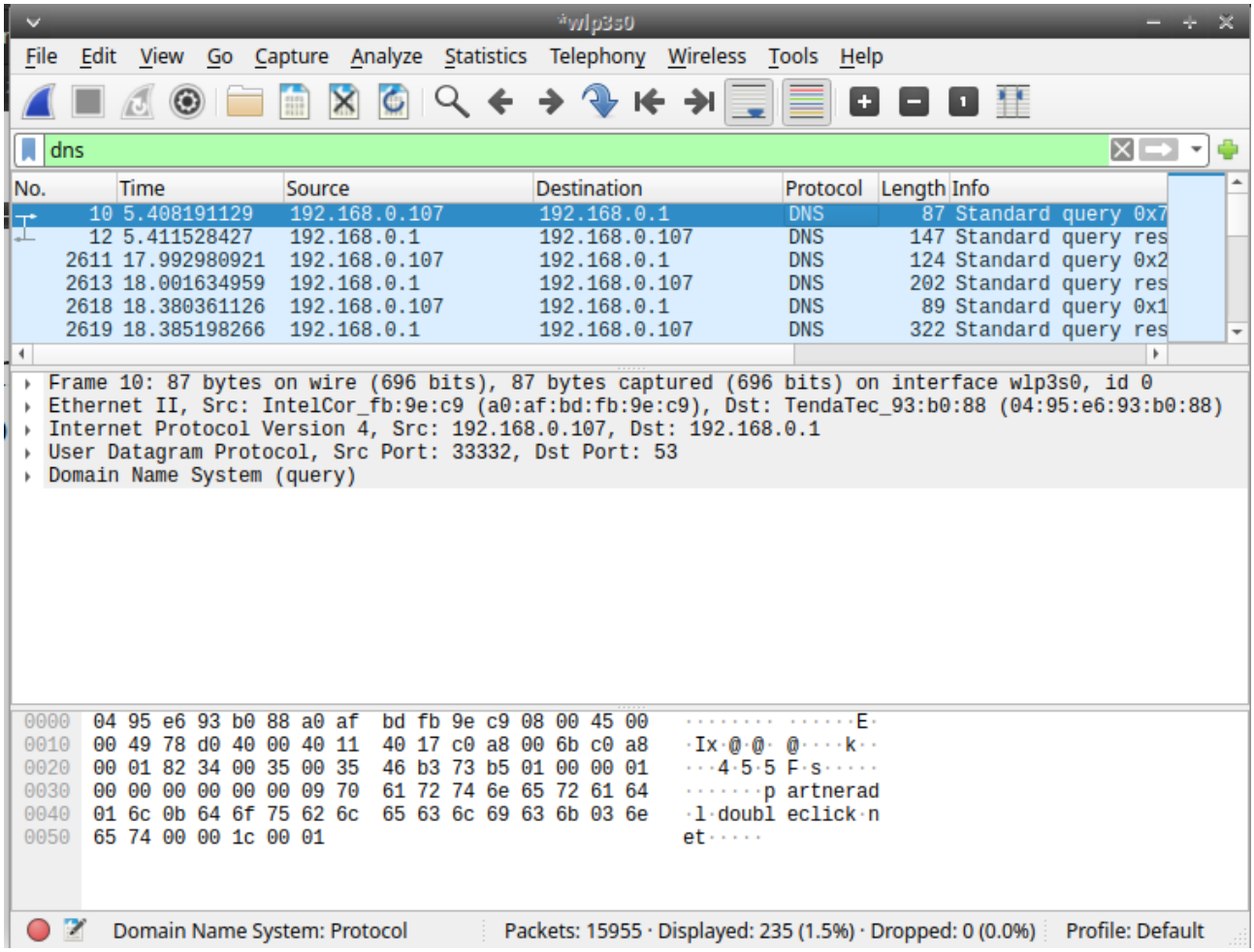
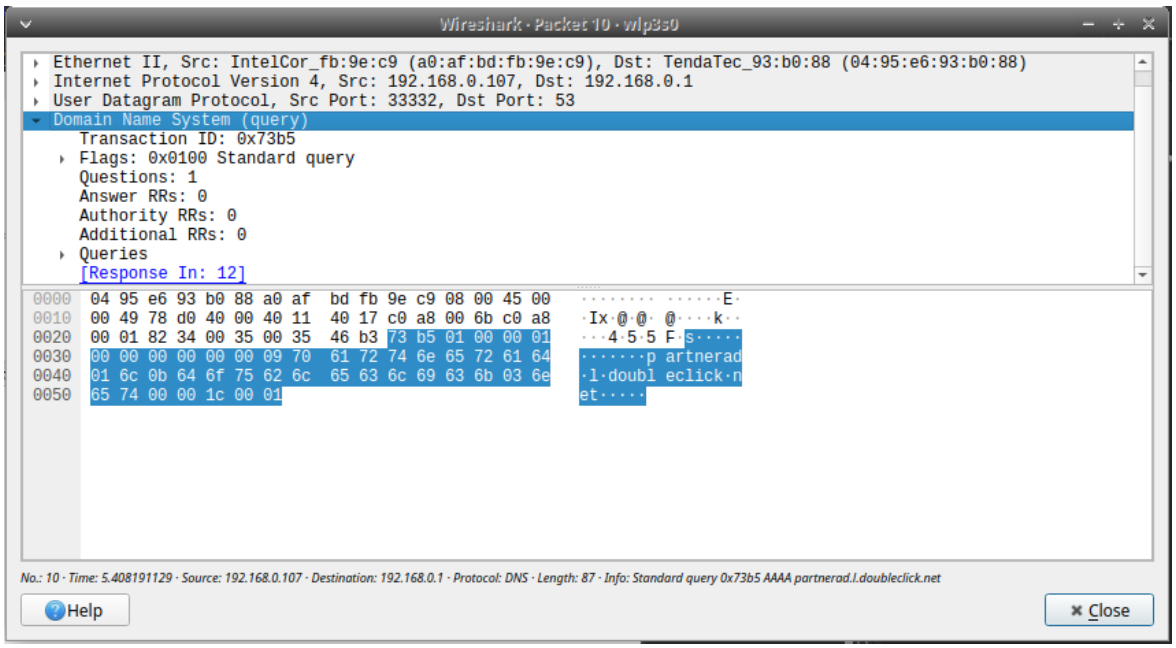
COMPUTER NETWORKS ASSIGNMENT (WIRESHARK)

