ABINASH GUPTA
120CS0157
COMPUTER NETWORKS LAB -3

Q1 . 1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
Ans -

```
  7 03:27:43.033671 Cisco_83:e4:54      Broadcast           ARP          60 Who has 128.238.38.38? Tell 128.238.38.
  8 03:27:43.582042 128.238.38.160      128.238.29.23       DNS          72 Standard query 0x006e A www.ietf.org
  9 03:27:43.582886 128.238.29.23       128.238.38.160      DNS         104 Standard query response 0x006e A www.ie
```

It is sent over UDP .

```
▾ Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 90
    Identification: 0xd595 (54677)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 126
    Protocol: UDP (17)
    Header Checksum: 0x216a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.238.29.23
    Destination Address: 128.238.38.160
```

Q2 .What is the destination port for the DNS query message? What is the source port of DNS response message?
Ans - Both are 53 .
Query:

```
▸ Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
▸ Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
▸ Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
▾ User Datagram Protocol, Src Port: 3163, Dst Port: 53
    Source Port: 3163
    Destination Port: 53
```

Response msg :

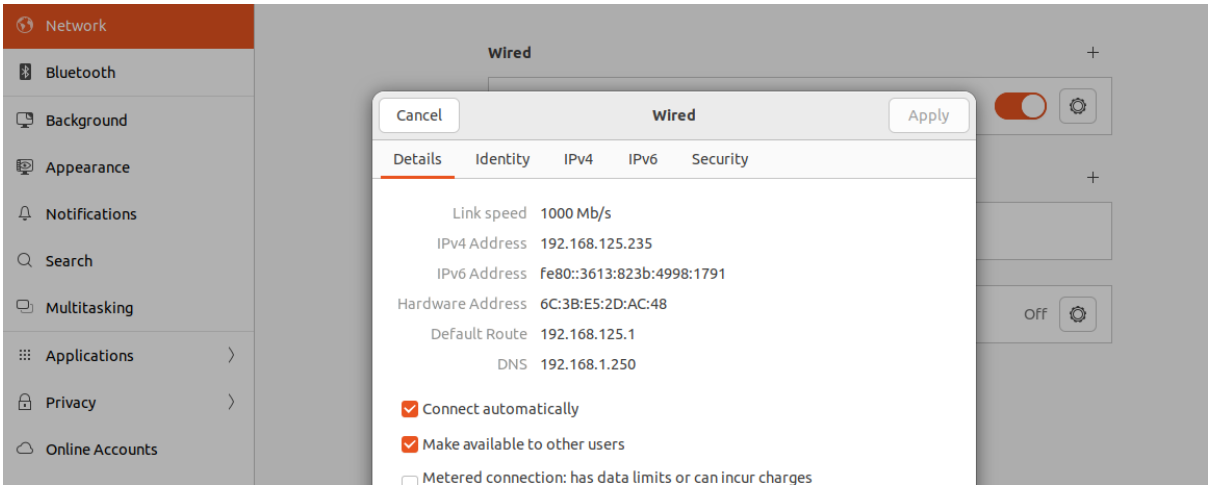
```
▸ Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
▸ Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
▸ Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160
▾ User Datagram Protocol, Src Port: 53, Dst Port: 3163
    Source Port: 53
    Destination Port: 3163
```

Q3 : To what IP address is the DNS query message sent? Use nm-tool command to determine
the IP address of your local DNS server. Are these two IP addresses the same?

Ans :- Query Destination: 128.238.29.23

```
  7 03:27:43.033671 Cisco_83:e4:54   Broadcast          ARP      60 Who has 128.238.38.38? Tell 128.238.38.
  8 03:27:43.582042 128.238.38.160   128.238.29.23      DNS      72 Standard query 0x006e A www.ietf.org
  9 03:27:43.582886 128.238.29.23    128.238.38.160     DNS     104 Standard query response 0x006e A www.ie
```

Local DNS : 192.168.1.250



They are different .

Q4 . Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans : Type A

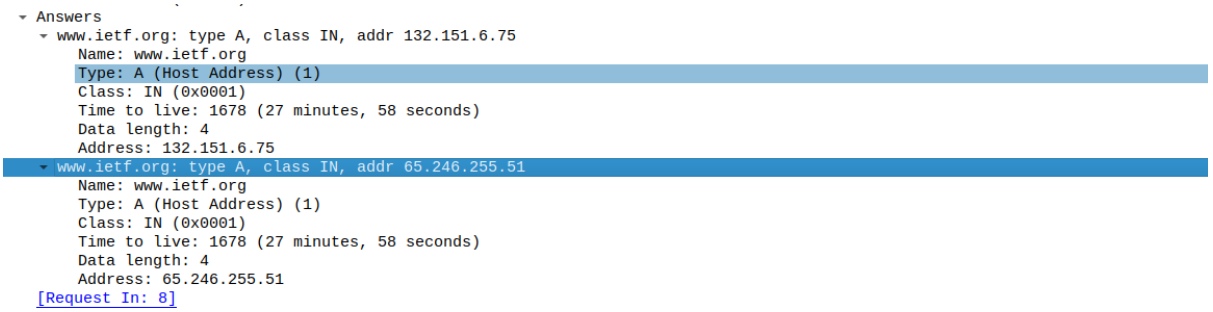
The query does not contain any answer .

```
Transaction ID: 0x006e
▸ Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▾ Queries
  ▾ www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 9]
```

Q5 . Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans - 2 answers are there

The contains of answers : address of the query
type , time span and message length and the destination address



Q6 . Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans - Yes It matches with the IP Address of the first answer provided in response msg .

