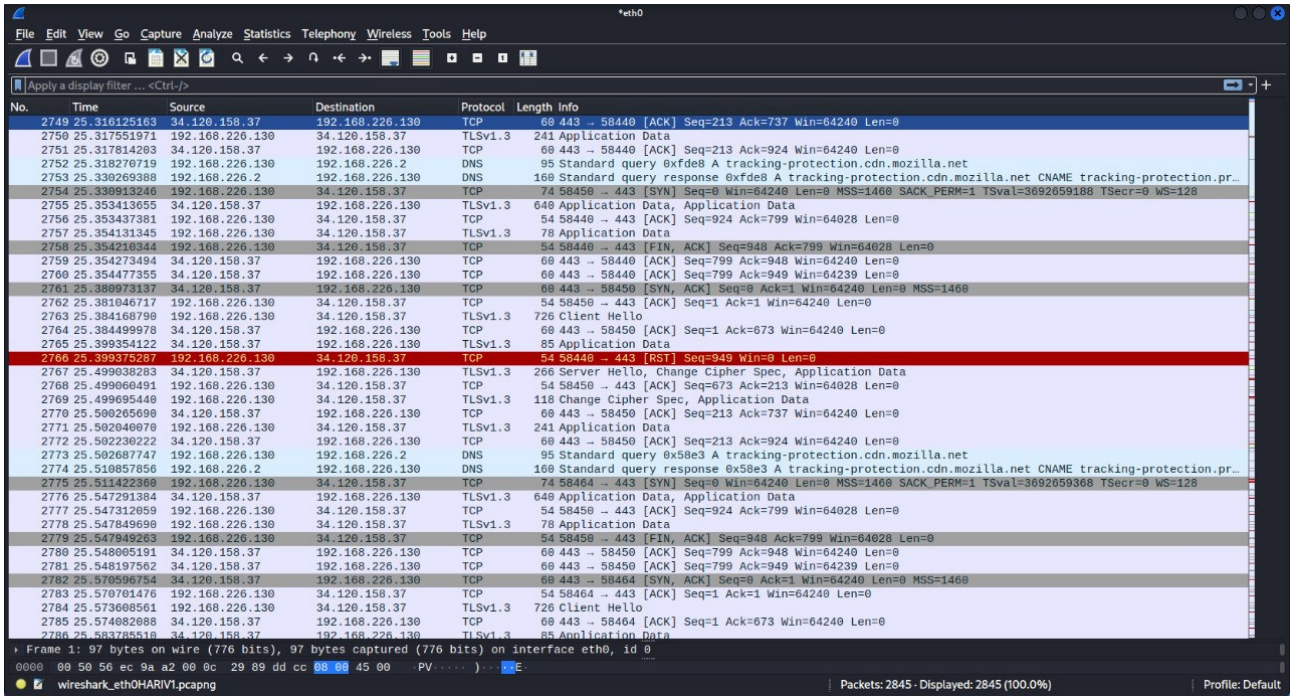
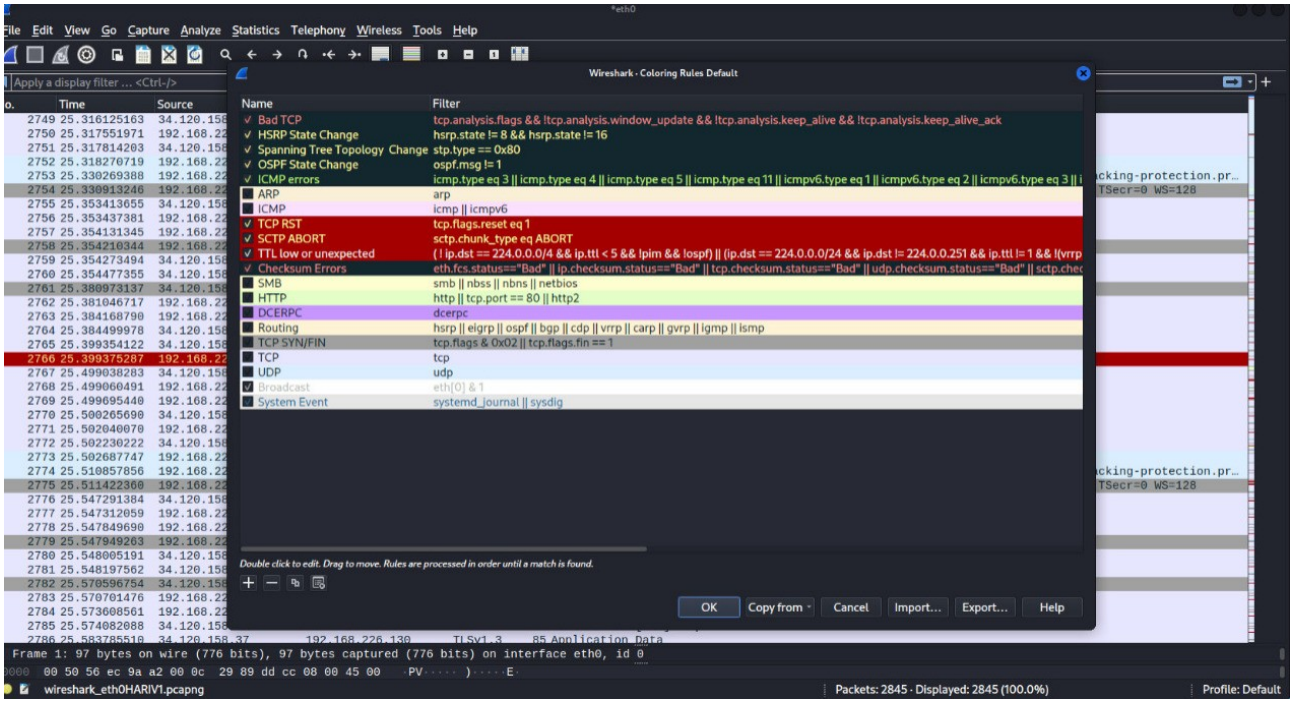
Lab Handout – 1

