CS 39006: Networks Lab

Assignment 1: Use Wireshark for Analyzing Network Packet Traces

Assignment Date: 11th January, 2018

Lab Report by:

Prajwal Singhania – 15CS30043

Tanay Bhartia - 15CS30036

Aim:

The objective of this assignment was to understand the Wireshark tool and the analysis of network packet traces(using UDP and TCP protocols at the Transport Layer) using the tool

Methodolody:

The following commands were run on the shell:

- UDP Client(with 28Kbits/sec) : **iperf -c 10.5.20.128 -u -b 28000**
- TCP Client : **wget --no-proxy http://10.5.20.128:8000/pic1.jpg**

The packets were captured using Wireshark tool with the filter:

ip.addr == 10.5.20.128

Further observations were made changing the bandwidth in the UDP analysis and for different pictures(pic1 to pic5) in the TCP analysis

Questions:

1. List the different protocols that you observe in the packet trace, at application, transport and network layer for each of the UDP and TCP test cases.

Ans.

Different protocols observed in the packet trace, at application, transport and network layer of **UDP** are:

Nil at Application Layer,
UDP at Transport Layer,
IPv4 at Network Layer.

Different protocols observed in the packet trace, at application, transport and network layer of all **TCP** test cases are:

HTTP at Application Layer,
UDP at Transport Layer,
IPv4 at Network Layer.

2. (a) How many TCP packets are transferred for each cases while accessing the files pic1.jpg to pic5.jpg? Are all the packets of same size? What are the different packet size you observe for each of the file access?

Ans.

Pic 1:

21 packets are transferred. All the packets are not of the same size. Different packet sizes observed are(all in bytes): 66, 74, 83, 217, 1514, 5128, 7306, 11650, 14546.

Pic 2:

4549 packets are transferred. All the packets are not of the same size. Different packet sizes observed are(all in bytes): 66, 74, 78, 86, 94, 217, 1514, 2962, 4410, 5858, 7306, 8421, 8754, 10202, 11650, 13098, 14546, 15994, 17442, 18890, 20338, 21786, 23234, 24682, 26130, 27578, 34818.

Pic 3:

217 packets are transferred. All the packets are not of the same size. Different packet sizes observed are(all in bytes): 66, 74, 217, 635, 1514, 2962, 4410, 5858, 7306, 8754, 10202, 11650, 13098, 15994.

Pic 4:

994 packets are transferred. All the packets are not of the same size. Different packet sizes observed are(all in bytes): 66, 74, 217, 1514, 2794, 2962, 4410, 5858, 7306, 8754, 10202, 11650, 13098, 14546, 15994, 17442, 18890, 20338, 21786, 23234, 24682, 29026, 30474, 33370.

Pic 5:

155 packets are transferred. All the packets are not of the same size. Different packet sizes observed are(all in bytes): 66, 74, 83, 217, 1514, 2962, 4410, 5858, 6945, 7306, 8754, 10202, 11650, 13098, 14546, 15994, 17442, 18890, 20338.

Justification: The TCP protocol has the concept of handshake and acknowledgements which provide a relaibility on the data being transferred but due to this, every packet is not a data packet and there are acknowledgement packets, packets to set up the connection, etc. as well due to which we observe different packet sizes

2. (b) For the test case with UDP, are all the UDP packets of same size? If not, what are the different UDP packet sizes you observe?

