CSP334: Computer Networks
Lab Assignment No 1
Assignment on Linux Networking Commands

Abhishek Gupta 2016UCS0012

September 11, 2018

1 Q1: Network Interfaces

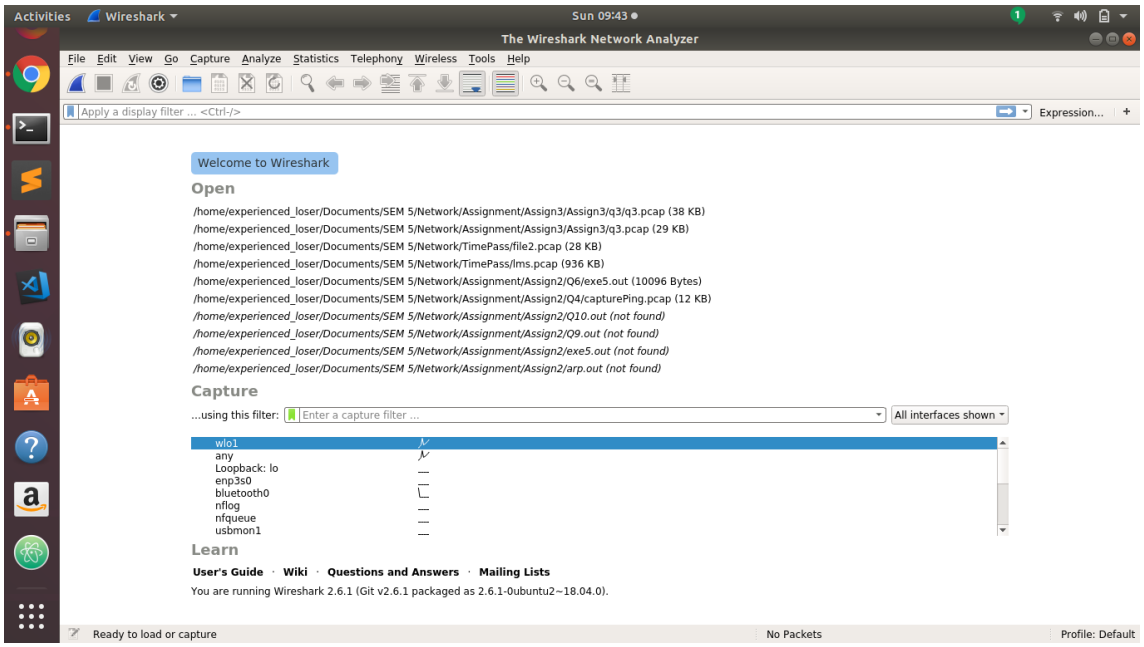

Figure 1: Screenshot of Network Interfaces

I selected **wlo1** network interface

2 Q2: Application Layer Protocol

HTTP Application Protocol is used

3 Q3: Protocols Displayed in Unfiltered Packet

The following protocols were displaced in Unfiltered Packet :-

1. ARP
2. DNS
3. TCP
4. TLSv1.2

4 Q4: IPA

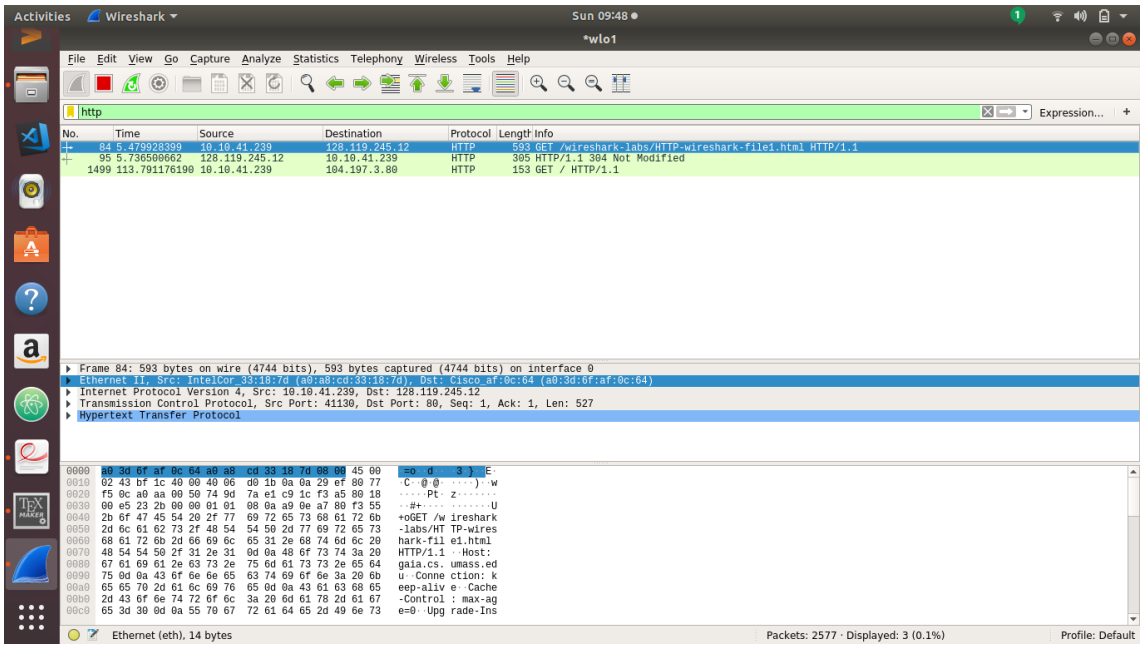

Figure 2: Screenshot of IPA

IPA of my machine : **10.10.41.239**
IPA of destination machine : **128.119.245.12**

4.1 How did I confirm destination IP

I did nslookup of http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html and got :