Name:	Shubham Rawat
Roll No. :	26
Subject:	Computer Networks
Semester:	First
Batch:	2020 - 2022

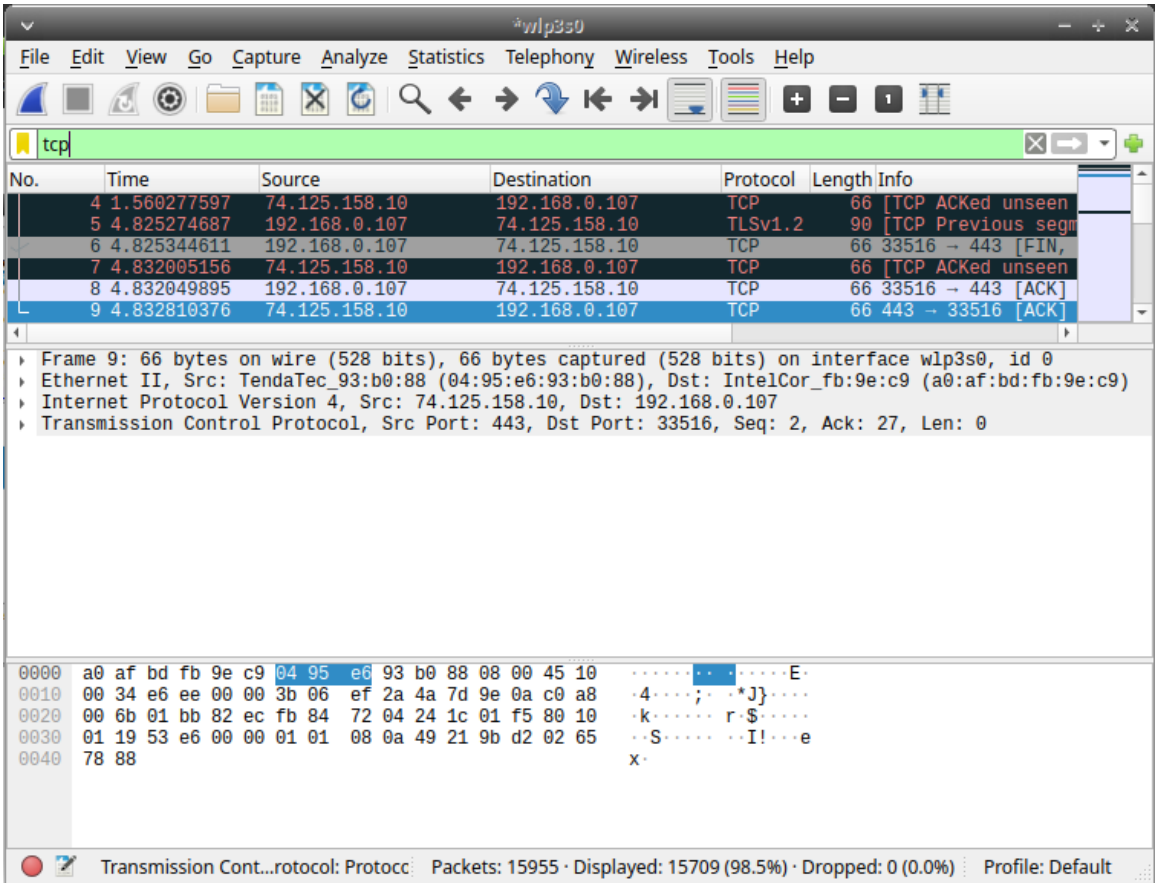
1. Find 3 different protocols that appear in the protocol list.