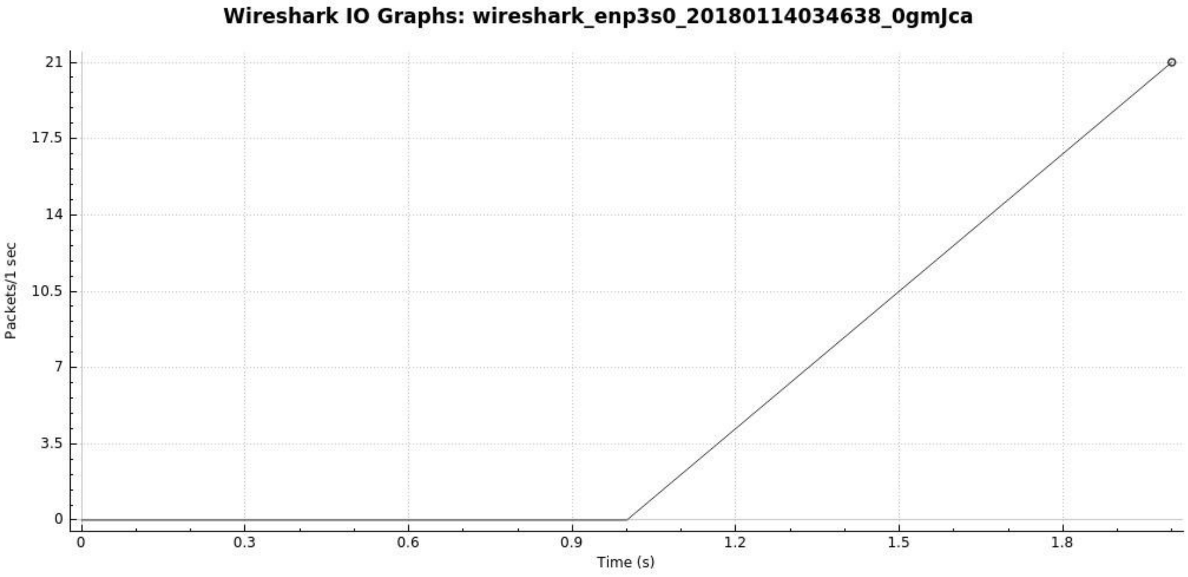
Ans. Yes, all the UDP packet are of same size. Packet size = 1470 bytes.

Justification: The UDP protocol has no concept of handshake and acknowledgements and so only data packets are transferred without any congestion control as well. So we observe packet sizes to be same.

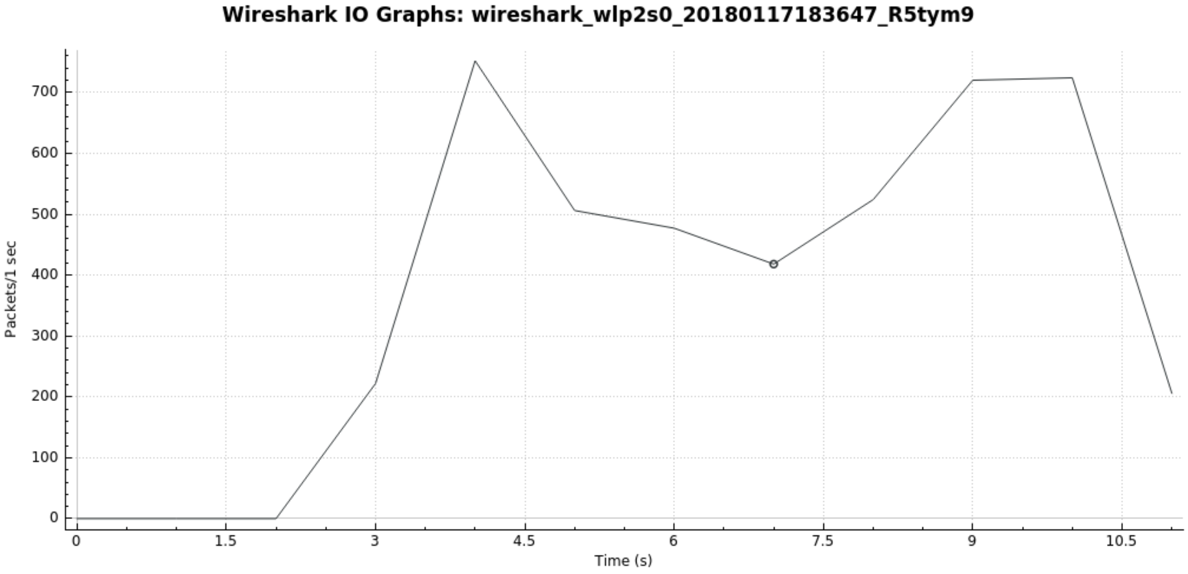
2. (c) Observe the TCP and the UDP throughput using Wireshark (Menu->Statistics->IO Graphs), as shown in the following figure.

