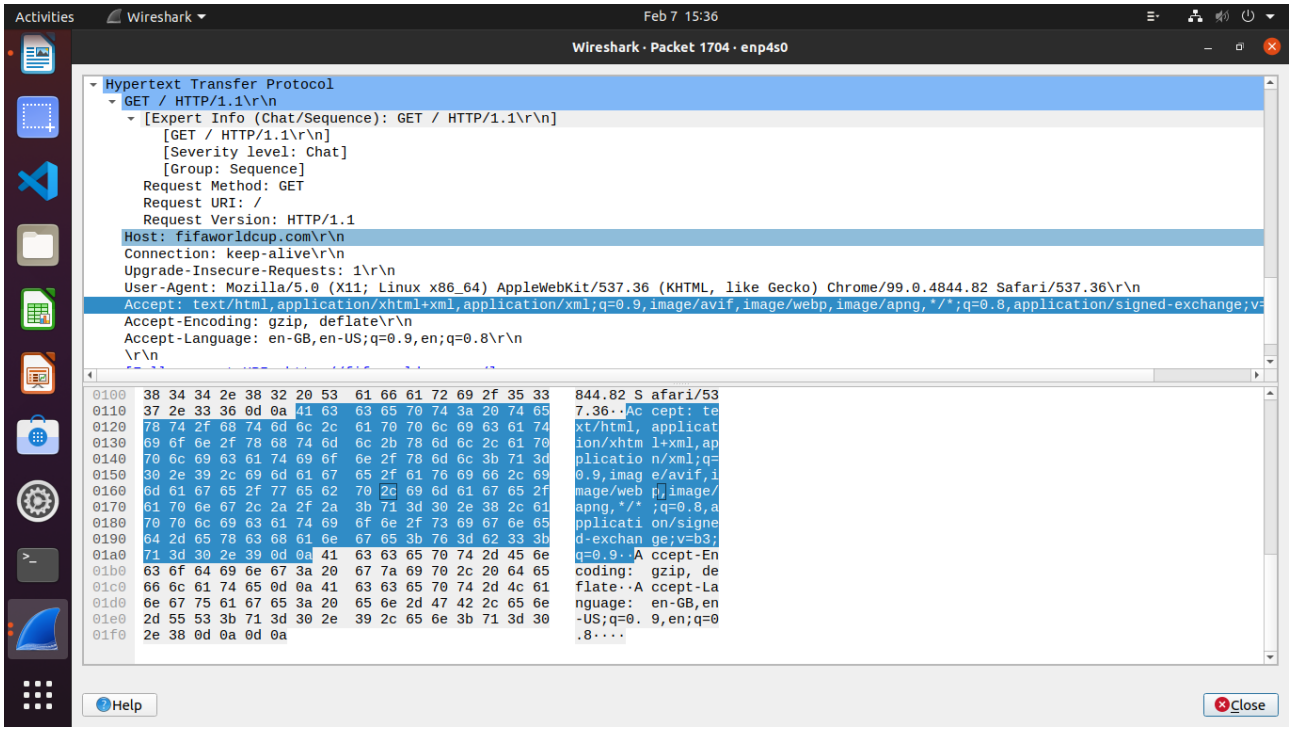
notification from the sender to the receiver that the receiver should pass all the data to the application quickly.

c. What are the lengths of the TCP segment and payload?

The TCP segment length: 87

• Consider the contents of the "GET" message.

a. Scroll down the third pane in the Wireshark window and compare the decoded text with the contents of the HTTP message in the second window.