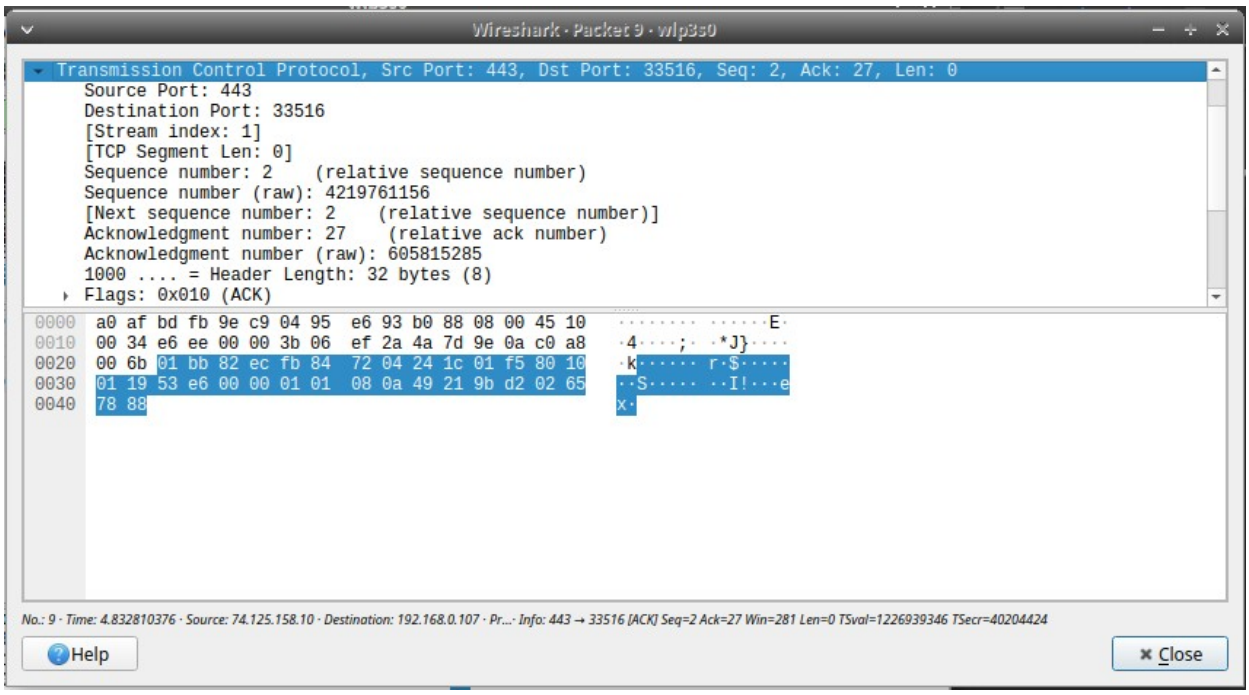
a. DNS



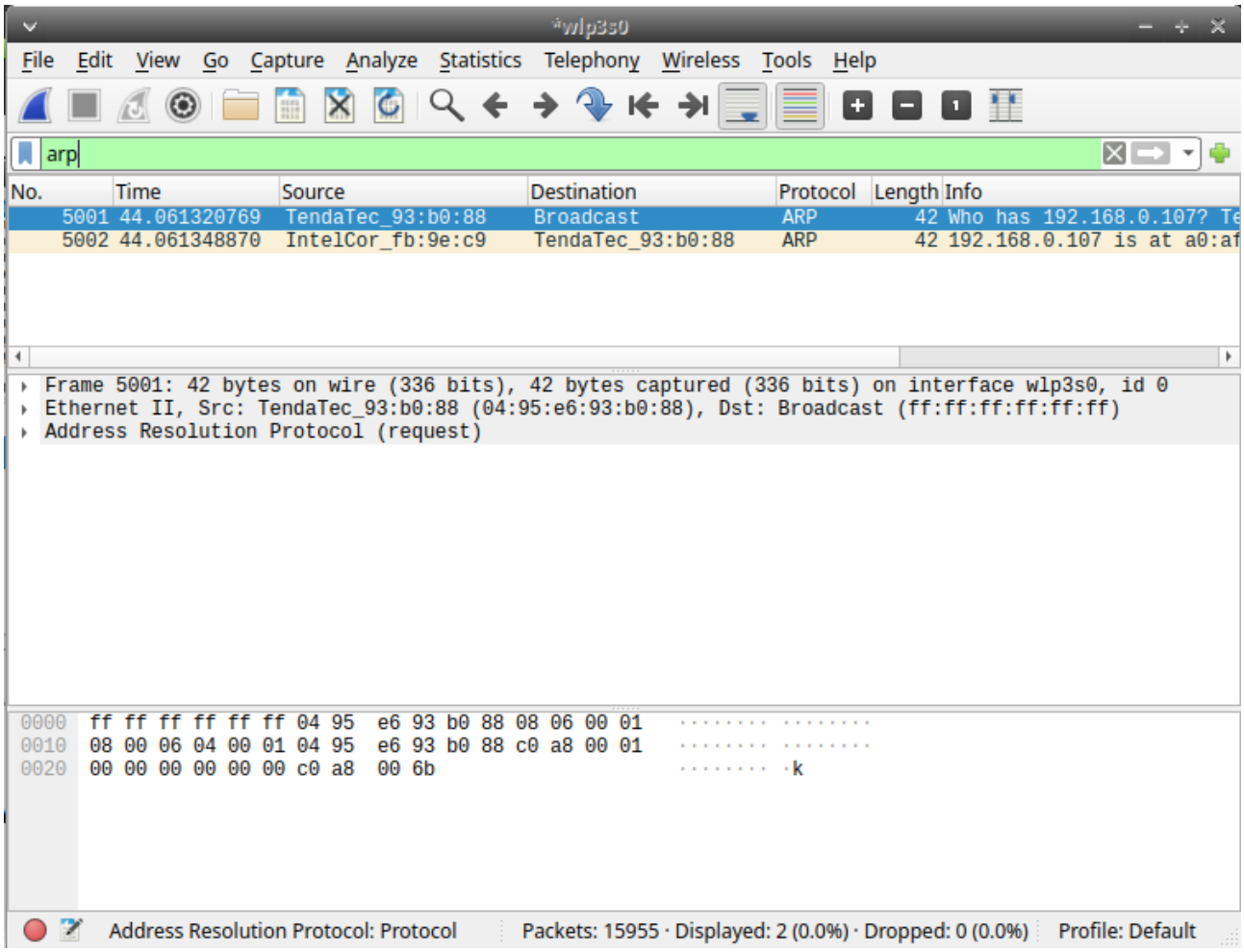

Wireshark · Packet 10 · wlp3s0
Ethernet II, Src: IntelCor_fb:9e:c9 (a0:af:bd:fb:9e:c9), Dst: TendaTec_93:b0:88 (04:95:e6:93:b0:88)
Internet Protocol Version 4, Src: 192.168.0.107, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 33332, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x73b5
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 12]
0000 04 95 e6 93 b0 88 a0 af bd fb 9e c9 08 00 45 00
0010 00 49 78 d0 40 00 40 11 40 17 c0 a8 00 6b c0 a8
0020 00 01 82 34 00 35 00 35 46 b3 73 b5 01 00 00 01
0030 00 00 00 00 00 00 09 70 61 72 74 6e 65 72 61 64
0040 01 6c 0b 64 6f 75 62 6c 65 63 6c 69 63 6b 03 6e
0050 65 74 00 00 1c 00 01
No.: 10 · Time: 5.408191129 · Source: 192.168.0.107 · Destination: 192.168.0.1 · Protocol: DNS · Length: 87 · Info: Standard query 0x73b5 AAAA partnerad.l.doubleclick.net
Help
Close