Ans.

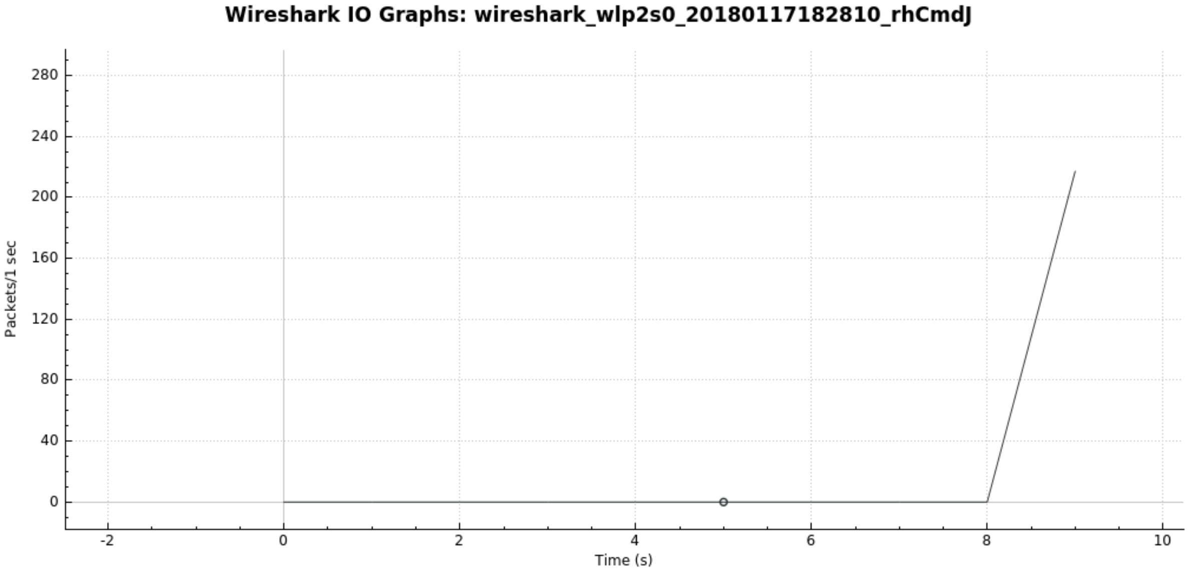
TCP Pic-1:



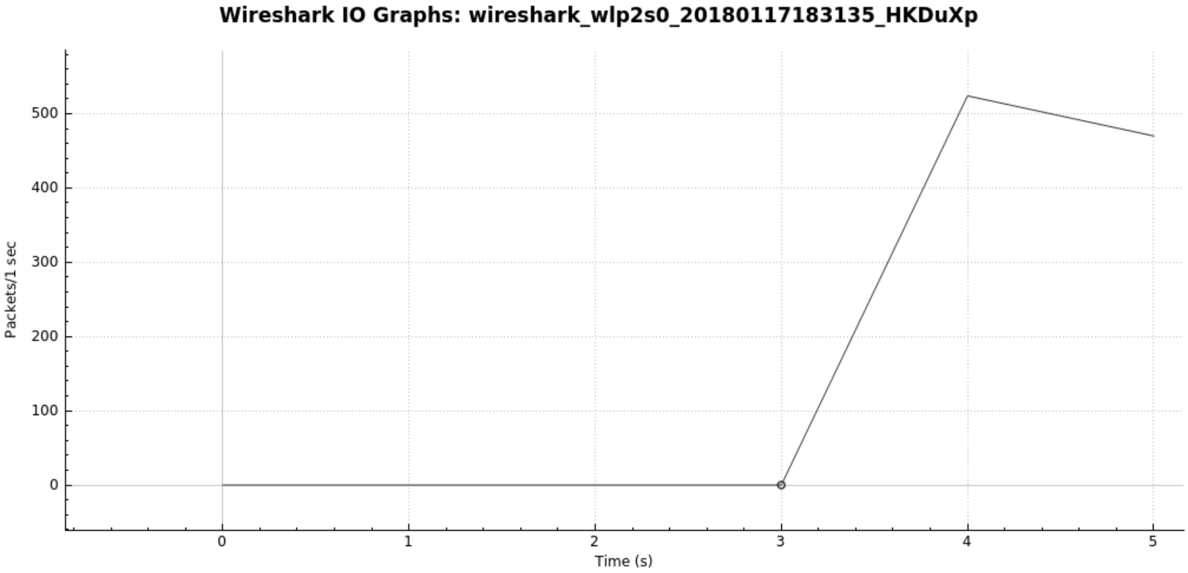
TCP Pic-2:



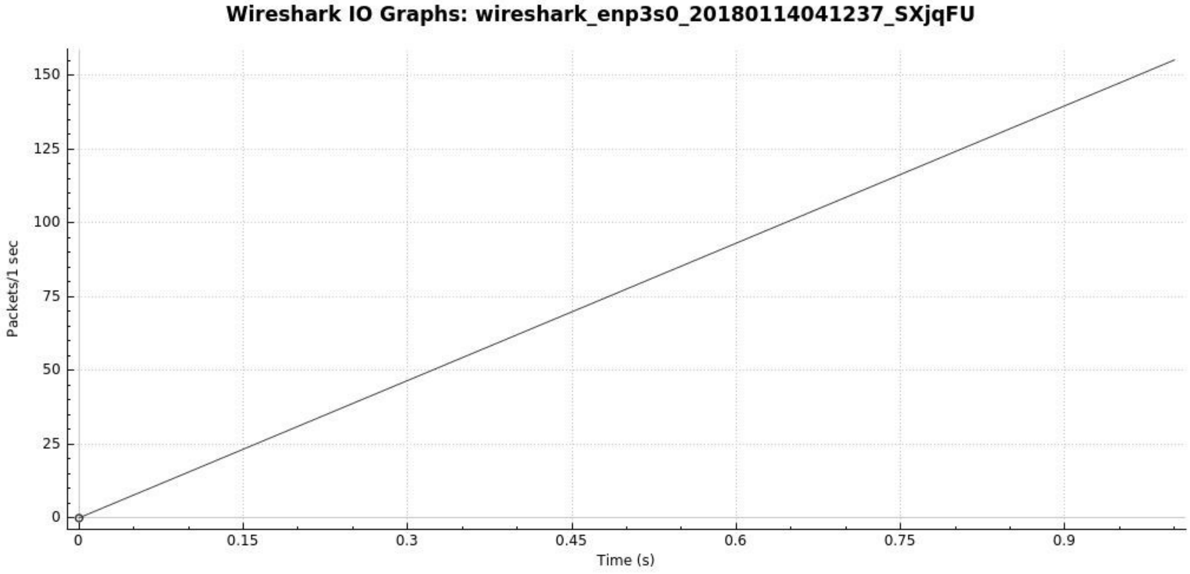
TCP Pic-3:



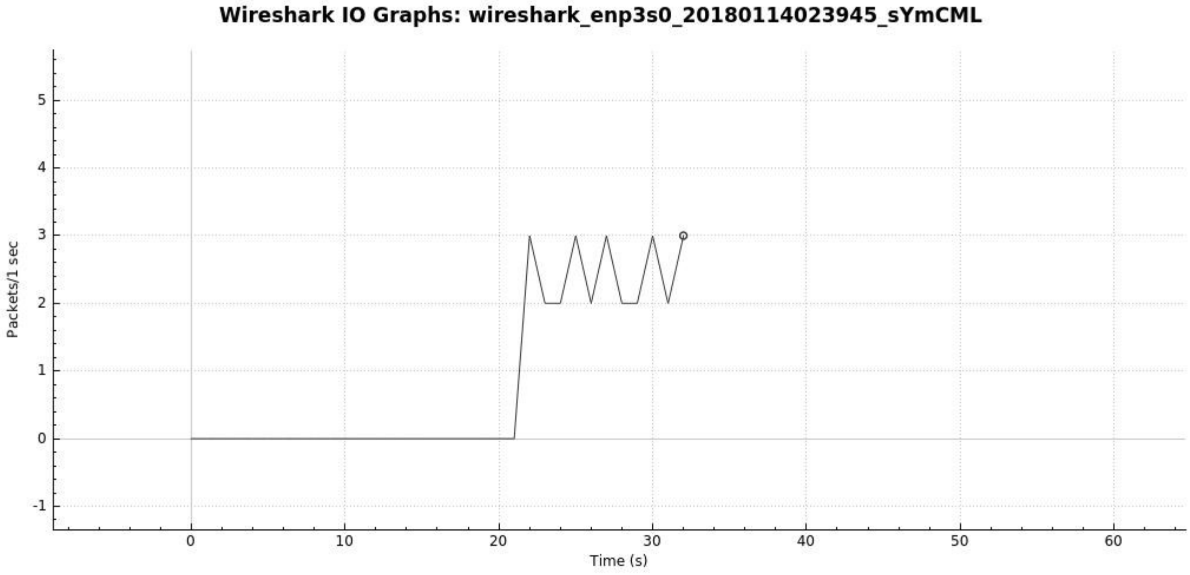
TCP Pic-4:



TCP Pic-5:



UDP 28 Kbps:



Justification: Pic2 for the TCP connection was the largest and thus had the most number of data packets transmitted and took the largest amount of completion time and it was much likely for the throughput to fluctuate due to fluctuations in the internet connection speed.

2. (d) Compute the UDP throughput (amount of UDP data received per second) for following cases of UDP traffic generation rates (bandwidth).

Ans.

Data Rate(As observed in Wireshark):

(i) 64 Kbps - 67 Kbps

(ii) 128 Kbps – 132 Kbps

(iii) 256 Kbps – 264 Kbps

(iv) 512 Kbps – 527 Kbps

(v) 1024 Kbps – 1054 Kbps

(vi) 2048 Kbps – 2107 Kbps

Throughput (As reported by iperf):

(i) 64 Kbps - 64 Kbps

(ii) 128 Kbps – 128 Kbps

(iii) 256 Kbps – 256 Kbps

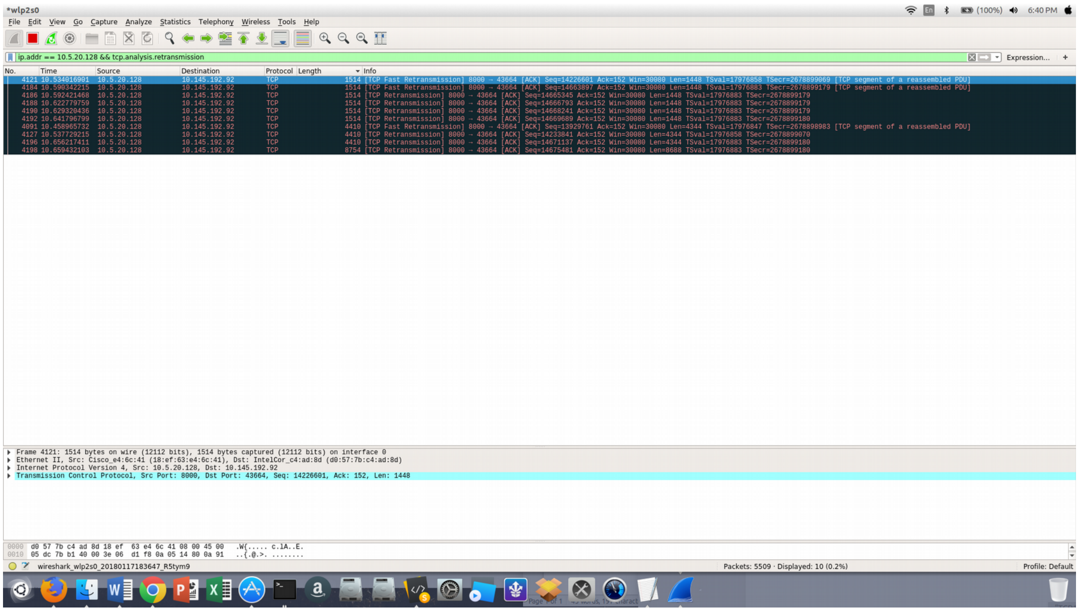
(iv) 512 Kbps – 512 Kbps

(v) 1024 Kbps – 1024 Kbps

(vi) 2048 Kbps – 2048 Kbps

3. Analyze the number of TCP packets retransmitted from Wireshark, as shown in figure below.

Ans. TCP packets were retransmitted only for 2nd pic. A total of 10 packets were retransmitted.