Ans 1 :-



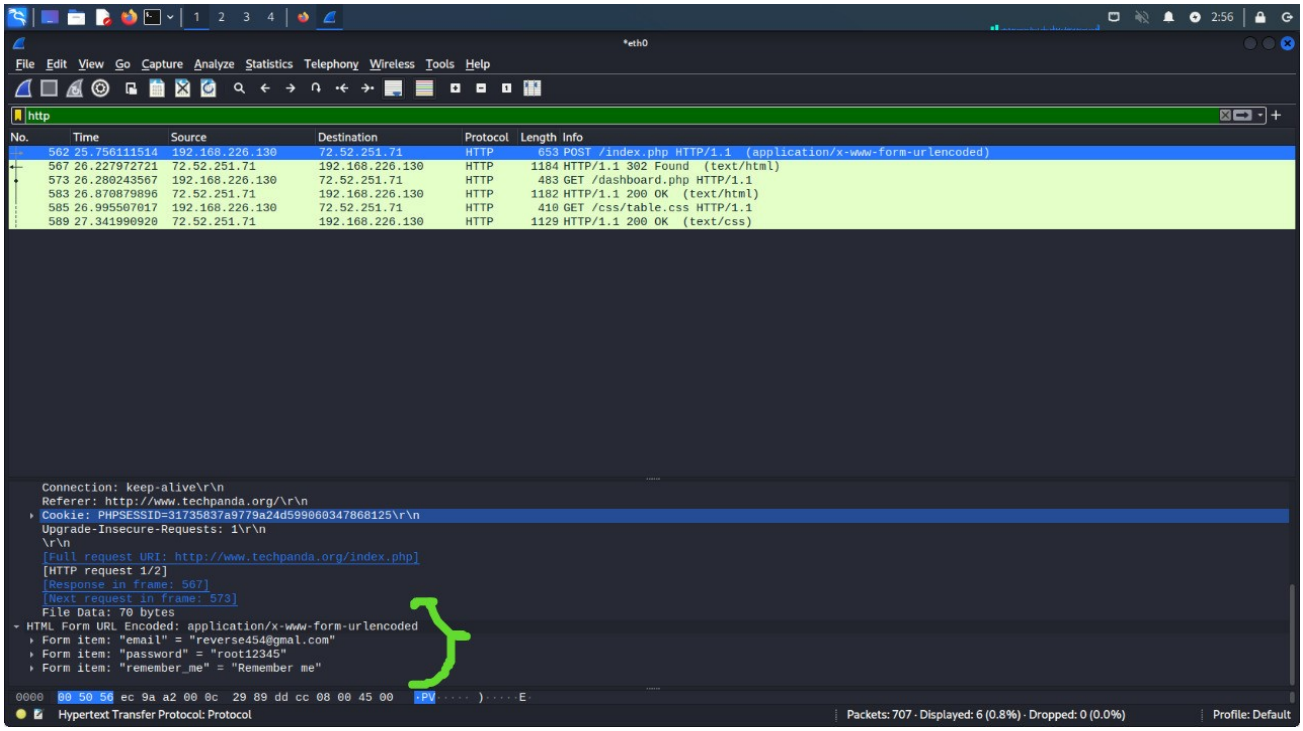
Ans 2 :-



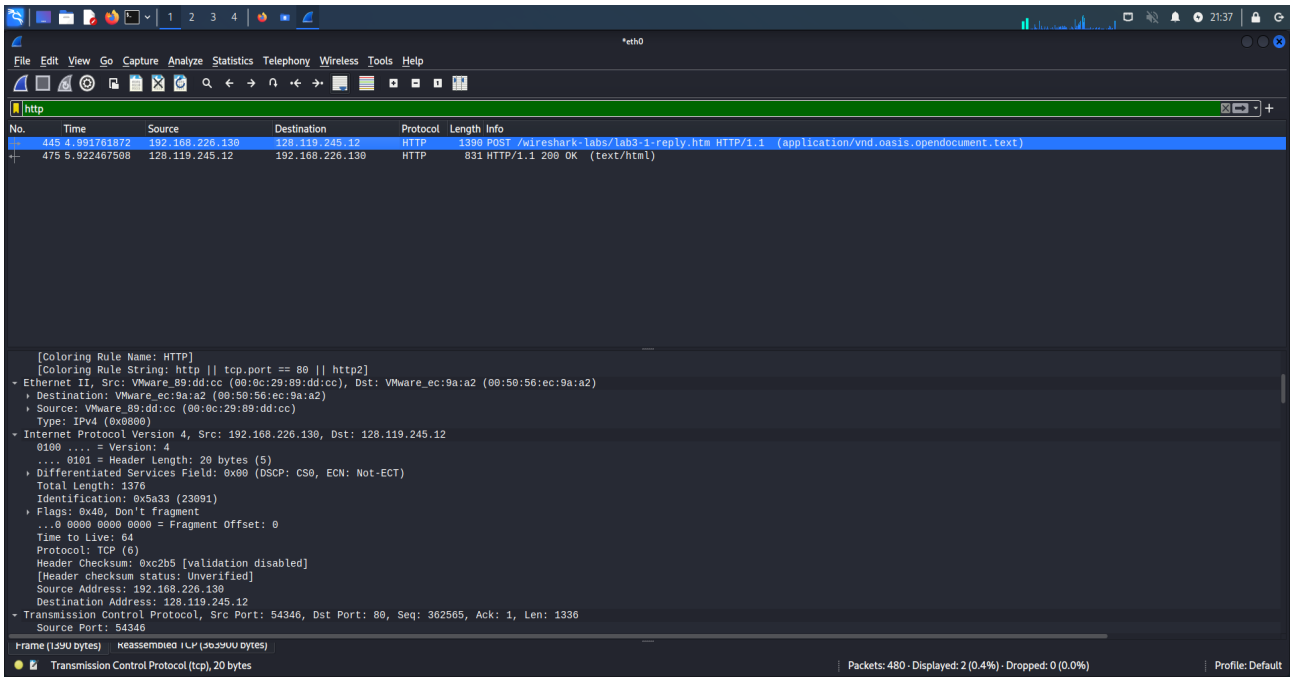
Ans 3 :- Change the filter to **ip.addr** == <destination>, where <destination> is the destination address of the HTTP packet.

Ans 4 : - DNS uses TCP for Zone transfer and UDP for name, and queries either regular (primary) or reverse. UDP can be used to exchange small information whereas TCP must be used to exchange information larger than 512 bytes.

