CS39006: Computer Networks Lab

Assignment 1 Report

Use Wireshark for Analyzing Network Packet Traces

Report by:

NISARG SHAH (15CS10030)

MAYANK BHUSHAN (15CS30019)

Objective:

The objective of this assignment is to understand the Wireshark tool and how you can analyse network packet traces. You have to use Wireshark for answering the questions.

Methodology used:

The following command were run on the terminal:
i) “iperf -c 10.5.20.128 -u -b 28000” for the UDP client(28 Kbps)
ii) “ wget --no-proxy http://10.5.20.128:8000/pic1.jpg” for TCP client

The packets were captured using Wireshark tool.
Filters applied: ip.addr == 10.5.20.128 and tcp/udp

Further, the values of the bandwidth(udp) and the url(tcp) were changed to get more observations.

Graphs were plotted using gnuplot.

Questions/Observations/Justifications:

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.**

   Solution:

a) UDP test case

i) Application layer:- Nil
ii) Transport layer:- UDP
iii) Network layer:- IPv4

b) TCP test case

i) Application layer:- HTTP
ii) Transport layer:- TCP
iii) Network layer:- IPv4

2. Analyse the packet trace using Wireshark and compute the following:

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?

Solution:

Pic1:

Number of packets:- 74
Sizes(Different, in bytes):- 66, 74,217,829,1514

Pic2:

Number of packets:- 18022
Sizes(Different, in bytes):- 66, 74, 78, 86, 94, 217, 1181, 1514

Pic3:

Number of packets:- 641
Sizes(Different, in bytes):- 66, 74, 217, 635, 1514

Pic4:

Number of packets:- 4178
Sizes(Different, in bytes):- 66, 74, 217, 1346, 1514

Pic5:

Number of packets:- 927
Sizes(Different, in bytes):- 66, 74, 217, 1198, 1514

Explanation: The number of packets depend on size of the data transferred and the speed of the connection. The packets have varying sizes because for TCP, packets other than the data packets are also transmitted and received (like acknowledgment, handshake, etc.) which have different sizes.

b) For the test case with UDP, are all the UDP packets of same size?

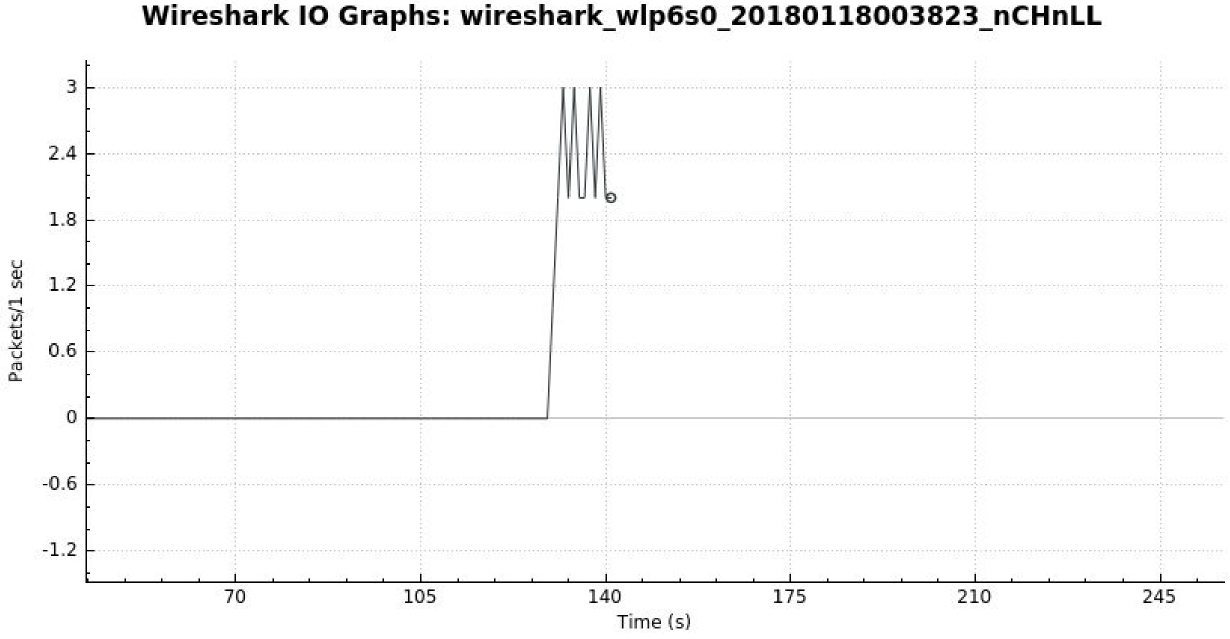
Solution:

Yes all the UDP packets were found to be of the same size.
Packet size : 1470 bytes.
The packets are of same size because for transmission through UDP UDP client, only the data packets are transferred and not any other packets(like handshake, acknowledgement, etc.). UDP client will divide the data into packets of the same size.

c) Observe the TCP and the UDP throughput using Wireshark.

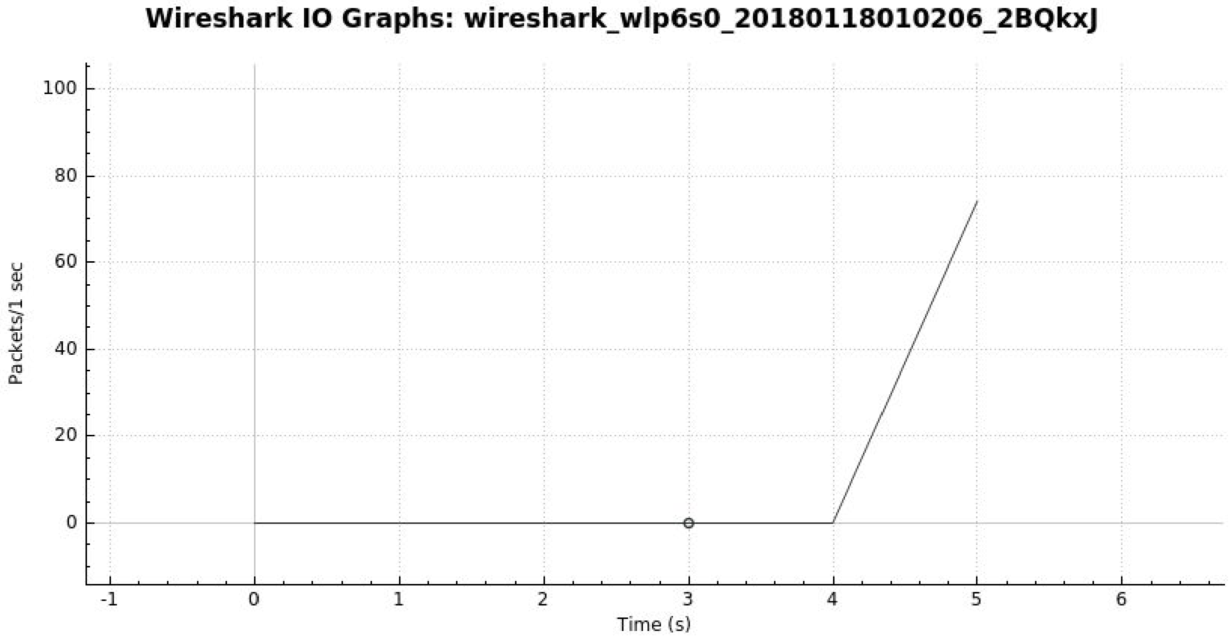
Plots:

i) UDP:

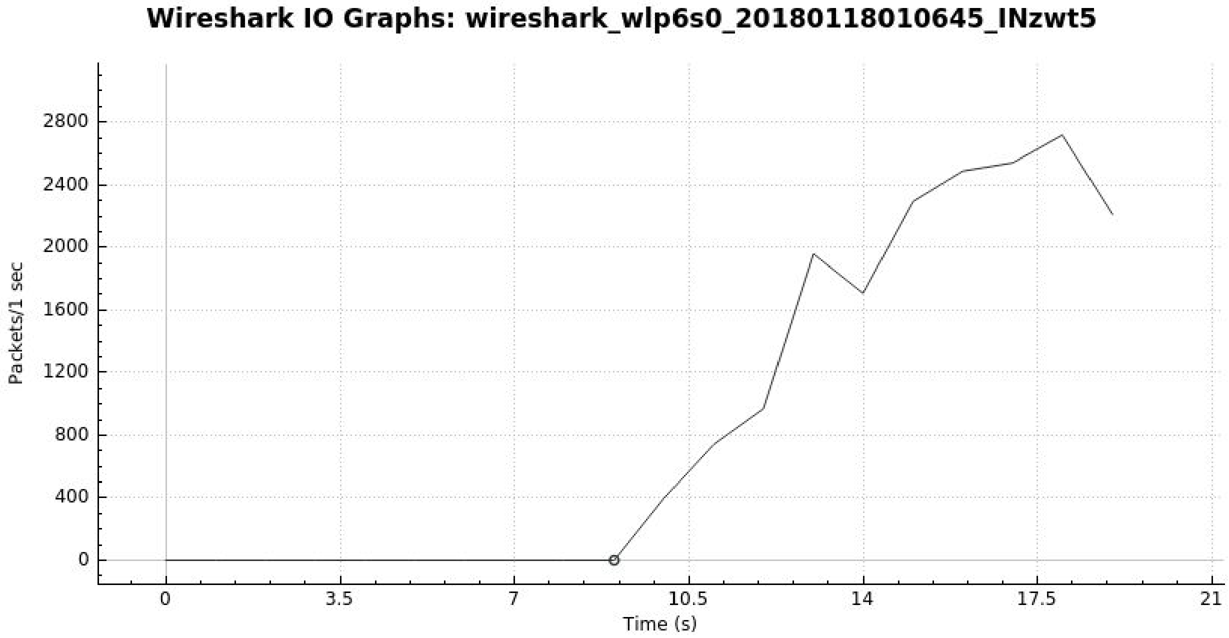


ii) TCP:

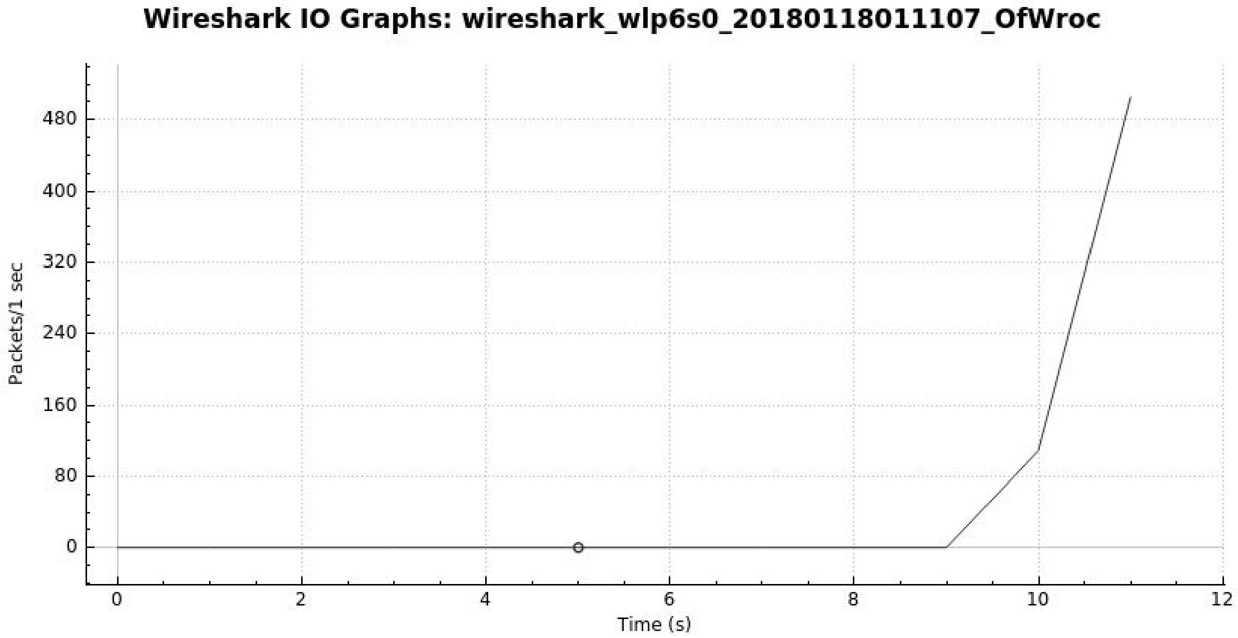
Pic1:



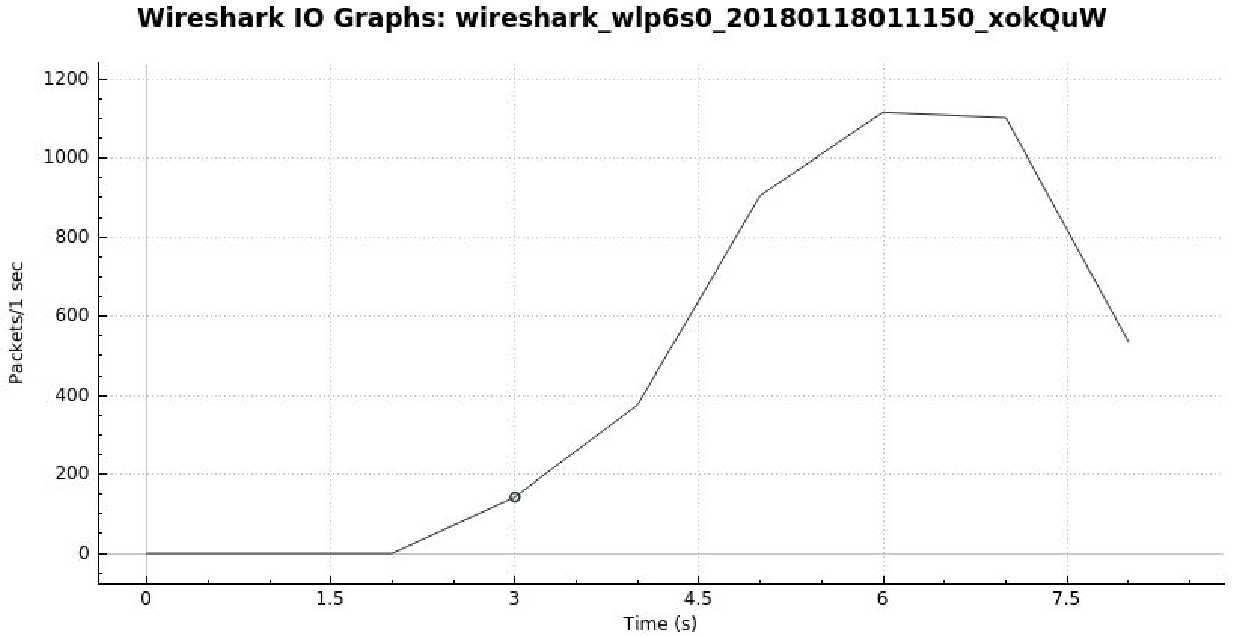
Pic2:



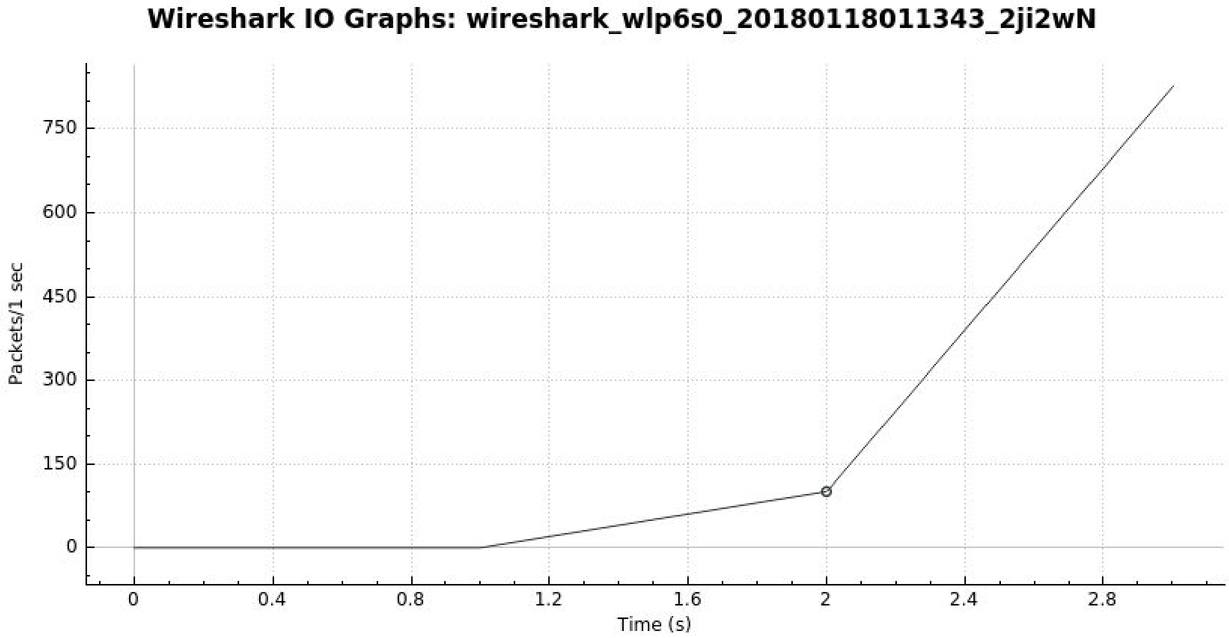
Pic3:


Wireshark IO Graphs: wireshark_wlp6s0_20180118011107_OfWroc

Pic4:


Wireshark IO Graphs: wireshark_wlp6s0_20180118011150_xokQuW

Pic5:



Explanation: The graph depends on the size of the data to be transferred and the speed of the internet. If the size is larger, more number of packets are transferred, which in turn leads to increase in time of transmission. If the network is fluctuating and the size is large, the graph will show the most fluctuation(as in pic2)

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

Solution:

Data rate vs Bandwidth (As captured by wireshark)
i) 64 Kbps: 68 Kbps
ii) 128 Kbps: 133 Kbps
iii) 256 Kbps: 264 Kbps
iv) 512 Kbps: 528 Kbps

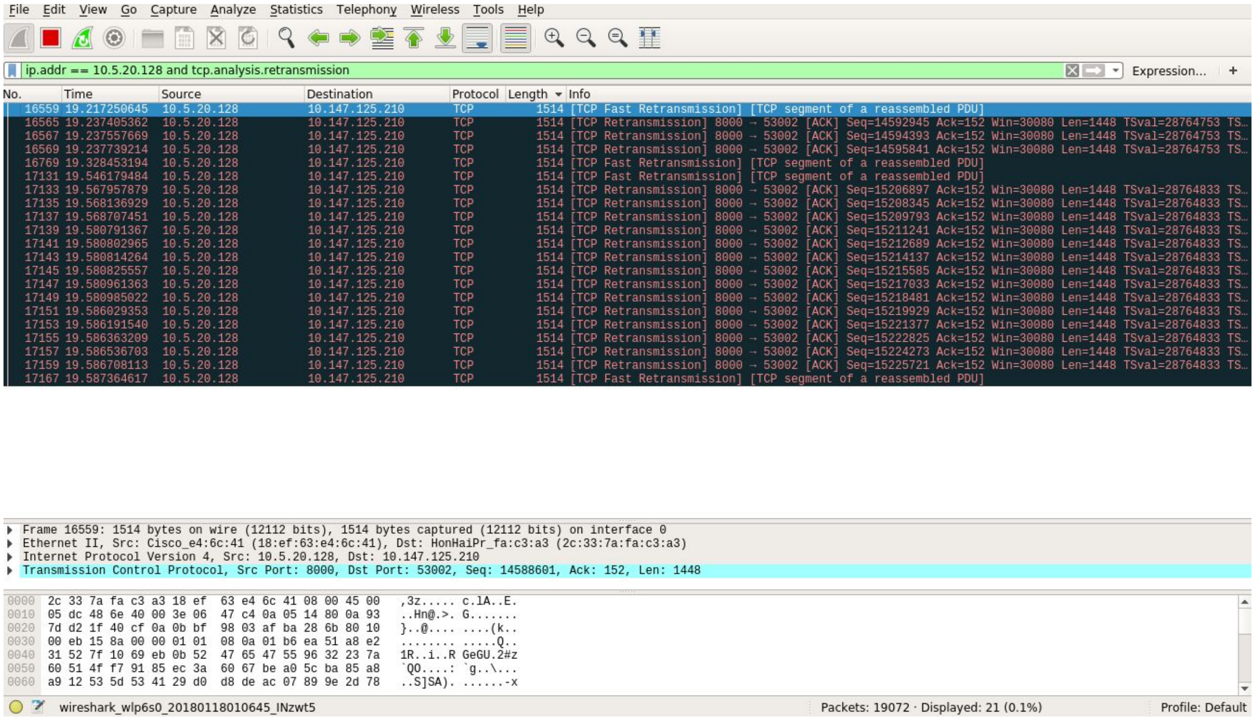
v) 1024 Kbps: 1054 Kbps
vi) 2048 Kbps: 2085 Kbps