*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
En
(100%)
6:40 PM
Expression…
+

```
ip.addr == 10.5.20.128 && tcp.analysis.retransmission
```

```
No.    Time         Source        Destination     Protocol Length  Info
  4121 10.534016901 10.5.20.128   10.145.192.92   TCP        1514 [TCP Fast Retransmission] 8000 → 43664 [ACK] Seq=14226601 Ack=152 Win=30080 Len=1448 TSval=17976858 TSecr=2678899069 [TCP segment of a reassembled PDU]
  4184 10.590342215 10.5.20.128   10.145.192.92   TCP        1514 [TCP Fast Retransmission] 8000 → 43664 [ACK] Seq=14663897 Ack=152 Win=30080 Len=1448 TSval=17976883 TSecr=2678899179 [TCP segment of a reassembled PDU]
  4186 10.592421468 10.5.20.128   10.145.192.92   TCP        1514 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14665345 Ack=152 Win=30080 Len=1448 TSval=17976883 TSecr=2678899179
  4188 10.622779759 10.5.20.128   10.145.192.92   TCP        1514 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14666793 Ack=152 Win=30080 Len=1448 TSval=17976883 TSecr=2678899179
  4190 10.629320436 10.5.20.128   10.145.192.92   TCP        1514 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14668241 Ack=152 Win=30080 Len=1448 TSval=17976883 TSecr=2678899179
  4192 10.641796799 10.5.20.128   10.145.192.92   TCP        1514 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14669689 Ack=152 Win=30080 Len=1448 TSval=17976883 TSecr=2678899180
  4091 10.458965732 10.5.20.128   10.145.192.92   TCP        4410 [TCP Fast Retransmission] 8000 → 43664 [ACK] Seq=13929761 Ack=152 Win=30080 Len=4344 TSval=17976847 TSecr=2678898983 [TCP segment of a reassembled PDU]
  4127 10.537729215 10.5.20.128   10.145.192.92   TCP        4410 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14233841 Ack=152 Win=30080 Len=4344 TSval=17976858 TSecr=2678899070
  4196 10.656217411 10.5.20.128   10.145.192.92   TCP        4410 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14671137 Ack=152 Win=30080 Len=4344 TSval=17976883 TSecr=2678899180
  4198 10.659432103 10.5.20.128   10.145.192.92   TCP        8754 [TCP Retransmission] 8000 → 43664 [ACK] Seq=14675481 Ack=152 Win=30080 Len=8688 TSval=17976883 TSecr=2678899180
```

```
▸ Frame 4121: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Cisco_e4:6c:41 (18:ef:63:e4:6c:41), Dst: IntelCor_c4:ad:8d (d0:57:7b:c4:ad:8d)
▸ Internet Protocol Version 4, Src: 10.5.20.128, Dst: 10.145.192.92
▸ Transmission Control Protocol, Src Port: 8000, Dst Port: 43664, Seq: 14226601, Ack: 152, Len: 1448
```