Ans 5 :- Http Password Sniffing through Wireshark on TechPanda website.



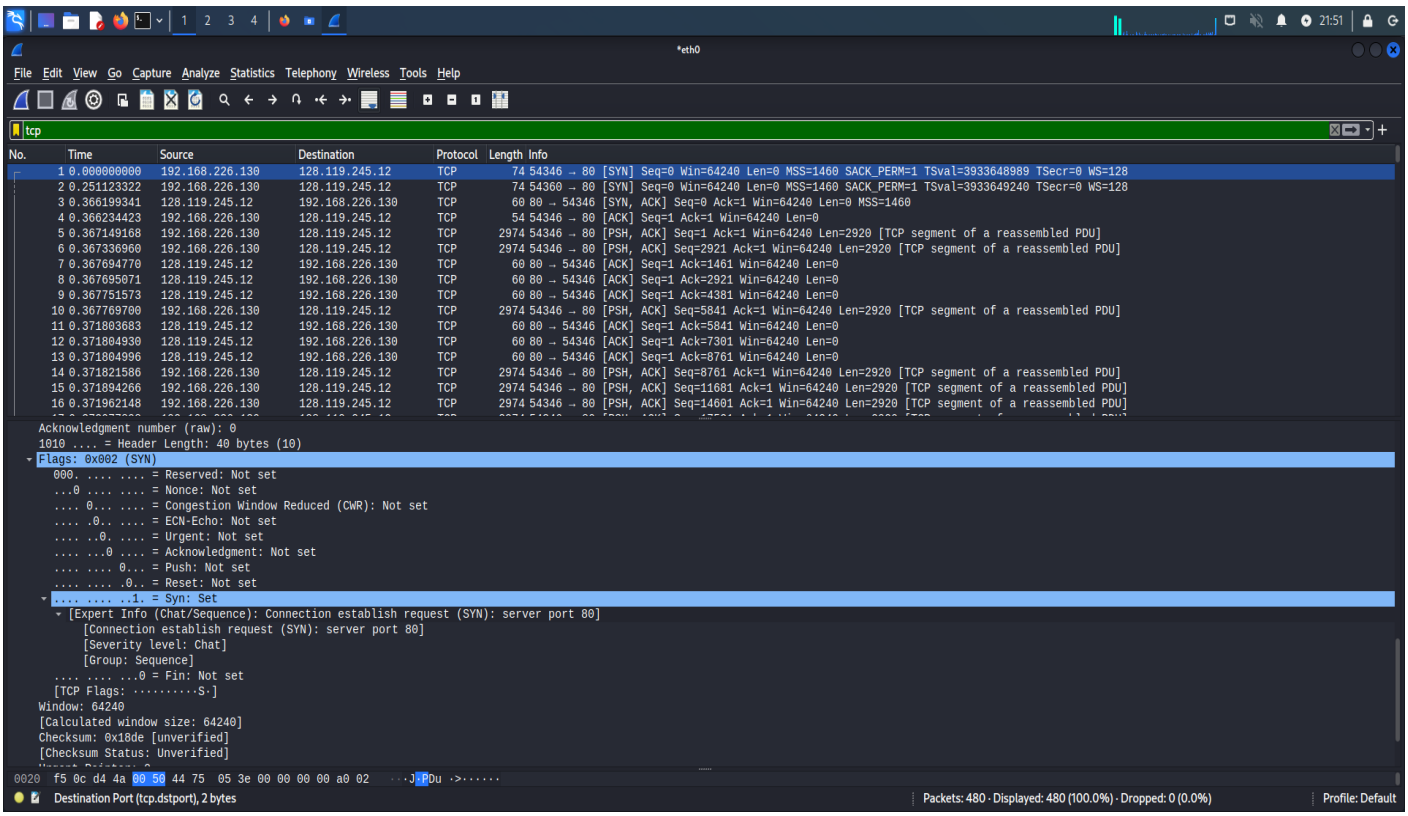
Lab Manual – 3



Ans 1 :- Source Address: 192.168.226.130, Source Port: 54346
Ans 2 :- Destination Address: 128.119.245.12, Destination Port: 80