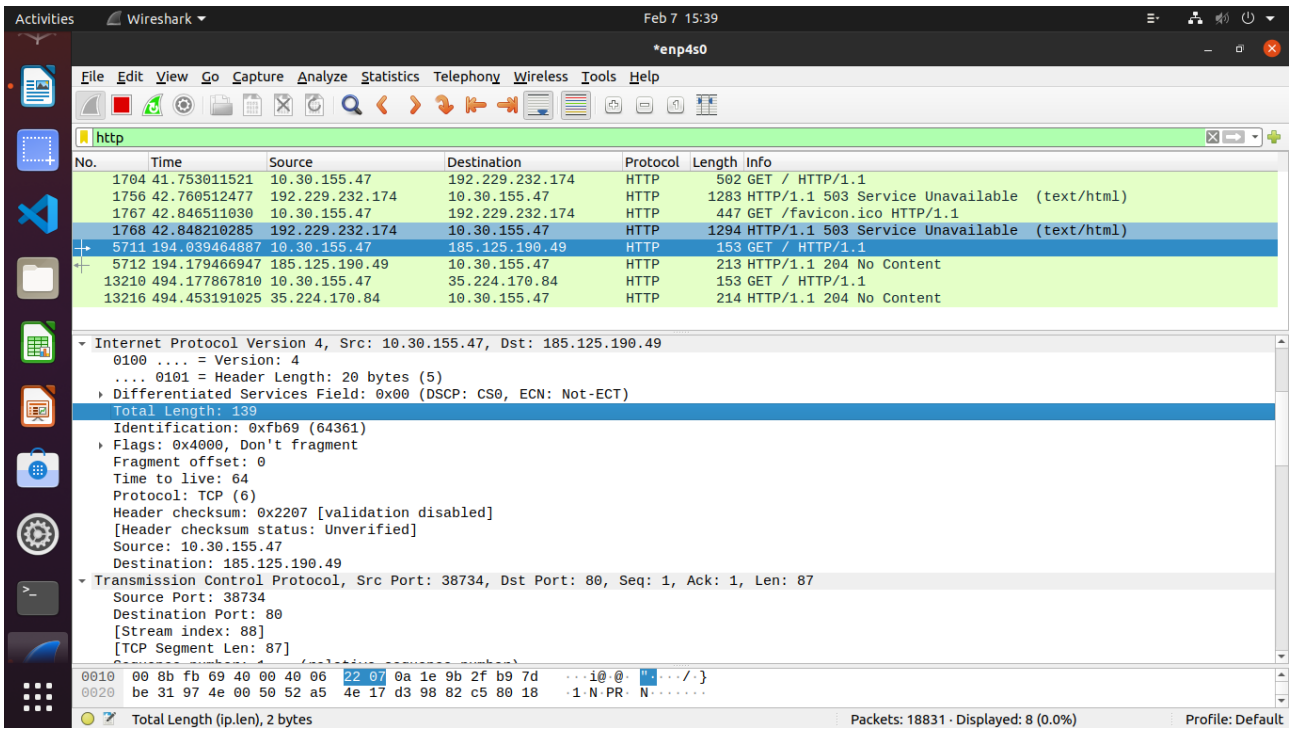
b. Count the number of octets in the message and verify that this number is consistent with the length information in the TCP header.

Total number of octets can be calculated by subtracting the header length of IP and header length of TCP from total length of IP. i.e.,

IP->Total length = (IP header length + TCP Header length + application)

Therefore, Total number of octets = IP_Length – IP_header_length – TCP_header_length