Throughput vs Bandwidth (As captured by iperf)
i) 64 Kbps: 62.8 Kbps
ii) 128 Kbps: 129 Kbps
iii) 256 Kbps: 254 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.

Solution:

TCP packets were retransmitted only for the pic2 (21 Packets).



ip.addr == 10.5.20.128 and tcp.analysis.retransmission

```
No.   Time         Source       Destination    Protocol Length Info
16559 19.217250645 10.5.20.128  10.147.125.210 TCP      1514 [TCP Fast Retransmission] [TCP segment of a reassembled PDU]
16565 19.237405362 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=14592945 Ack=152 Win=30080 Len=1448 TSval=28764753 TS…
16567 19.237557669 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=14594393 Ack=152 Win=30080 Len=1448 TSval=28764753 TS…
16569 19.237739214 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=14595841 Ack=152 Win=30080 Len=1448 TSval=28764753 TS…
16769 19.328453194 10.5.20.128  10.147.125.210 TCP      1514 [TCP Fast Retransmission] [TCP segment of a reassembled PDU]
17131 19.546179484 10.5.20.128  10.147.125.210 TCP      1514 [TCP Fast Retransmission] [TCP segment of a reassembled PDU]
17133 19.567957879 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15206897 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17135 19.568136929 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15208345 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17137 19.568707451 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15209793 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17139 19.580791367 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15211241 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17141 19.580802965 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15212689 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17143 19.580814264 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15214137 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17145 19.580825557 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15215585 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17147 19.580961363 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15217033 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17149 19.580985022 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15218481 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17151 19.586029353 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15219929 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17153 19.586191540 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15221377 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17155 19.586363209 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15222825 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17157 19.586536703 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15224273 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17159 19.586708113 10.5.20.128  10.147.125.210 TCP      1514 [TCP Retransmission] 8000 → 53002 [ACK] Seq=15225721 Ack=152 Win=30080 Len=1448 TSval=28764833 TS…
17167 19.587364617 10.5.20.128  10.147.125.210 TCP      1514 [TCP Fast Retransmission] [TCP segment of a reassembled PDU]
```

```
▸ Frame 16559: 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: HonHaiPr_fa:c3:a3 (2c:33:7a:fa:c3:a3)
▸ Internet Protocol Version 4, Src: 10.5.20.128, Dst: 10.147.125.210
▸ Transmission Control Protocol, Src Port: 8000, Dst Port: 53002, Seq: 14588601, Ack: 152, Len: 1448
```

```
0000  2c 33 7a fa c3 a3 18 ef  63 e4 6c 41 08 00 45 00   ,3z..... c.lA..E.
0010  05 dc 48 6e 40 00 3e 06  47 c4 0a 05 14 80 0a 93   ..Hn@.>. G.......
0020  7d d2 1f 40 cf 0a 0b bf  98 03 af ba 28 6b 80 10   }..@.... ....(k..
0030  00 eb 15 8a 00 00 01 01  08 0a 01 b6 ea 51 a8 e2   ........ .....Q..
0040  31 52 7f 10 69 eb 0b 52  47 65 47 55 96 32 23 7a   1R..i..R GeGU.2#z
0050  60 51 4f f7 91 85 ec 3a  60 67 be a0 5c ba 85 a8   `QO....: `g..\...
0060  a9 12 53 5d 53 41 29 d0  d8 de ac 07 89 9e 2d 78   ..S]SA). ......-x
```