==========

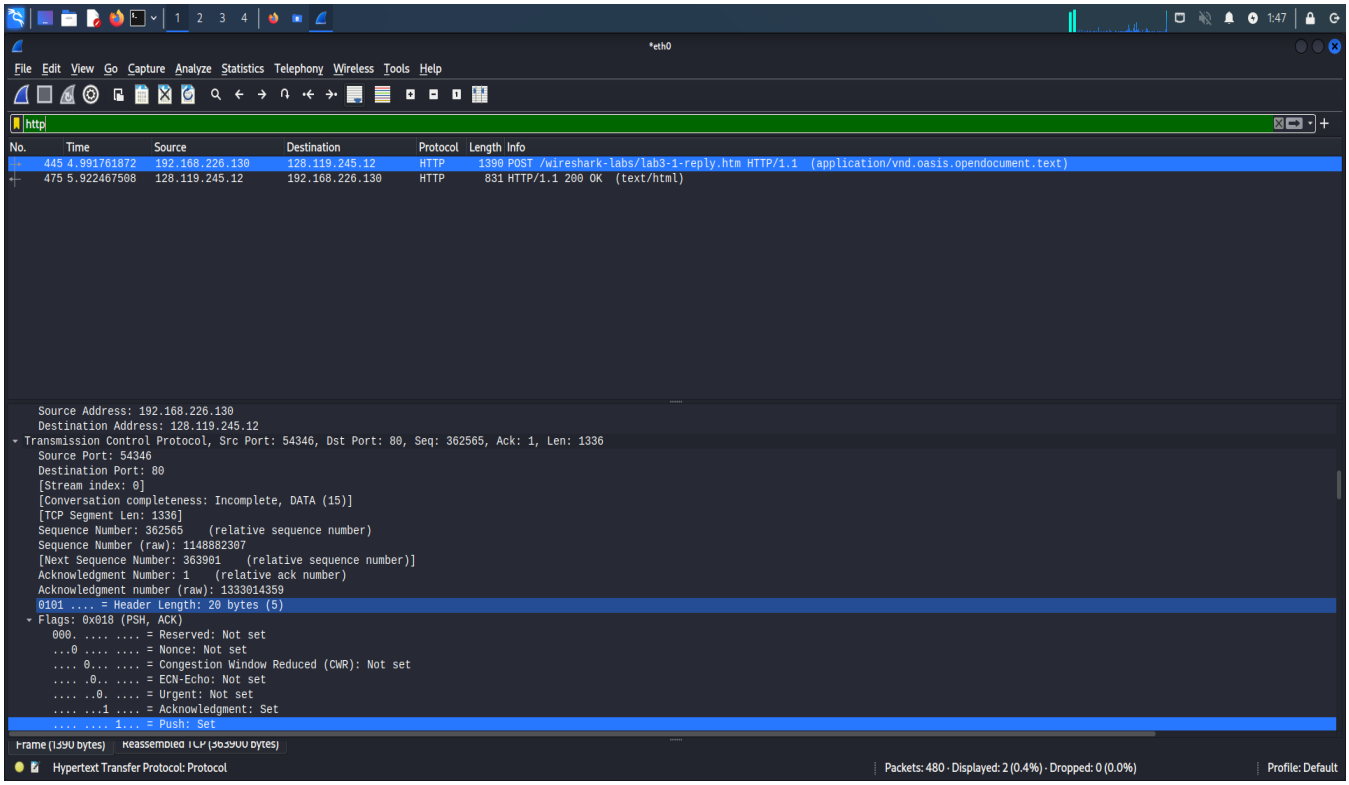
Image for Question 3,4,5,6



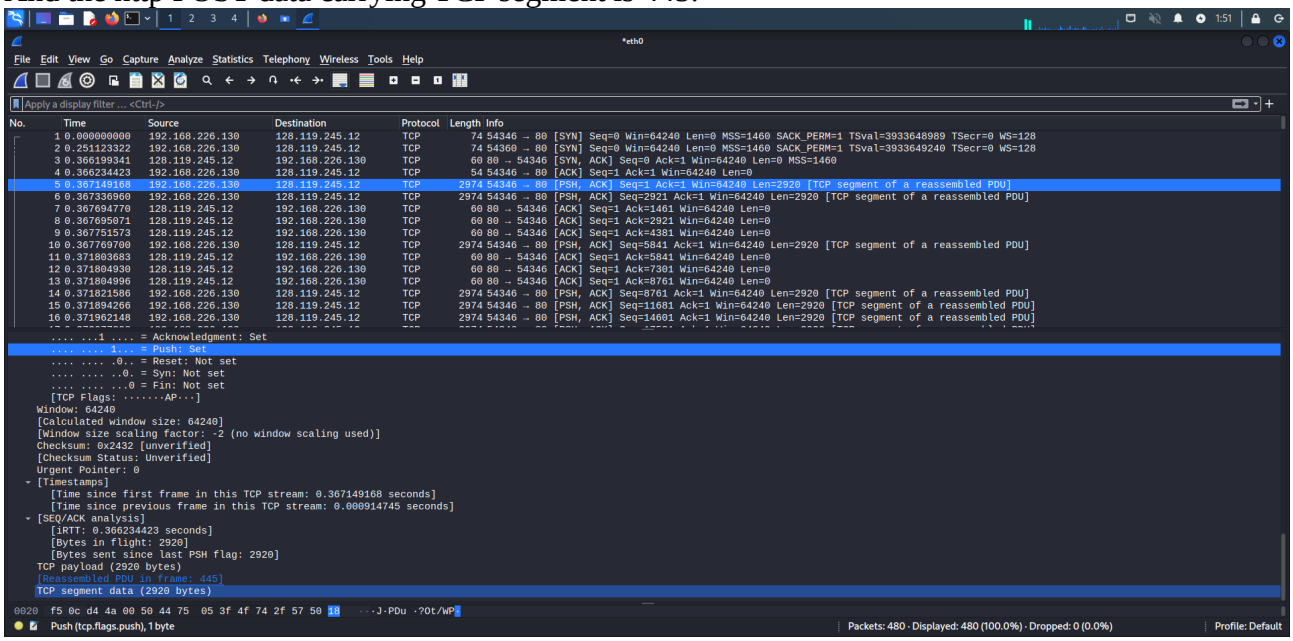
Segment 1- 4 are used for the connection between client and the given website to complete the hanshake. Total 4 segments were used.
[SEQ/ACK analysis] in TCP Header Flags segment identifies TCP segment as handshaking segments