Q7 . This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Ans : No

Q2: Answer the following questions for captured file tcp.pcap (TCP Protocol)

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

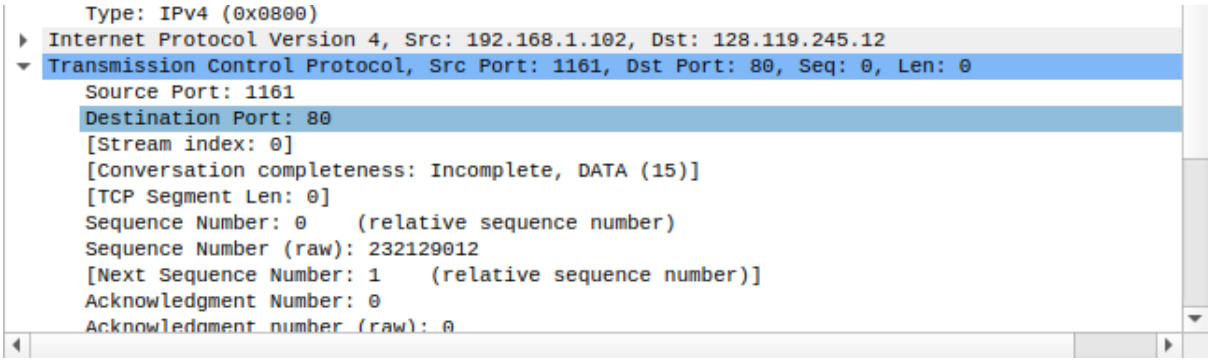
Ans : IP Address : 192.168.102
Port Number : 1161

2 .What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Ans - The destination IP address is 128.119.245.12 receiving on port 80
3 .What is the IP address and TCP port number used by your client computer (source) to
transfer the file to gaia.cs.umass.edu?
Ans :- IP Address : 192.168.1.102
Port Number 1161

4 . What is the sequence number of the TCP SYN segment that is used to initiate the TCP
connection between the client computer and
gaia.cs.umass.edu? What is it in the segment
that identifies the segment as a SYN segment?

Ans -
Seq Number 0



5 . What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

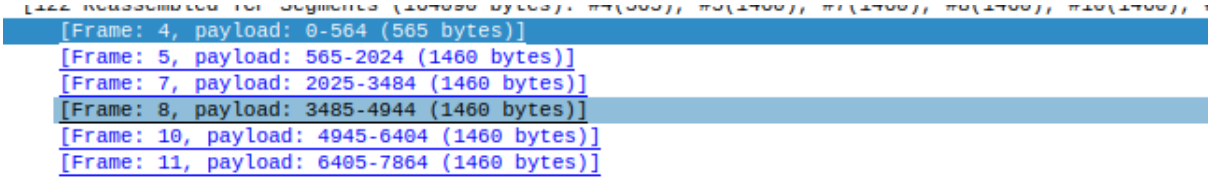
Ans -

- The sequence number of the SYNACK segment is 0.
- The value of the acknowledgement field is 1. This value is determined by the initial sequence number +1.
- The message carries flags that show it to be a SYN ACK message.

6 .What is the sequence number of the TCP segment containing the HTTP POST
command? Note that in order to find the POST command; you'll need to dig into the
packet content field at the bottom of the Wireshark window, looking for a segment with a
"POST" within its DATA field .
Ans -
Seq Number 164041

**7 .Consider the TCP segment containing the HTTP POST as the first segment in the TCP
connection. What is the length of each of the first six TCP segments?**

Ans -



Length of 1st TCP segment 565 Bytes
Length of 2ndTCP segment 1460 Bytes
Length of 3rd TCP segment 1460 Bytes
Length of 4thTCP segment 1460 Bytes
Length of 5th TCP segment 1460 Bytes
Length of 6th TCP segment 1460 Bytes

8 .What is the EstimatedRTTvalue (see Section 3.5.3, page 239 in text from Kurose Book) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment. [Hint:Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server.Select as Statistics->TCP Stream Graph->Round Trip Time Graph.]

The HTTP POST segment is considered as the first segment.
Segments 1 – 6 are
No. 4, 5, 7, 8, 10, and 11 in this trace respectively. The ACKs of segments 1 – 6 are
No. 6, 9, 12, 14, 15, and 16 in this trace.

	Sent time	ACK Received time	RTT (seconds)
Segment 1	0.026477	0.053937	0.02746
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.11443
Segment 5	0.077405	0.217299	0.13989

Segment 6 0.078157 0.267802 0.18964

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT
EstimatedRTT after the receipt of the ACK of segment 1:
EstimatedRTT = RTT for Segment 1 = 0.02746 second
EstimatedRTT after the receipt of the ACK of segment 2:
EstimatedRTT = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.0285
EstimatedRTT after the receipt of the ACK of segment 3:
EstimatedRTT = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337
EstimatedRTT after the receipt of the ACK of segment 4:
EstimatedRTT = 0.875 * 0.0337+ 0.125 * 0.11443 = 0.0438
EstimatedRTT after the receipt of the ACK of segment 5:
EstimatedRTT = 0.875 * 0.0438 + 0.125 * 0.13989 = 0.0558
EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725 second

Ans - 0.0725 seconds