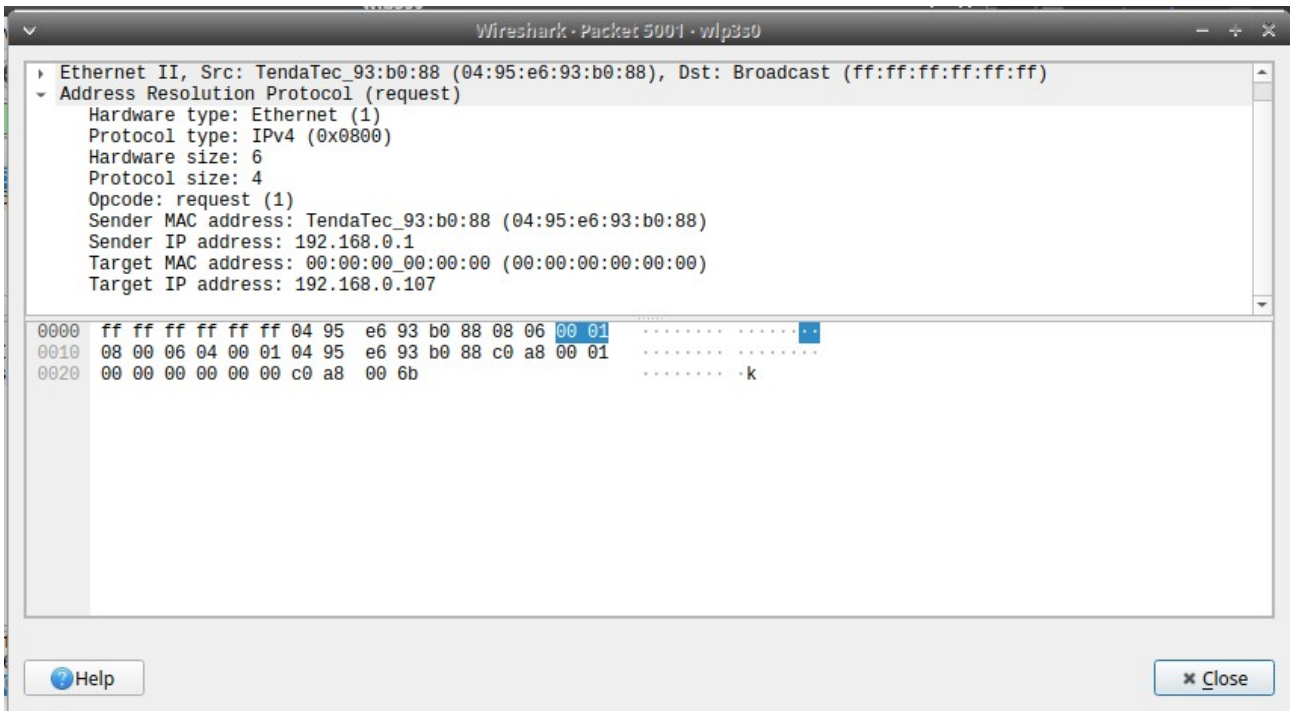
b. TCP


*wlp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
4 1.560277597 74.125.158.10 192.168.0.107 TCP 66 [TCP ACKed unseen
5 4.825274687 192.168.0.107 74.125.158.10 TLSv1.2 90 [TCP Previous segm
6 4.825344611 192.168.0.107 74.125.158.10 TCP 66 33516 → 443 [FIN,
7 4.832005156 74.125.158.10 192.168.0.107 TCP 66 [TCP ACKed unseen
8 4.832049895 192.168.0.107 74.125.158.10 TCP 66 33516 → 443 [ACK]
9 4.832810376 74.125.158.10 192.168.0.107 TCP 66 443 → 33516 [ACK]
Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp3s0, id 0
Ethernet II, Src: TendaTec_93:b0:88 (04:95:e6:93:b0:88), Dst: IntelCor_fb:9e:c9 (a0:af:bd:fb:9e:c9)
Internet Protocol Version 4, Src: 74.125.158.10, Dst: 192.168.0.107
Transmission Control Protocol, Src Port: 443, Dst Port: 33516, Seq: 2, Ack: 27, Len: 0
0000 a0 af bd fb 9e c9 04 95 e6 93 b0 88 08 00 45 10
0010 00 34 e6 ee 00 00 3b 06 ef 2a 4a 7d 9e 0a c0 a8
0020 00 6b 01 bb 82 ec fb 84 72 04 24 1c 01 f5 80 10
0030 01 19 53 e6 00 00 01 01 08 0a 49 21 9b d2 02 65
0040 78 88
Transmission Cont...rotocol: Protocc
Packets: 15955 · Displayed: 15709 (98.5%) · Dropped: 0 (0.0%)
Profile: Default