[This is an ACK to the segment in frame: 1]
[The RTT to ACK the segment was: 0.366199341 seconds]
[iRTT: 0.366234423 seconds]

Ans 4:- TCP first six data carrying segments are :- 5,6,10,14,15,16.



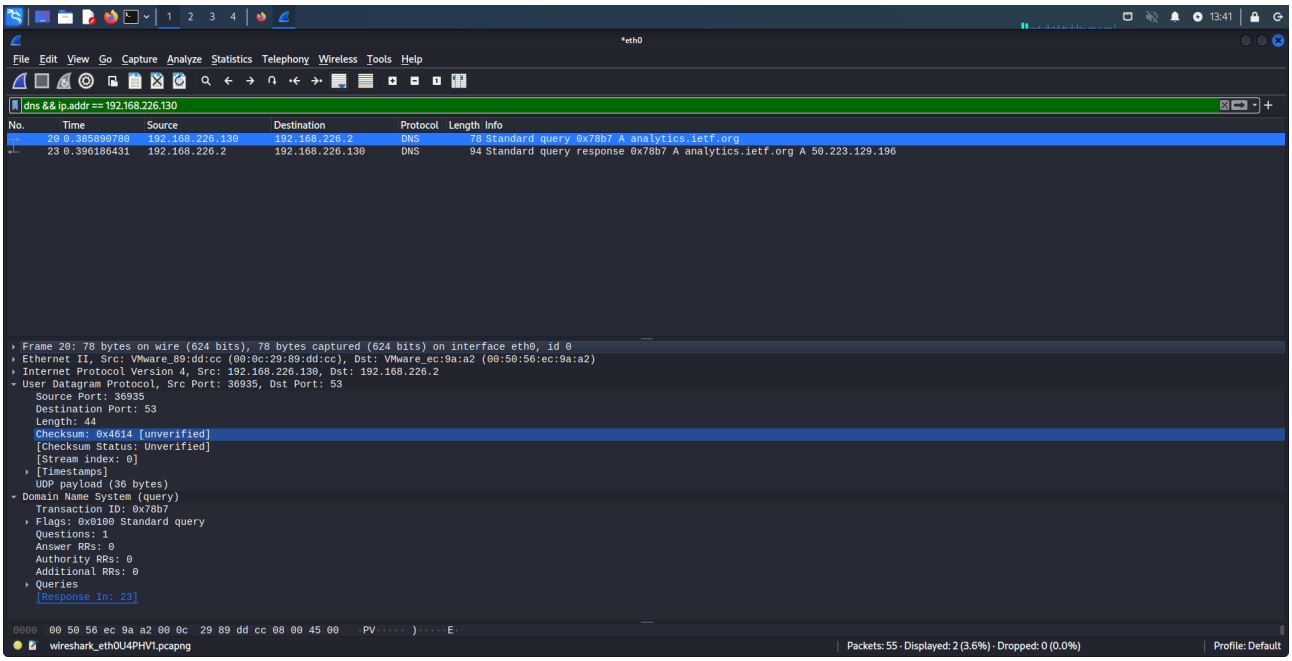
And the http POST data carrying TCP segment is 445.