Total number of octets = 139 – 20 – 32 = 87

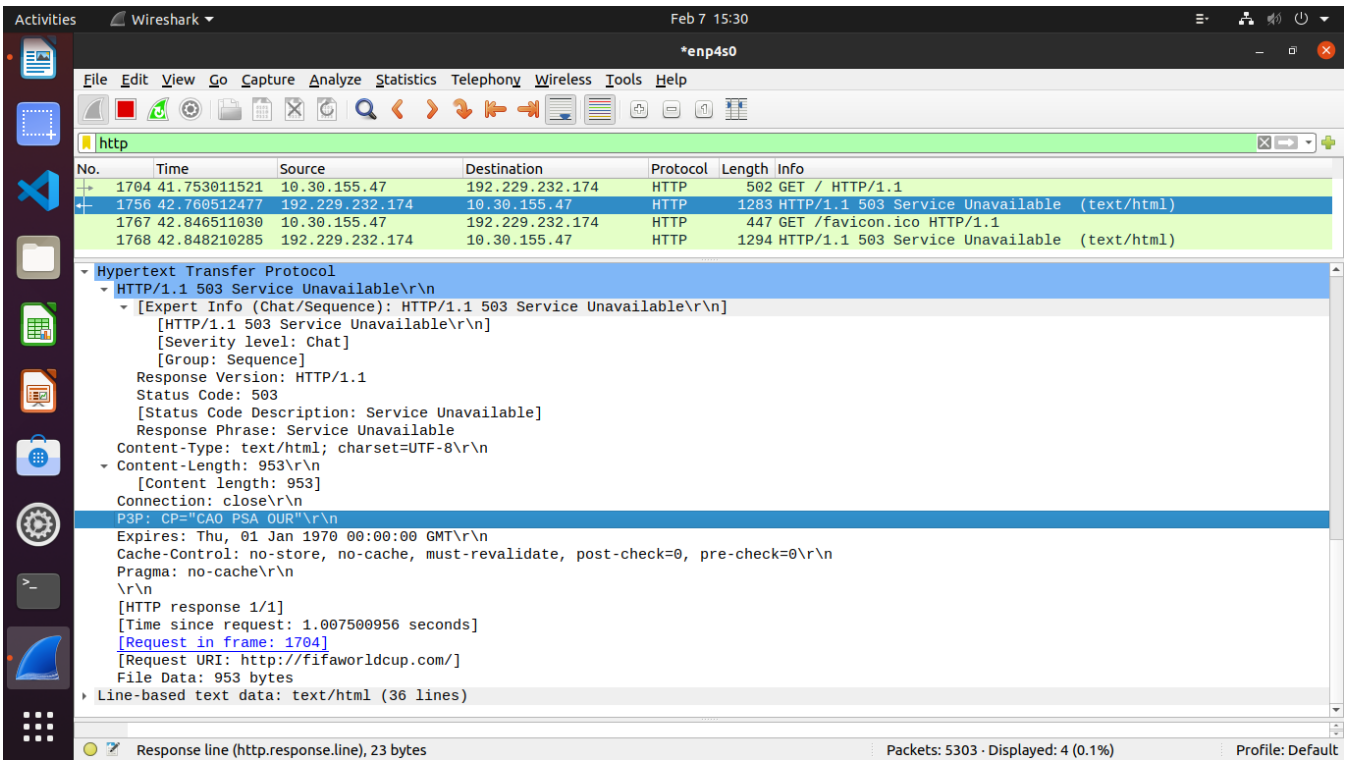


c. What is the next sequence number that is expected in the next segment from the server?

The next sequence number that is expected in the next segment is same. Since, the server acknowledge with sequence number that it has received and ask it for next segment.

• HTTP Response

• *How much time elapses between the capture of the GET message and the capture of the corresponding Response message?*

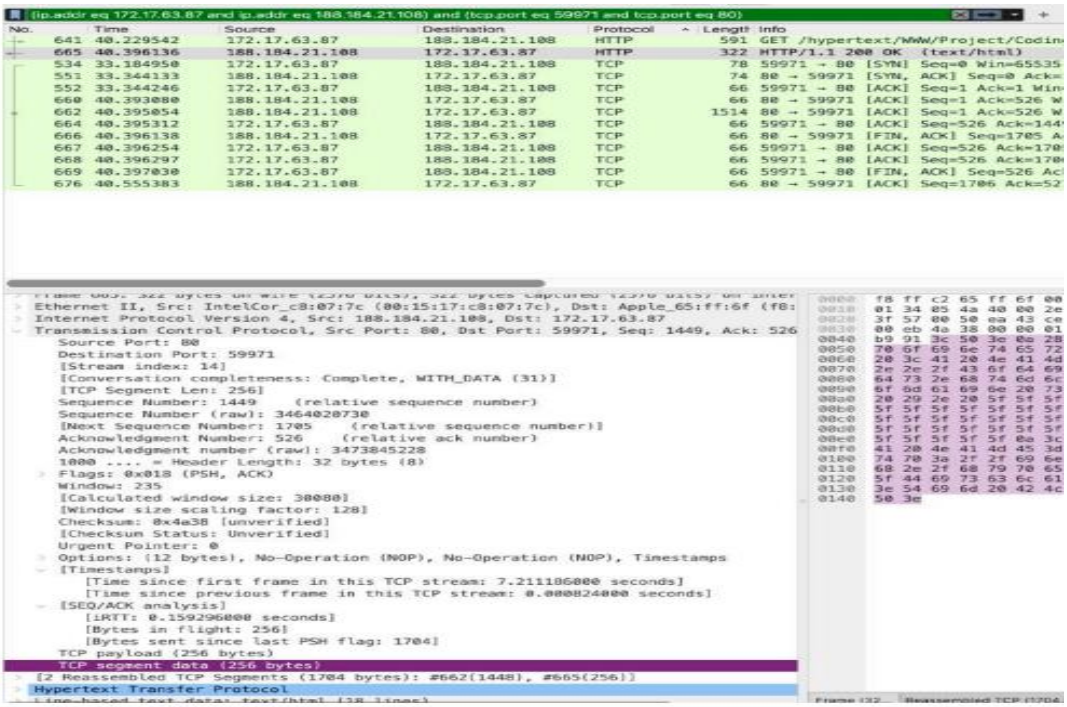


• *Determine whether the server responds with an HTTP response message or simply with a TCP ACK segment. Verify that the sequence number in the segment from the server is as expected*