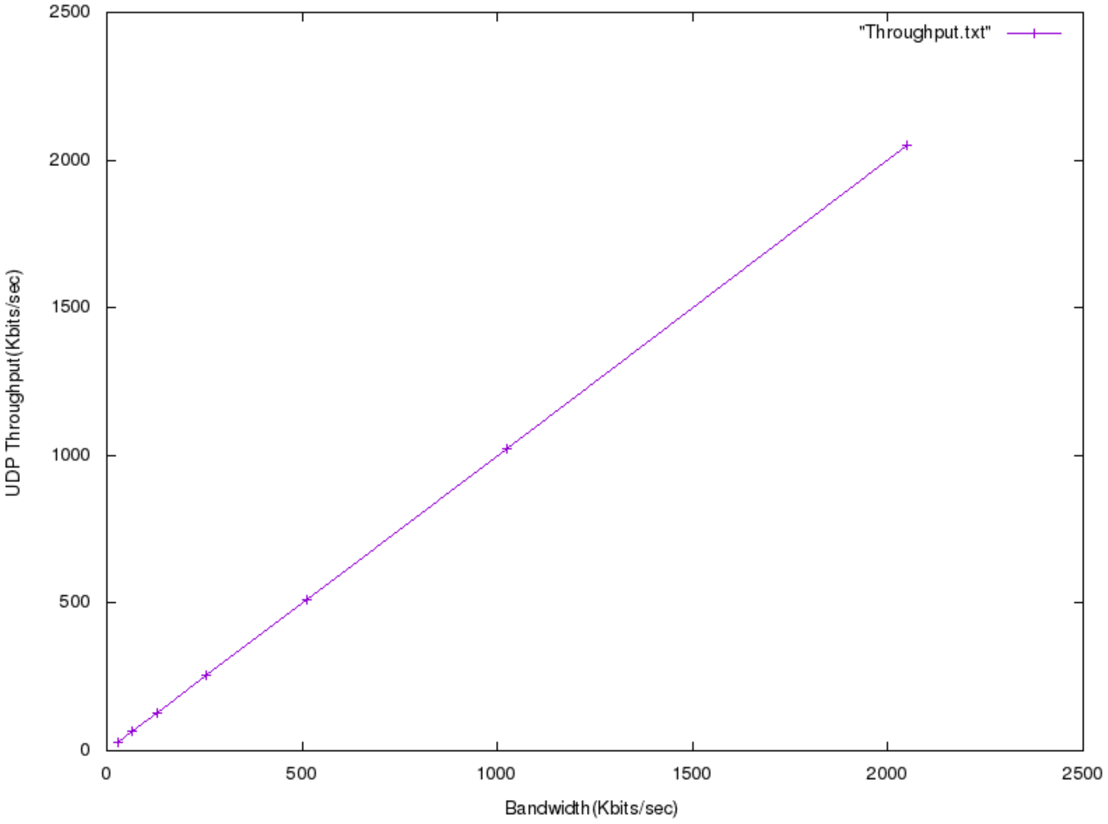
```
0000  d0 57 7b c4 ad 8d 18 ef  63 e4 6c 41 08 00 45 00   .W{..... c.lA..E.
0010  05 dc 7b b1 40 00 3e 06  d1 f8 0a 05 14 80 0a 91   ..{.@.>. ........
```

wireshark_wlp2s0_20180117183647_R5tym9   Packets: 5509 · Displayed: 10 (0.2%)   Profile: Default