From the Above Diagram :-
TCP Segment 5:- TCP segment data (2920 bytes)
TCP Segment 6:- TCP segment data (2920 bytes)
TCP Segment 10:- segment data (2920 bytes)
TCP Segment 14:- segment data (2920 bytes)
TCP Segment 15:- segment data (2920 bytes)
TCP Segment 16:- segment data (2920 bytes)
TCP Segment 445 (HTTP Post) :- TCP segment data (1336 bytes)

Ans 5:- Time relative to the first Frame in the TCP Stream i.e, 0.000000sec
TCP Segment 5:- Sent : 0.367149168 seconds , received : 0.368063913 seconds
TCP Segment 6:- Sent :0.367336960 seconds , received : 0.367769700 seconds
TCP Segment 10:- Sent : 0.367769700 seconds, received : 0.371821586 seconds
TCP Segment 14:- Sent : 0.371821586 seconds, received : 0.371894266 seconds
TCP Segment 15:- Sent :0.371894266 seconds , received : 0.371962148 seconds
TCP Segment 16:- Sent :0.371962148 seconds , received : 0.371966148 seconds

Lab Manual – 4



Ans 1 :- From the above diagram we can see that the response message is transported using UDP(User Datagram Packet).We can only tell that the reason being data sent over UDP so that the data can we transferred Quickly and there is no such data where the lost of data can be a problem.