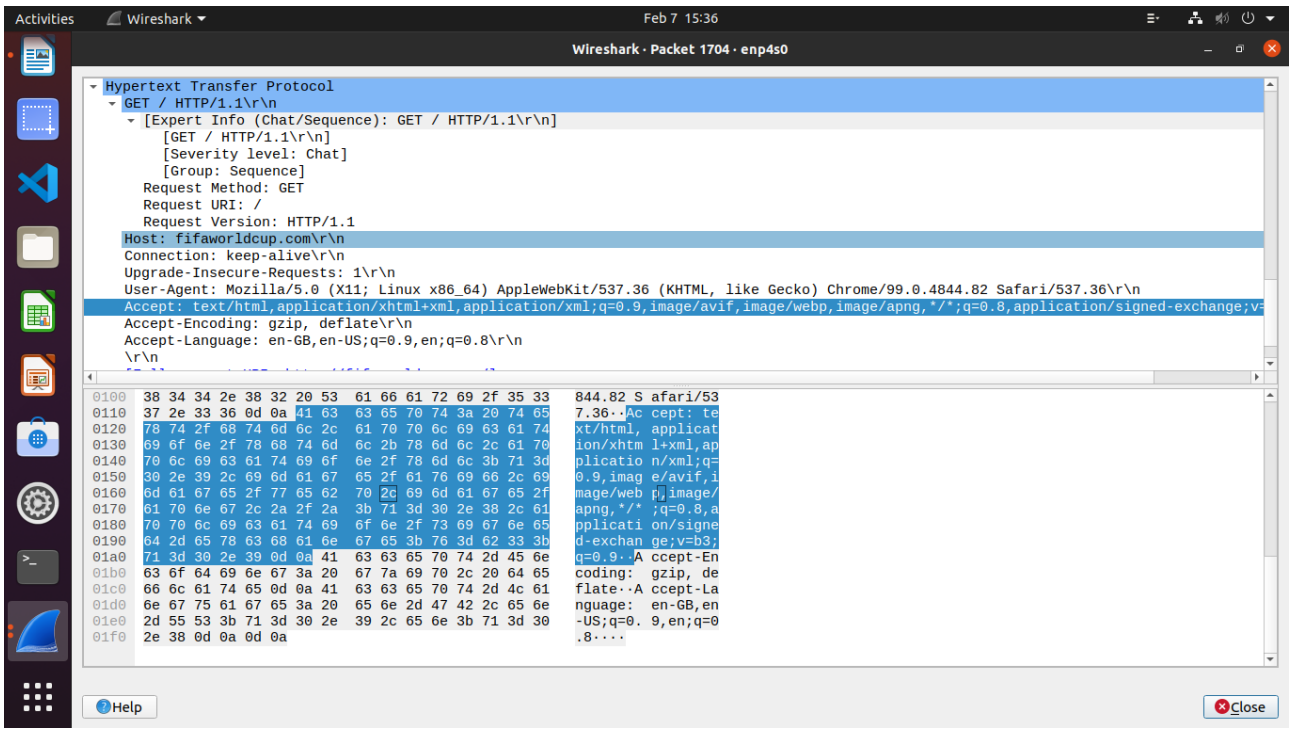
Server response with a message. In this case, server response with a text/html file.

• *Consider the segment that contains the HTTP response message a. What is the length of the payload in the TCP segment?*

The length of the TCP segment is found to be 256 bytes



b. Examine whether any of the flags are set and explain why they are set
ACK flags are set because server is acknowledging the request received by it and PSH is set because it shows the end of the data.
c. What acknowledgement number is expected in the next segment from the client?
Acknowledgement number would be increased for the next segment upon the request made by client.
• *Consider the HTTP response message*
a. What is the result code in the response message?
The result code in the response message is 200 which means OK.
b. Highlight the "data" section of the HTTP response message. Scroll down the third pane in the Wireshark window and compare the decoded text with the contents of the web page that was displayed on your screen.


Activities
Wireshark
Feb 7 15:36
Wireshark · Packet 1704 · enp4s0
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
[GET / HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: fifaworldcup.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
\r\n
0100 38 34 34 2e 38 32 20 53 61 66 61 72 69 2f 35 33 844.82 S afari/53
0110 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 7.36··Ac cept: te
0120 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 xt/html, applicat
0130 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 ion/xhtm l+xml,ap
0140 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
0150 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 0.9,imag e/avif,i
0160 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f mage/web p,image/
0170 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 apng,*/* ;q=0.8,a
0180 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 pplicati on/signe
0190 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b d-exchan ge;v=b3;
01a0 71 3d 30 2e 39 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.9··A ccept-En
01b0 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de
01c0 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 flate··A ccept-La
01d0 6e 67 75 61 67 65 3a 20 65 6e 2d 47 42 2c 65 6e nguage: en-GB,en
01e0 2d 55 53 3b 71 3d 30 2e 39 2c 65 6e 3b 71 3d 30 -US;q=0. 9,en;q=0
01f0 2e 38 0d 0a 0d 0a .8····
Help
Close