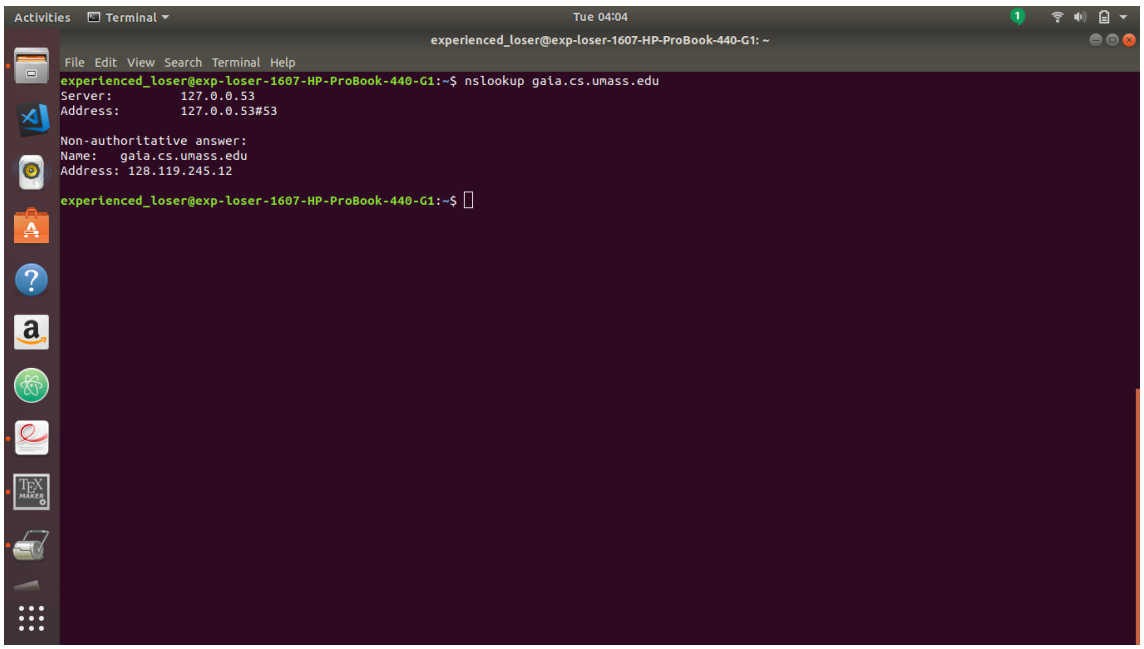

Figure 3: Screenshot of dest IP

Hence IPA of Dest Verified

5 Q5: Class of IPA

source : **CLASS A**
destination : **CLASS B**

6 Q6: Bits captured

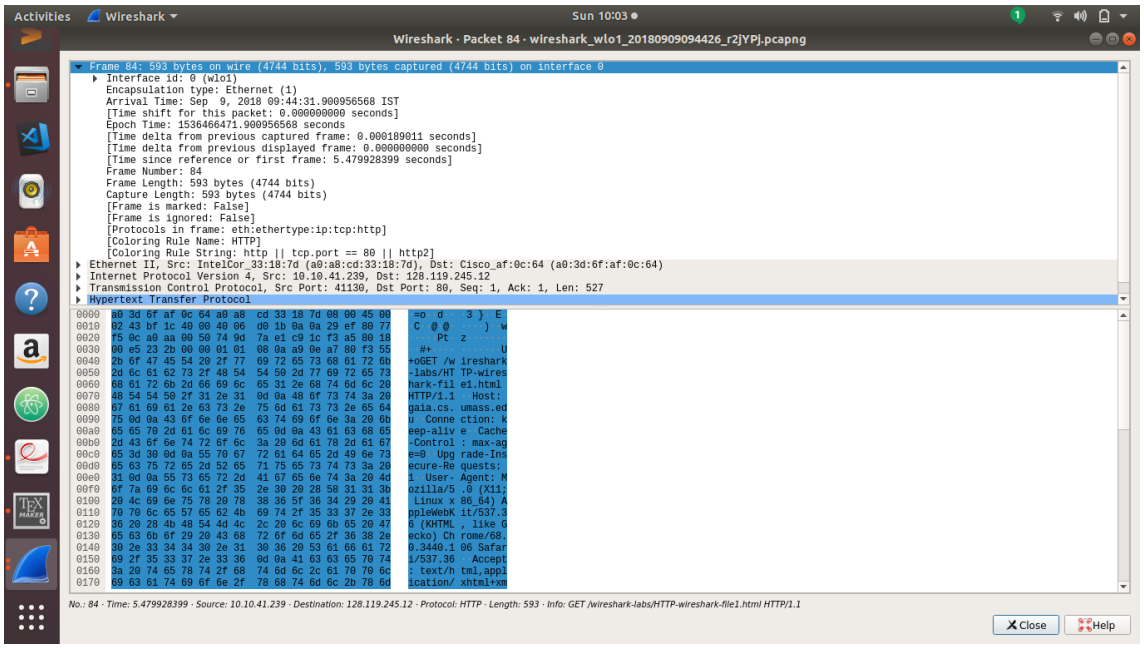

Figure 4: Screenshot of captured Bits

593 Bytes ie 593 X 8 = **4744** Bits were captured on **Sep 9 2018 at 9:44:31 IST**