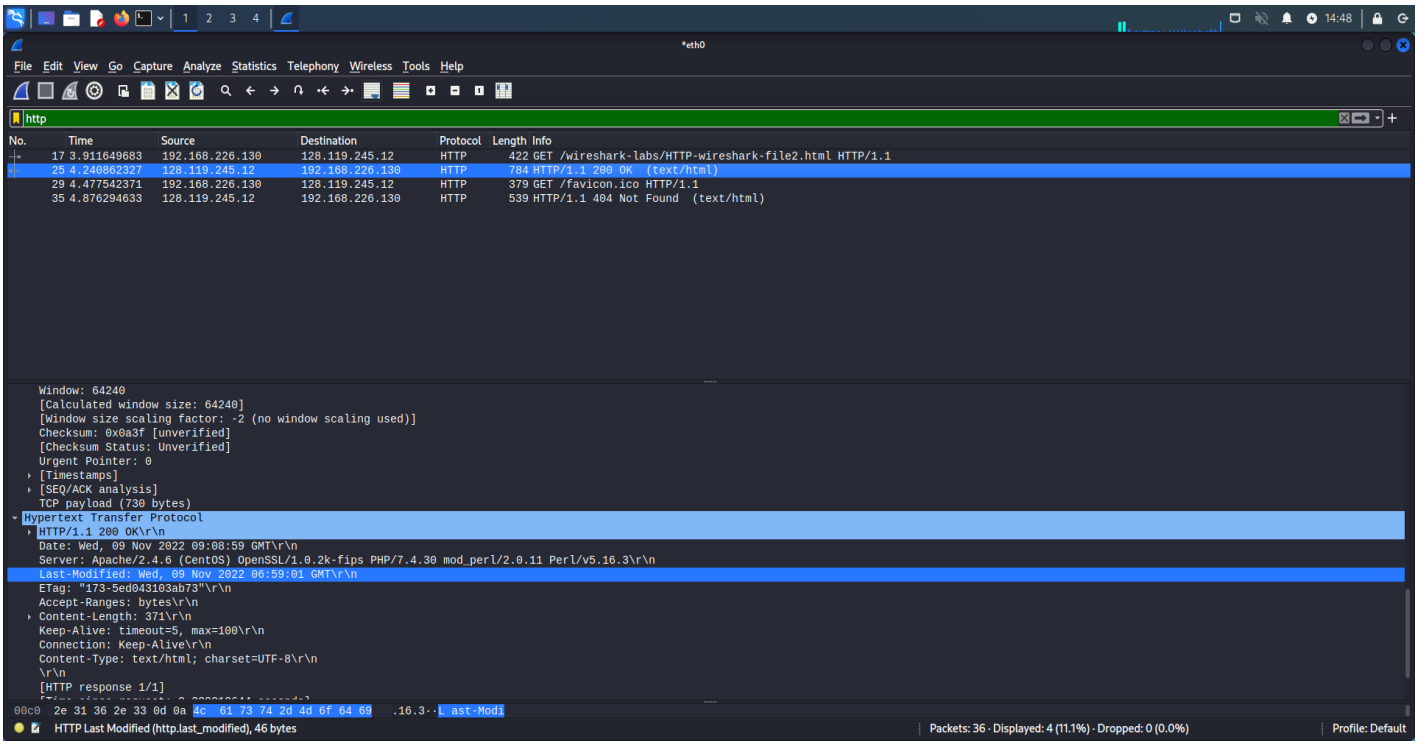
Ans 2:- Destination port : 53
Ans 3:- Source Port: 36935
Ans 4:- Destination IP address : 192.168.226.2 Yes they are same.
Ans 5:- analytics.ietf.org: type A, class IN, this data is present under “Domain Name System(Query)” Section under “Queries” .
Ans 6:- Under Domain Name System (response) are the Answers is Present, and 1 Answer is present and it’s Highlighted below:-

Transaction ID: 0x78b7
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
analytics.ietf.org: type A, class IN
Answers
analytics.ietf.org: type A, class IN, addr 50.223.129.196
Name: analytics.ietf.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 5 (5 seconds)
Data length: 4
Address: 50.223.129.196
[Request In: 20]
[Time: 0.010295651 seconds]

Ans 7:- No, because that Image requested is present on that server only.

LAB MANUAL – 2

All answers will be answered Using Below Screenshot :-



Ans 1,3:- From the Above Image we can see, “Last-Modified-Since” is present in response of HTTP in “200 Ok” status message, and there was no IF_MODIFIED_SINCE in HTTP GET response and the content is : **“Last-Modified: Wed, 09 Nov 2022 06:59:01 GMT\r\n”**.

Ans 2:- The content was provided under “Line based text data” header in HTTP 200 Ok (text/html) packet as highlighted below :-

Line-based text data: text/html (10 lines)
\n
<html>\n
\n
**Congratulations again! Now you've downloaded the file lab2-2.html.
\n**
This file's last modification date will not change. <p>\n
**Thus if you download this multiple times on your browser, a complete copy
\n**
**will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n**
field in your browser's HTTP GET request to the server.\n
\n
</html>\n

Ans 4:- In the second GET request there was not status code and phrase and content of the message was also not explicitly returned from the server.

LAST PAGE Q/A

Ans 1:- One HTTP GET request were present. And was sent to 118.215.154.3 IP address. And the response code was 388 that tell it was internally redirected to this address 142.250.182.3 Request address.

Ans 2:- The web browser has downloaded the image serially, can be verified by analysing timestamp of response from the server.

Ans 1 :- From the Above Image we can see the response message is transported using UDP(User Datagram packet).