Computer Networks
Lab Assignment 3 Report

Karthik Kancharla
190020020

February 1, 2021

Questions

1) The protocols used by the application(Google Hangouts) at different layers are:

   - TCP (Transport Layer)
   - DNS (Application Layer)
   - TLSv1.2, TLSv1.3.(Transport and Application Layer)
   - UDP (Transport Layer)
   - I didn't find http protocol due to redirection to https.
   - I was getting OCSP packets sometimes, not some other times.(Please check in trace files if needed)

2)

- For TCP Protocol:

  Source IP Address: 10.0.2.15,
  Destination IP Address: 172.217.26.14
  Source Port: 39722,
  Destination Port: 443
  Sequence Number: 10028,
  Acknowledgement Number: 146346,
  Window Size: 65535,
  TCP Segment Length: 0
  Protocol Number: 6
  Ethernet Address Source: PcCompuc3:f4:34 (08:00:27:c3:f4:34)
  Ethernet Address Destination: RealtekU12:35:02 (52:54:00:12:35:02)

- For DNS Protocol:

  Source IP Address: 10.0.2.15,
  Destination IP Address: 172.217.26.14
  Protocol Number: 17(UDP) Source Port: 41320,
  Destination Port: 53,
  Length Captured: 79,
  Transaction ID: 0xcfd6,
  Type: Standard Query
  Ethernet Address Source: PcCompuc3:f4:34 (08:00:27:c3:f4:34)
  Ethernet Address Destination: RealtekU12:35:02 (52:54:00:12:35:02)

- For TLSv1.3 Protocol:

  Source IP Address: 10.0.2.15,
  Destination IP Address: 142.250.67.35
  Length Captured: 689 bytes
  Type: Client Hello,
  Protocol Number: 6(TCP)
  Ethernet Address Destination: PcCompuc3:f4:34 (08:00:27:c3:f4:34)
  Ethernet Address Source: RealtekU12:35:02 (52:54:00:12:35:02)

- For TLSv1.2 Protocol:

  Source IP Address: 34.214.254.242,
  Destination IP Address: 10.0.2.15
  Length Captured: 199 bytes
  Ethernet Address Source: PcCompuc3:f4:34 (08:00:27:c3:f4:34)
  Ethernet Address Destination: RealtekU12:35:02 (52:54:00:12:35:02)
  Info about Transport Layer Security: Handshake Protocol: Server Hello, Change Cipher Spec Protocol: Change Cipher Spec, Handshake Protocol: Encrypted Handshake Message

3) - First Activity: Sending and receiving messages.

  From the line 10 to line 12 we can see a TCP three-way handshake. In line 10, synchronise request is sent from source to destination, in line 11, acknowledgement and synchronize request is sent from the destination confirming it's active, then In line 12 acknowledgement is sent from source to destination.
  In lines 13,15,17 we can see a TLS handshake happening between server and client using client hello, server hello, Change Cipher Spec, Change Cipher Spec finished.

- Second activity : Video Calling.

  From the line 5 to line 7 we can see a TCP three-way handshake.In line 5, synchronise request is sent from source to destination, inline 6, acknowledgement and synchronize request is sent from thedestination confirming it's active, then In line 7 acknowledgementis sent from source to destination.

  In lines 8,10,12 we can see a TLS handshake happening between server and client using client hello, server hello, Change Cipher Spec, Change Cipher Spec finished.

  Same as above TCP 3 way handhakes and TLS hanshakes are observed for different activities at different scenarios.

4) Protocols observed in part 1 and their uses:

Protocol Name	Use of the Protocol
TCP	This first establishes a connection between source and destination. It ensures first that connection is possible and then using a 3 way handshake establishes a connection. It ensures no packet loss while sending messages and talking in hangouts. It ensures that there is no loss in messages while sending.
DNS	It helps the computer to get to the ip address from the given domain name and with this we can establish a connection between source and destination.
TLS	It is the Transport layer security protocol. As the name says it provides end-to-end security of the data sent between source and destination. For example it doesn't allow any random person read the messages sent on google hangouts and securely transfers it only to the desired person.
UDP	User Diagram Protocol is used for the processes which can tolerate some packet loss and should be fast. For example in the video call a little of voice cut can be accepted, so sometimes this can be used when connection is bad and should be fast and when little packet loss can be accepted.

5) At first time of day:

- Throughput = Bytes/Timespan = 1690124/24.372 = 69346.955 bytes/sec
  Number of UDP packets is 130.
  Number of TCP packets is 1364.
  There were 3 packets in black colour which indeed shows the lost packets. So, No. of packets lost = 3.
  RTT = 0.065582893 seconds
  No. of responses per one request is 1.
  Packet Length: 74

At second time of day:

- Throughput = Bytes/Timespan = 1556788/24.180 = 64383.291 bytes/sec
  Number of UDP packets is 1328.
  Number of TCP packets is 1486.
  There were 3 packets in black colour which indeed shows the lost packets. So, No. of packets lost = 1.
  RTT = 0.000549489 seconds
  No. of responses per one request is 1.
  Packet Length : 54

6) Yes, there are multiple servers as you can see in the screenshots. This happens because of many events in all these packets. One of them is sign in, i.e verifying your own account, then one of them is for receiving messages from other persons, one of them is for showing people online etc., So, there are many IP addresses all of which correspond to different activities but are of the same company google. From each different server of google, each activity of the required task is performed, so there are multiple IP addresses found in the wireshark packets list.