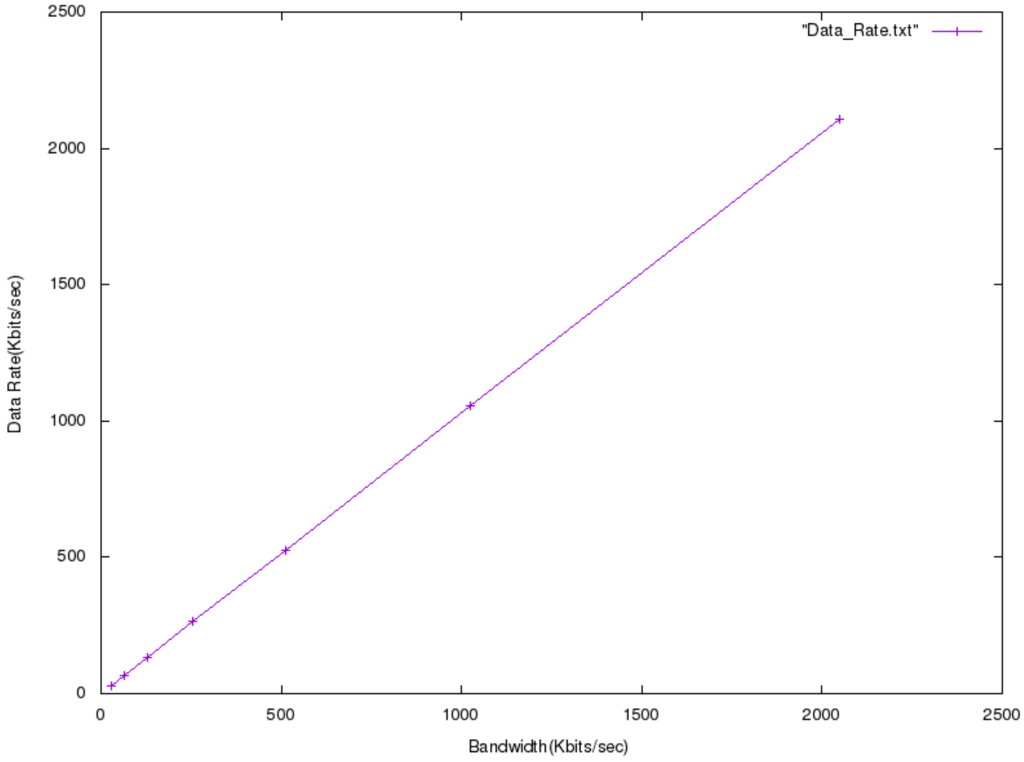
Justification : Since the 2nd pic was the largest in size, no of packets transmitted was greater and the likelihood of a packet being dropped and retransmitted was higher.

4. (a)

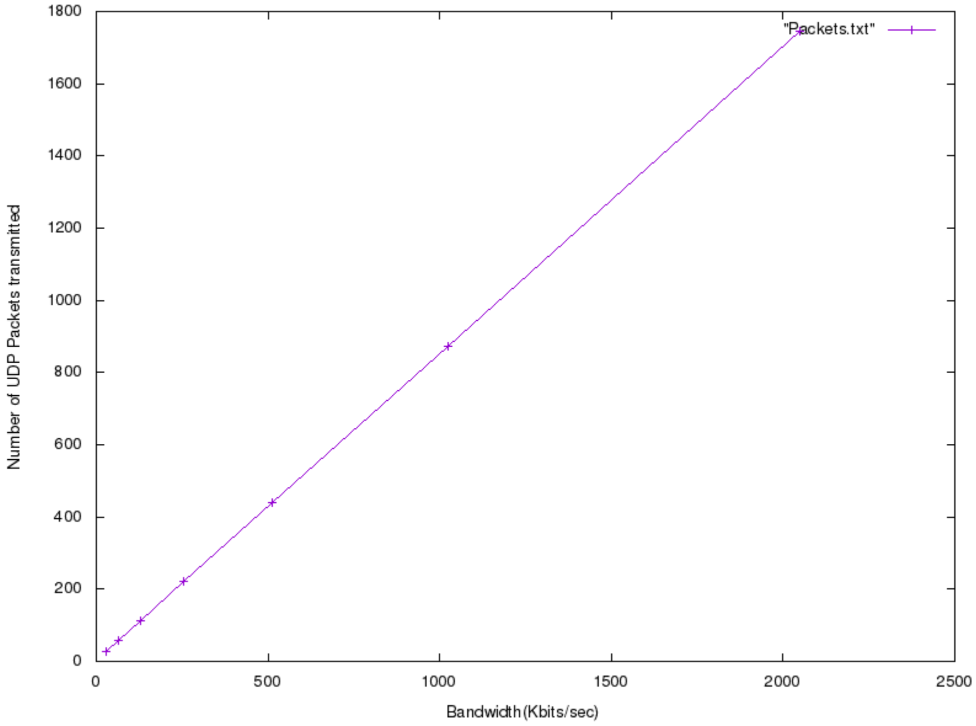
UDP throughput with respect to the UDP bandwidth.



Data Rate with respect to UDP bandwidth.



4. (b) Number of UDP packets transmitted with respect to the UDP bandwidth.



Observations from the plots:

- Both the UDP throughput and number of UDP packets increase linearly with the UDP Bandwidth.
- The UDP throughput is close to the UDP bandwidth in all the cases.