Wireshark · Packet 9 · wlp3s0
Transmission Control Protocol, Src Port: 443, Dst Port: 33516, Seq: 2, Ack: 27, Len: 0
Source Port: 443
Destination Port: 33516
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 2 (relative sequence number)
Sequence number (raw): 4219761156
[Next sequence number: 2 (relative sequence number)]
Acknowledgment number: 27 (relative ack number)
Acknowledgment number (raw): 605815285
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
0000 a0 af bd fb 9e c9 04 95 e6 93 b0 88 08 00 45 10
0010 00 34 e6 ee 00 00 3b 06 ef 2a 4a 7d 9e 0a c0 a8
0020 00 6b 01 bb 82 ec fb 84 72 04 24 1c 01 f5 80 10
0030 01 19 53 e6 00 00 01 01 08 0a 49 21 9b d2 02 65
0040 78 88
No.: 9 · Time: 4.832810376 · Source: 74.125.158.10 · Destination: 192.168.0.107 · Pr...· Info: 443 → 33516 [ACK] Seq=2 Ack=27 Win=281 Len=0 TSval=1226939346 TSecr=40204424
Help
Close

c. ARP

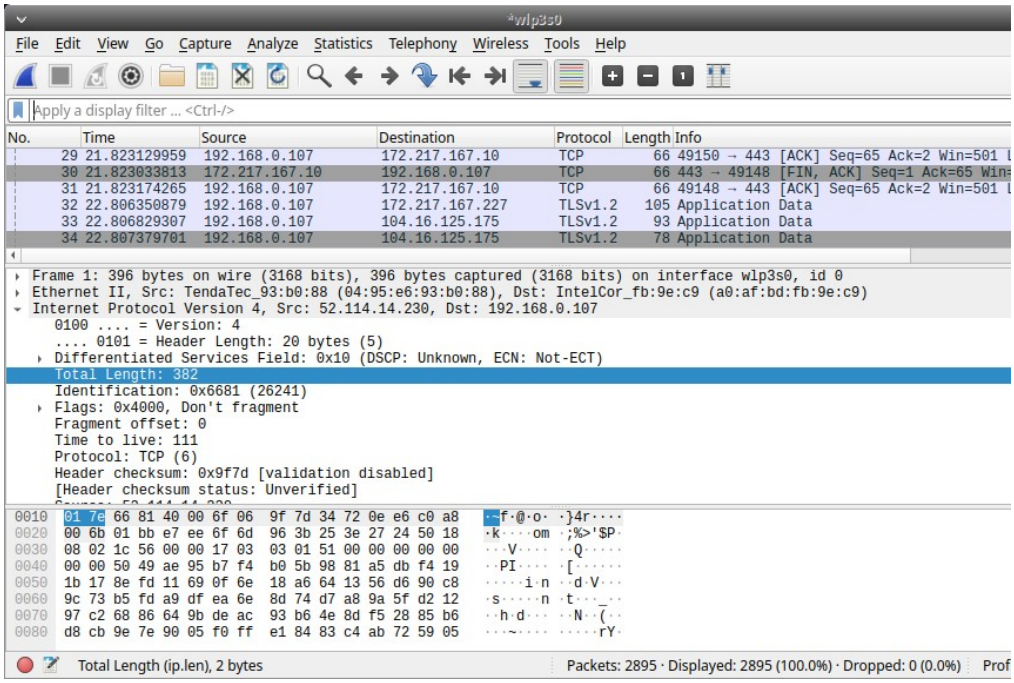

*wlp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
5001 44.061320769 TendaTec_93:b0:88 Broadcast ARP 42 Who has 192.168.0.107? Te
5002 44.061348870 IntelCor_fb:9e:c9 TendaTec_93:b0:88 ARP 42 192.168.0.107 is at a0:af
Frame 5001: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp3s0, id 0
Ethernet II, Src: TendaTec_93:b0:88 (04:95:e6:93:b0:88), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 04 95 e6 93 b0 88 08 06 00 01
0010 08 00 06 04 00 01 04 95 e6 93 b0 88 c0 a8 00 01
0020 00 00 00 00 00 00 c0 a8 00 6b
Address Resolution Protocol: Protocol
Packets: 15955 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default



2. Find the internet address of your computer and your server. Identity the internet address of any one homepage captured.

IP address of the computer - 192.168.0.107

IP of google home page - 172.217.167.14



Terminal - shubham@shubham-Vostro-3561: ~

File Edit View Terminal Tabs Help

```
;; MSG SIZE  rcvd: 54

shubham@shubham-Vostro-3561:~$ dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58763
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             1271    IN      A       172.217.167.14

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Jan 26 17:44:04 IST 2021
;; MSG SIZE  rcvd: 55

shubham@shubham-Vostro-3561:~$
```