7 Q7: Interface id

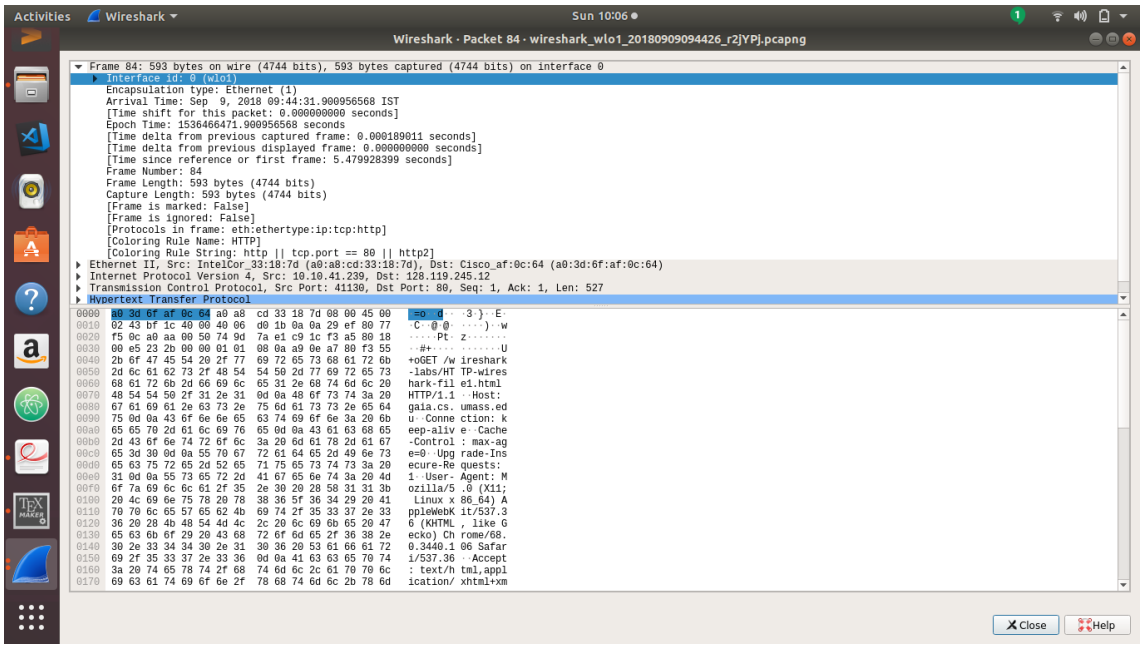

Figure 5: Screenshot of interface id

Interface Id : 0
Interface Address: wlo1

8 Q8: Time for HTTP OK reply to Receive

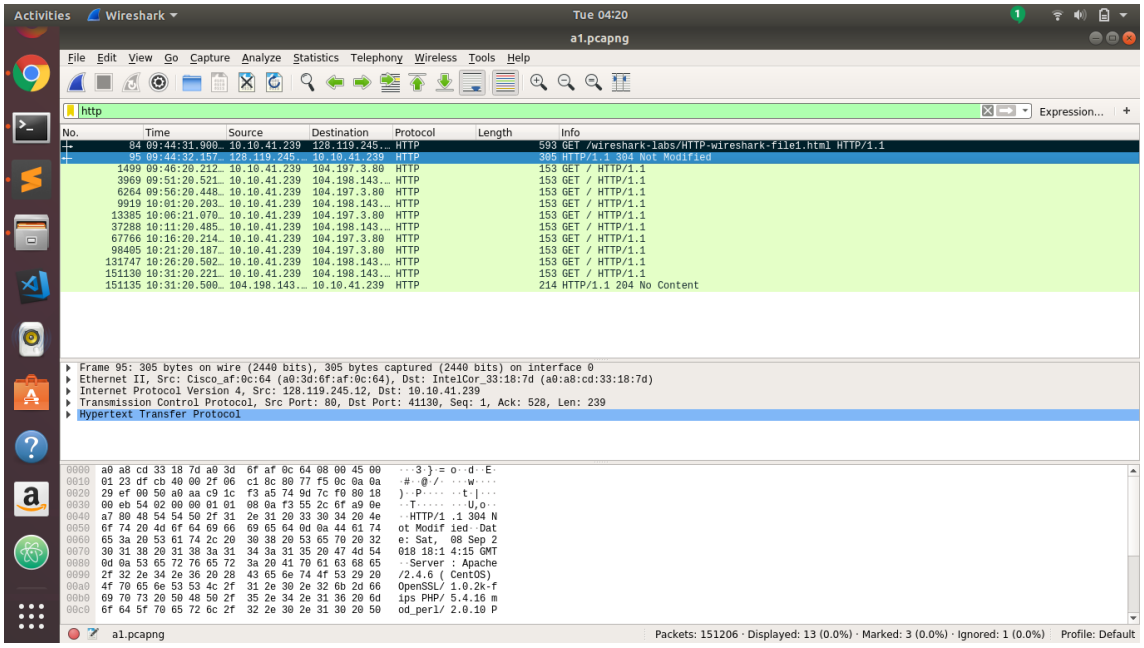

Figure 6: Screenshot of http filtered packets

Request (Black Highlighted) at **9:44:31:900 IST**
Response (Blue Highlighted) at **9:44:32.157 IST**

Site took **0.257 sec** to respond

9 Q9 : No such question

10 Q10: 2 HTTP messages

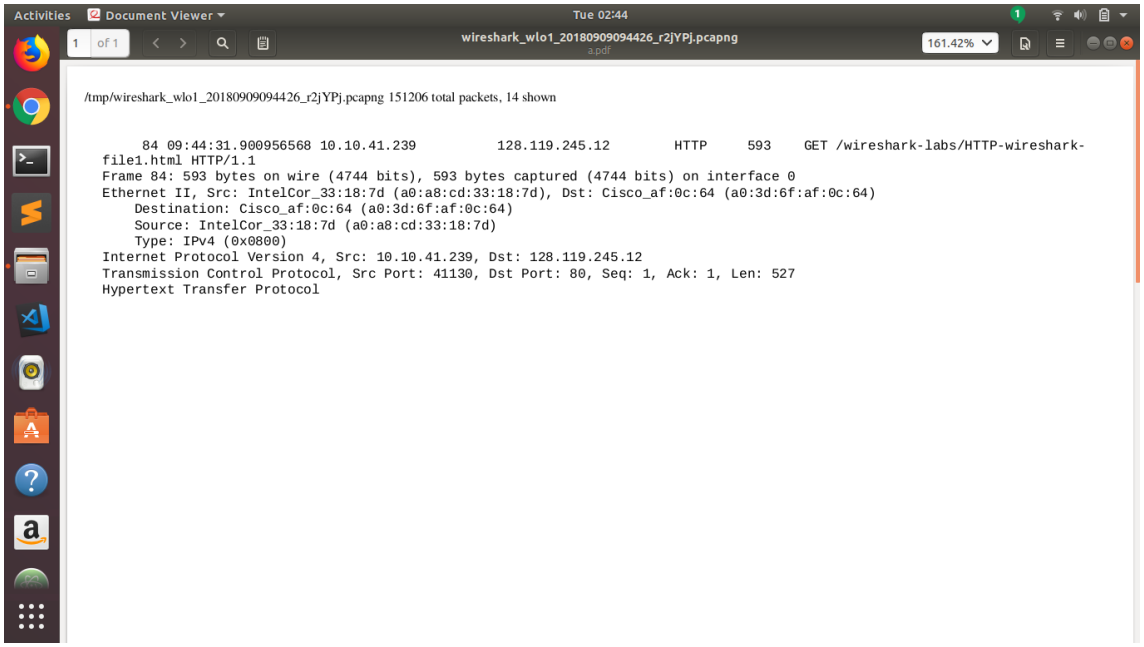

Figure 7: Screenshot of http message 1

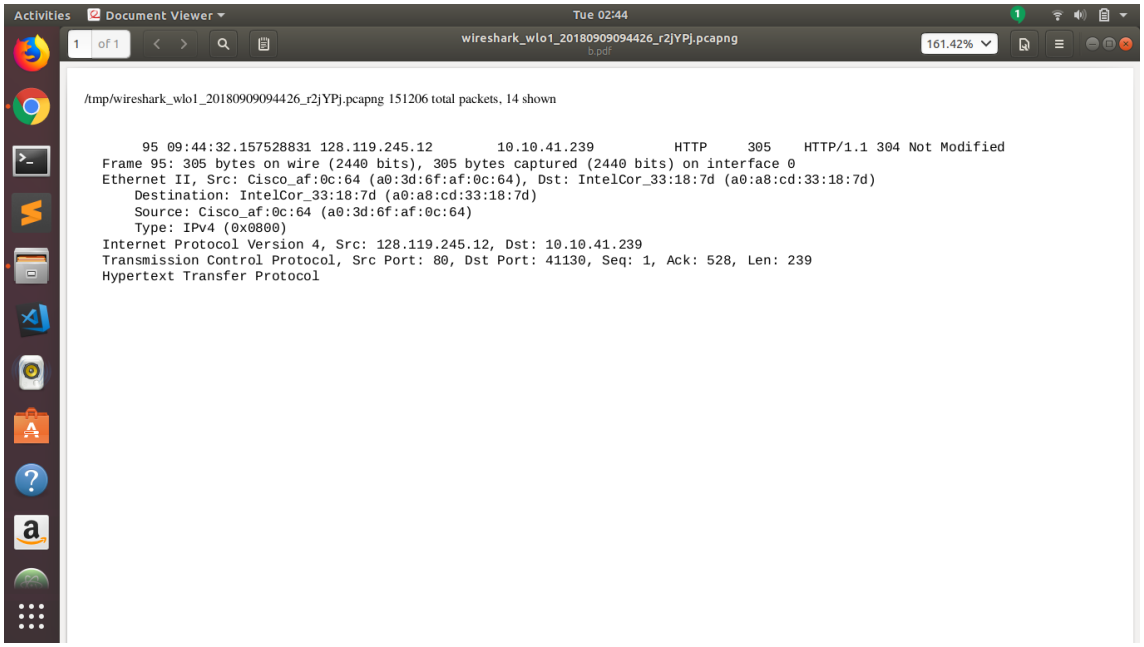

Figure 8: Screenshot of http message 2

11 Q11: Destination Physical Address

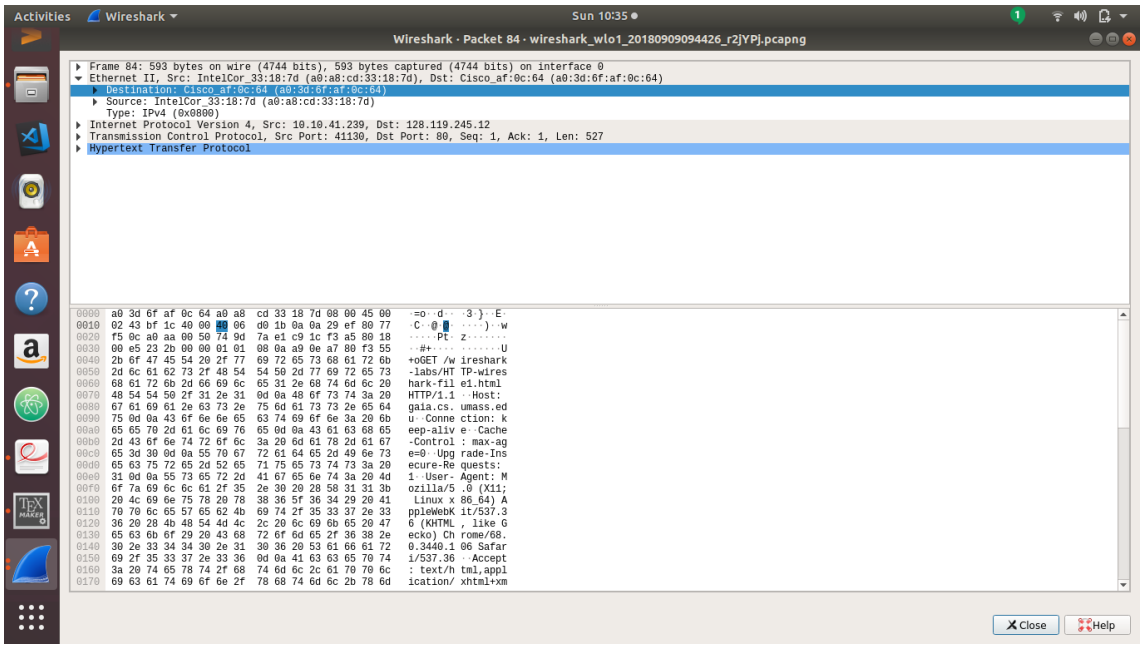

Figure 9: Screenshot of dest physical address

Destination Physical Address : $Cisco_af : 0c : 64(a0 : 3d : 6f : af : 0c : 64)$
This belong to the physical address of our gateway ie the first router of our system