*wlp3s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr ==172.217.167.10

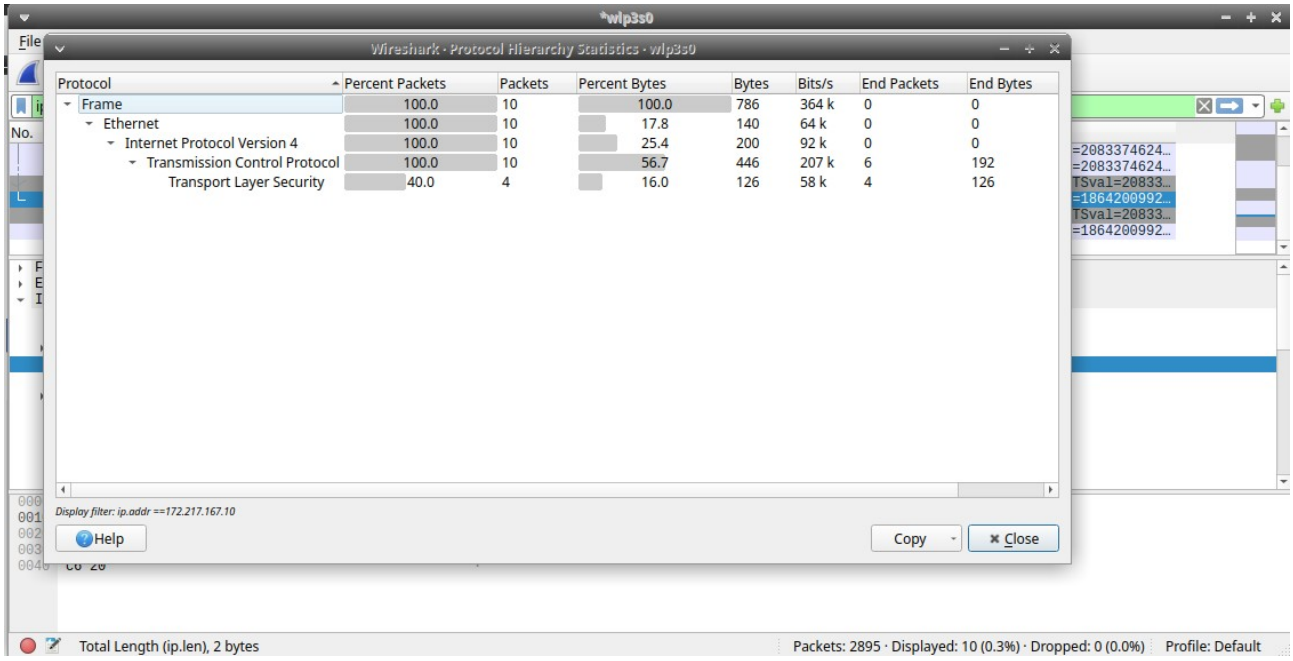
No.	Time	Source	Destination	Protocol	Length	Info
26	21.823033237	172.217.167.10	192.168.0.107	TCP	66	443 → 49150 [ACK] Seq=1 Ack=65 Win=273 Len=0 TSval=2083374624…
27	21.823033633	172.217.167.10	192.168.0.107	TCP	66	443 → 49148 [ACK] Seq=1 Ack=65 Win=273 Len=0 TSval=2083374624…
28	21.823033717	172.217.167.10	192.168.0.107	TCP	66	443 → 49150 [FIN, ACK] Seq=1 Ack=65 Win=273 Len=0 TSval=20833…
29	21.823129959	192.168.0.107	172.217.167.10	TCP	66	49150 → 443 [ACK] Seq=65 Ack=2 Win=501 Len=0 TSval=1864200992…
30	21.823033813	172.217.167.10	192.168.0.107	TCP	66	443 → 49148 [FIN, ACK] Seq=1 Ack=65 Win=273 Len=0 TSval=20833…
31	21.823174265	192.168.0.107	172.217.167.10	TCP	66	49148 → 443 [ACK] Seq=65 Ack=2 Win=501 Len=0 TSval=1864200992…

```
▸ Frame 29: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp3s0, id 0
▸ Ethernet II, Src: IntelCor_fb:9e:c9 (a0:af:bd:fb:9e:c9), Dst: TendaTec_93:b0:88 (04:95:e6:93:b0:88)
▾ Internet Protocol Version 4, Src: 192.168.0.107, Dst: 172.217.167.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x25cd [validation disabled]
    [Header checksum status: Unverified]

0000  04 95 e6 93 b0 88 a0 af  bd fb 9e c9 08 00 45 00   ······· ·····E·
0010  00 34 00 00 40 00 40 06  25 cd c0 a8 00 6b ac d9   ·4··@·@· %····k··
0020  a7 0a bf fe 01 bb cf c5  93 ae 3b 5f 59 b6 80 10   ····· ··;_Y···
0030  01 f5 81 01 00 00 01 01  08 0a 6f 1d 73 20 7c 2d   ····· ··o·s |-
0040  c6 20                                              ·
```