12 Q12: Length of header

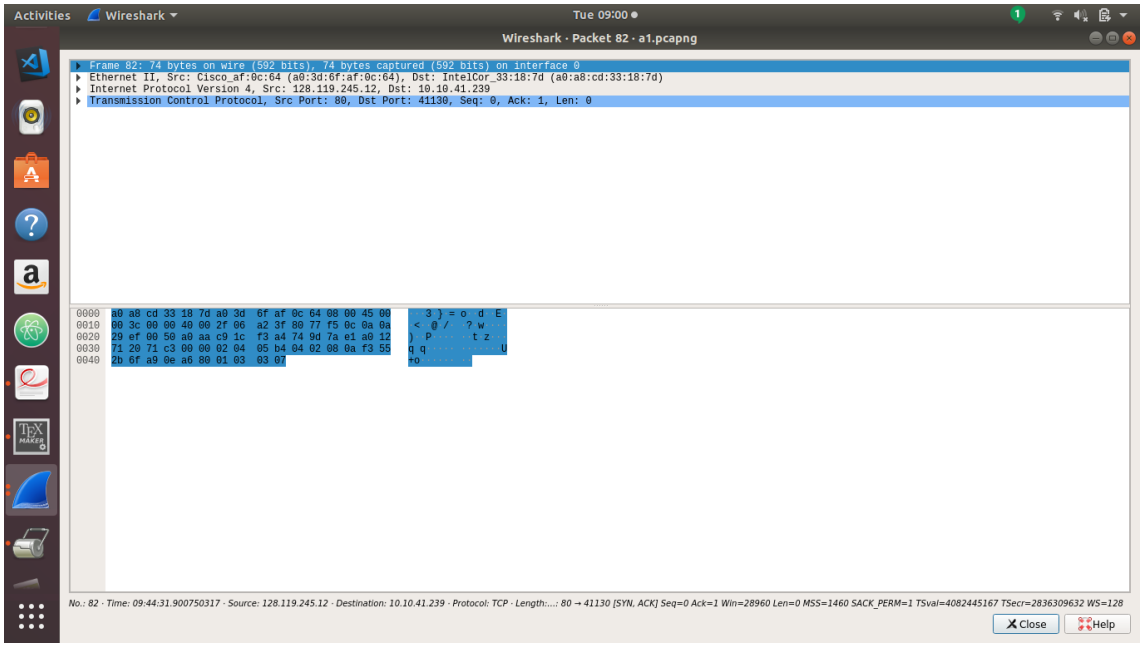

Figure 10: Screenshot of tcp header

Total **74 Byte**

13 Q13: Ethernet header of a frame

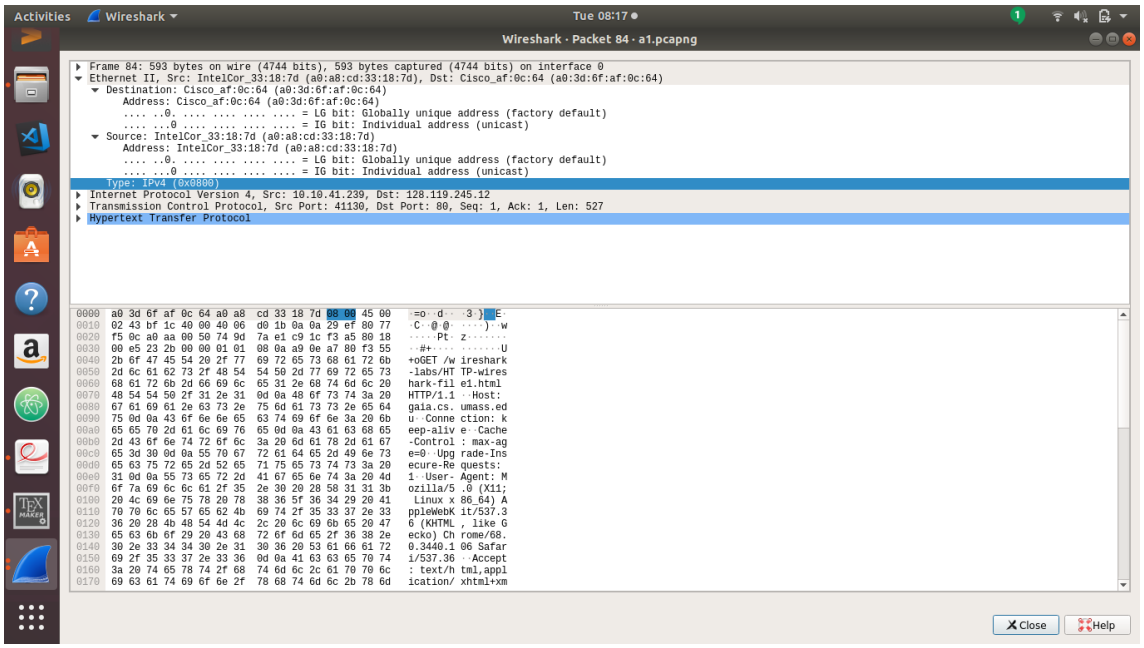

Figure 11: Screenshot of ethernet header frame

Yes we can determine and above is the proof.

14 Q14: TCP or UDP as transport protocol

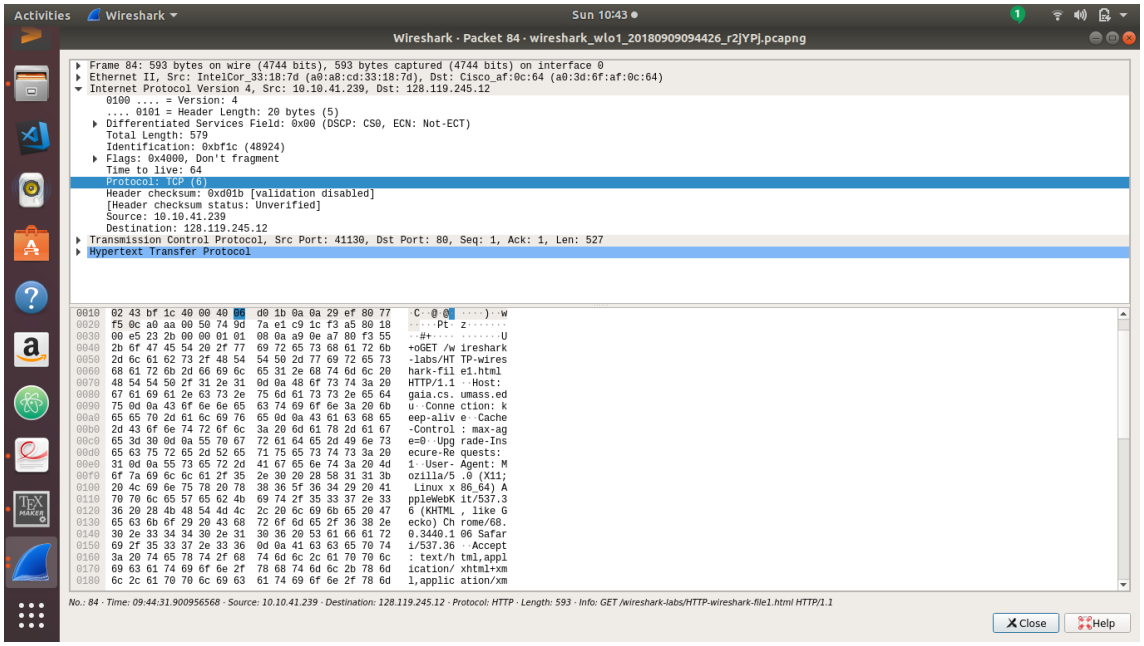

Figure 12: Screenshot of tcpdump file

Yes it is possible to know whether the first packet captured has TCP or UDP as transport protocol . The upper picture is the proof. Highlighted TCP(6)

15 Q15: SYN and ACK

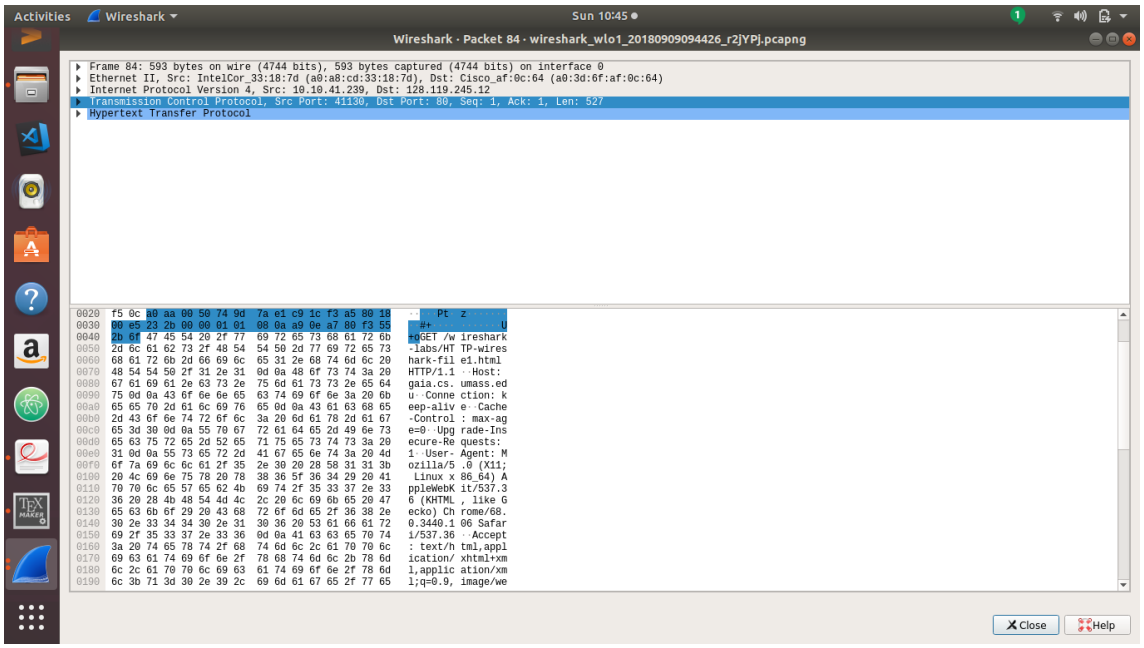

Figure 13: Screenshot of request from client

Ports (SYN) request from client:

Client Port: 41139
Server Port: 80

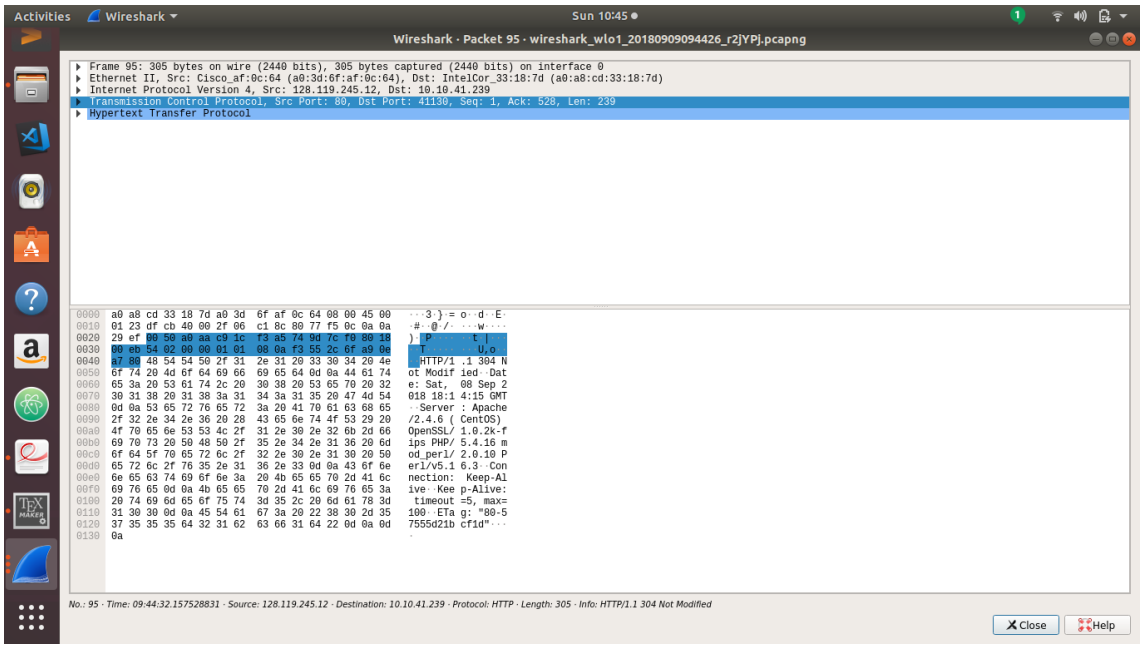

Figure 14: Screenshot of response from server

Ports (ACK) response from server:

Client Port: 41139
Server Port: 80

We can see that the client and server Port is NOT Same as thw one is well known port and other is empheral port which can change for many requests

16 Q16: Server Hello Message

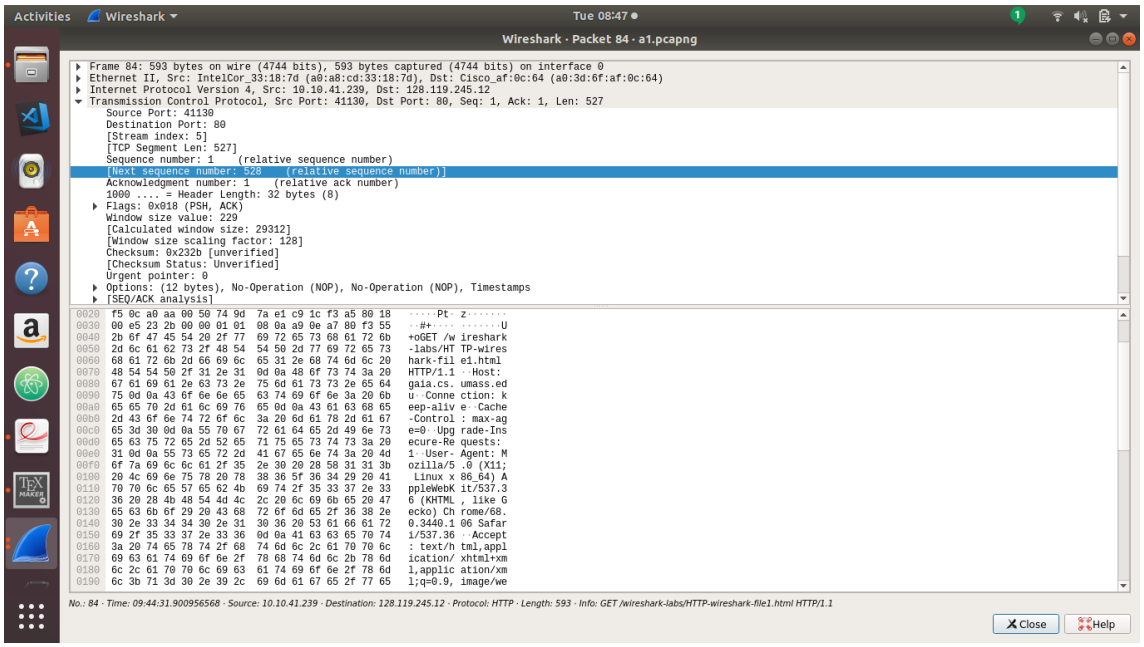

Figure 15: Screenshot of request

We can see that the next sequence number in the image is 528. Which will become ACK for the server.

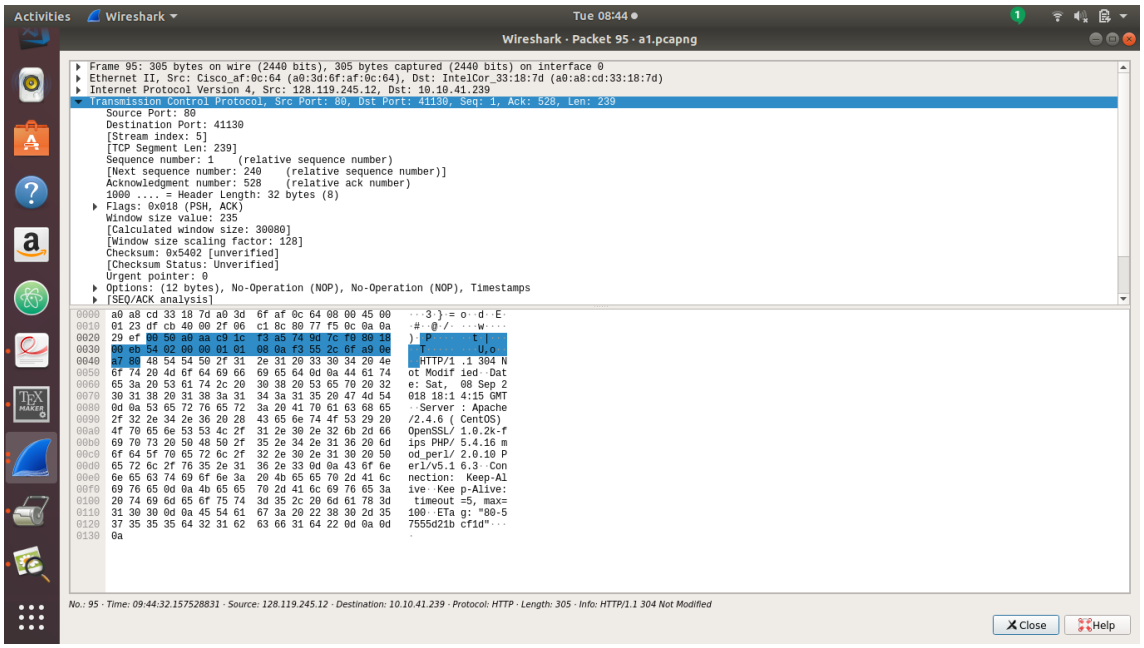

Figure 16: Screenshot of response

Server Hello message sent by the server have 1 as a relative sequence number and 528 as a relative acknowledgement number not 185.

Becoz of 3-way-handshake the next sequence number in the request packet becomes ACK number in the response packet. Now the ACK from client would be 240 in next request packet.