Total Length (ip.len), 2 bytes Packets: 2895 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%) Profile: Default

3. Find and capture the protocol hierarchy for a UDP/ SSDP segment.

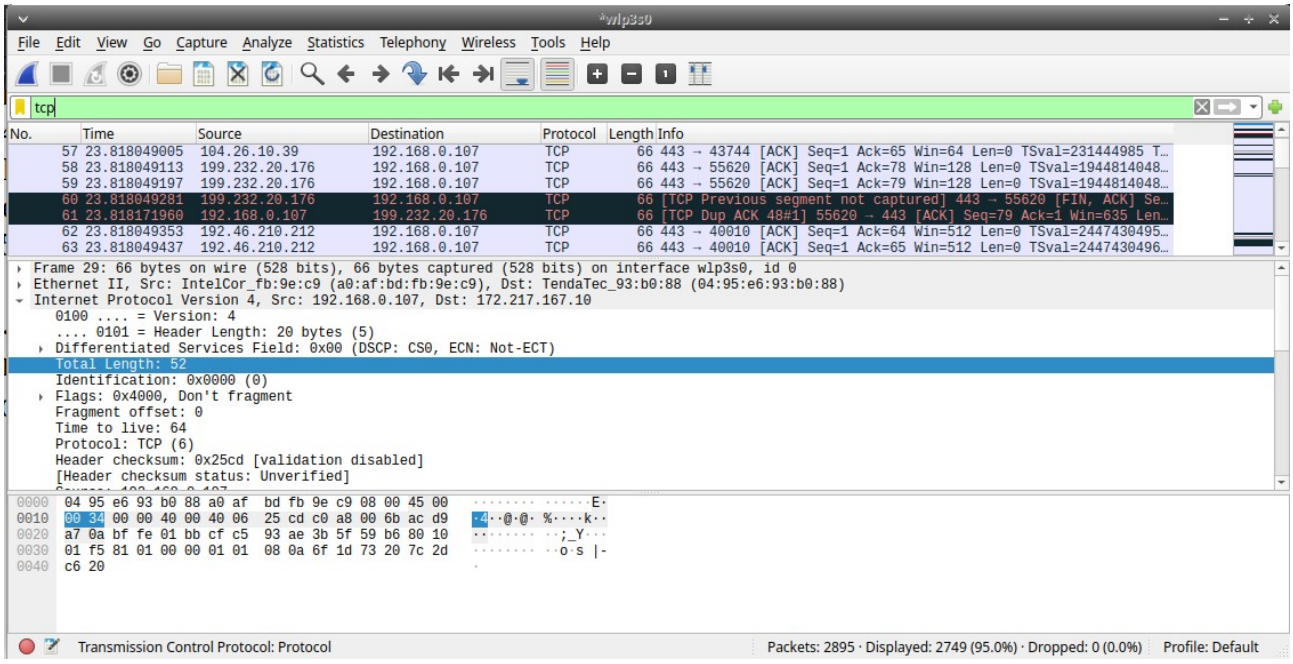


"Protocol","Percent Packets","Packets","Percent Bytes","Bytes","Bits/s","End Packets","End Bytes","End Bits/s"
"Frame",100,10,100,786,364833.0827500346,0,0,0
"Ethernet",100,10,17.8117048346056,140,64982.99183842855,0,0,0
"Internet Protocol Version 4",100,10,25.44529262086514,200,92832.84548346935,0,0,0
"Transmission Control Protocol",100,10,56.74300254452926,446,207017.24542813667,6,192,89119.53166413058

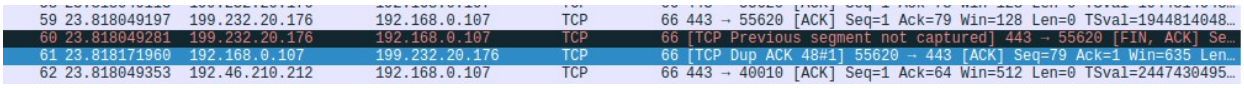
"Transport Layer Security",40,4,16.03053435114504,126,58484.6926545857,4,126,58484.6926545857

4. Apply display filter to show all TCP segments on an interface. Also state what does black coloured TCP Segments indicate?

a.



b. Black TCP segment indicate what



The packet highlight in black identifies that the TCP packet with problem – for example ,they could have been delivered out of the order.

5. Identify the time difference between a set of DNS query and its DNS response. Show it with the help of an example

DNS query to ISP time 91.895391378
DNS response from ISP time 91.916807185