17 Q17: First Sequence number sent by the server to the client

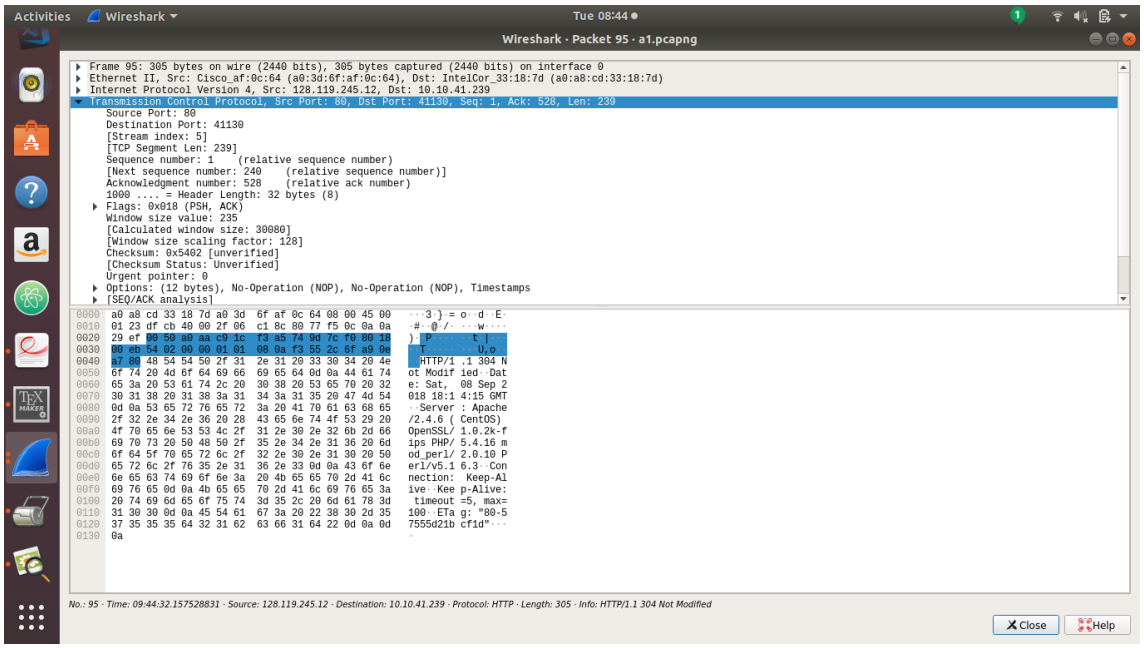

Figure 17: Screenshot of response

the first sequence number sent by the server to the client is 1.

Let's see what happens if sequence number is initiated as '0' ,

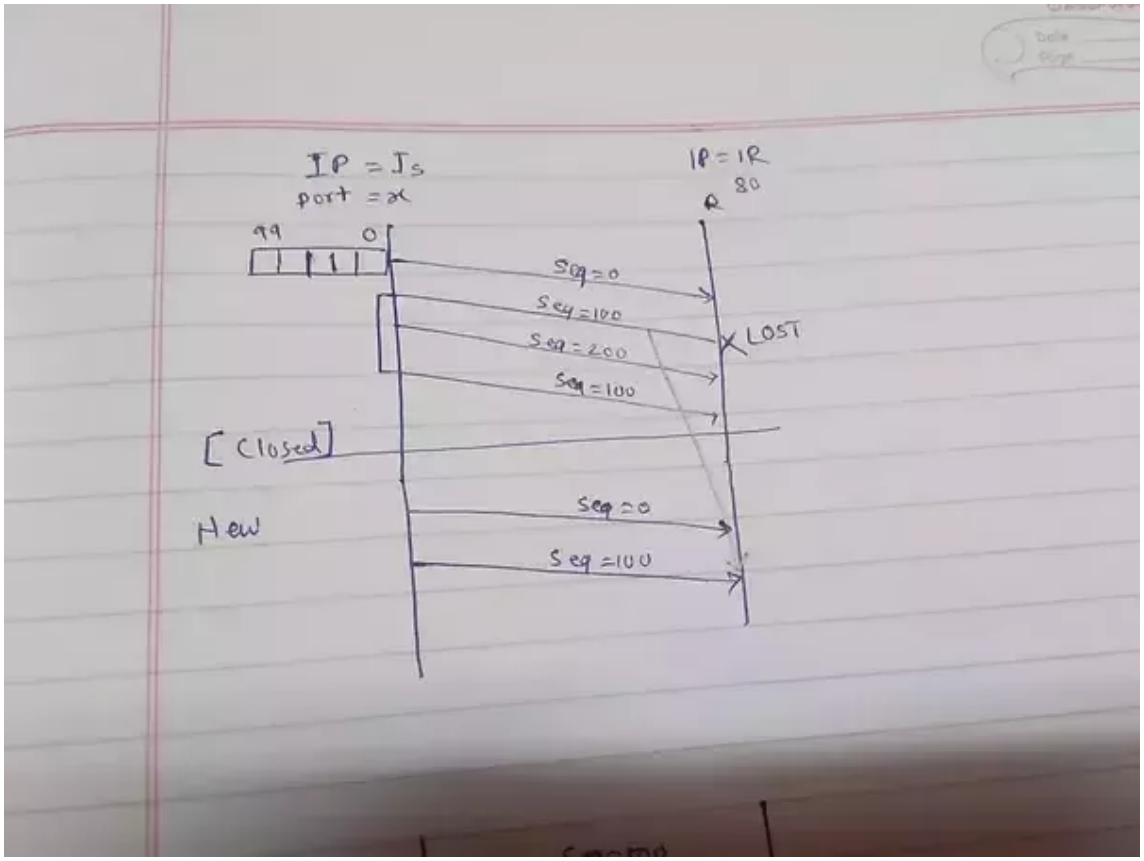

Figure 18: Screenshot of explanation

A sender sends 100B segment with initial sequence number as zero then next with sequence number 100 and so on. Consider that seq no 100 segment was delayed or lost and all three(assume only three) segments are transferred as well as that TCP connection was closed. Now a new connection with same IP:port as previous connection is established again and sequence number is initialized to '0'. now that delayed sequence number 100 seg is arrived now at seq num 100 of new connection as shown in picture, now that's an issue here.