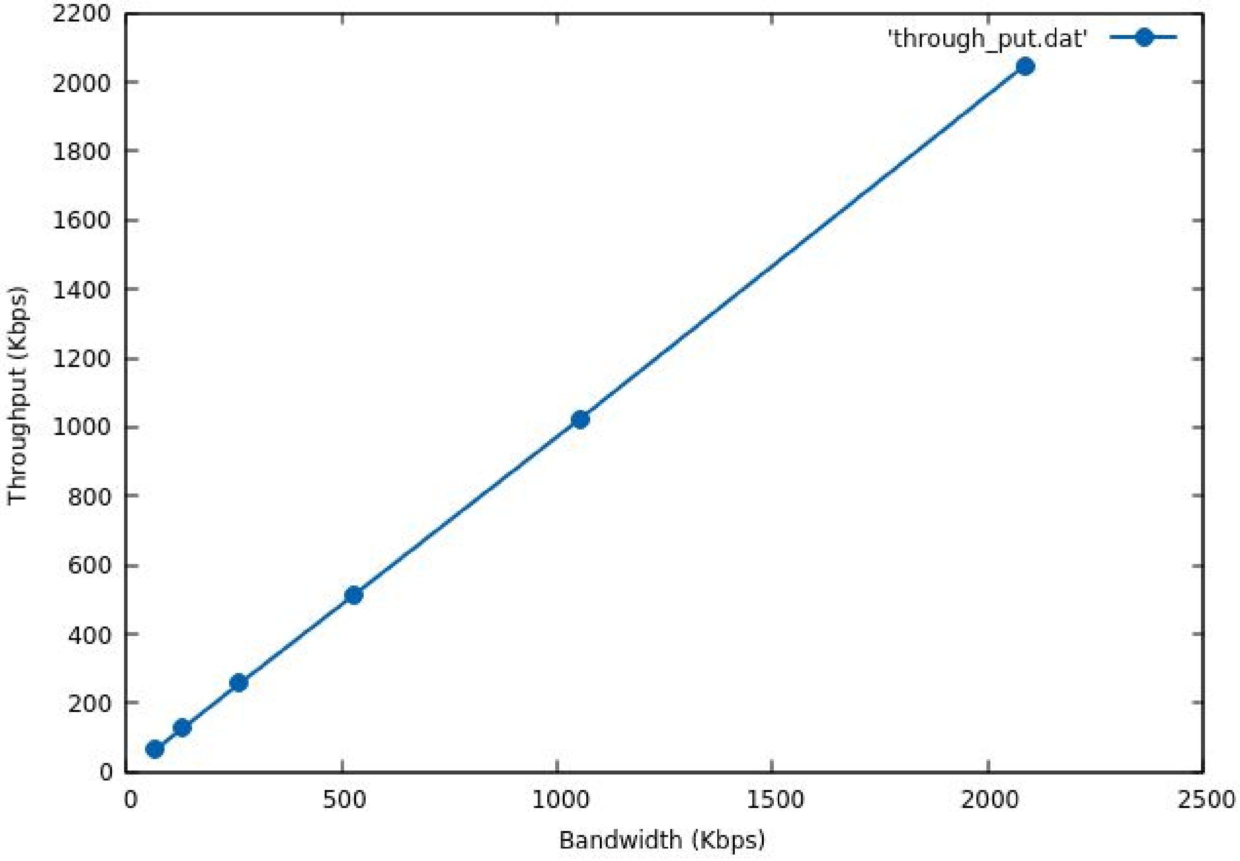
wireshark_wlp6s0_20180118010645_INzwt5   Packets: 19072 · Displayed: 21 (0.1%)   Profile: Default

Explanation: Since pic2's size is very large, it takes significant of time to be transferred. Also, the number of packets transferred are also high. Due to this, there are higher chances of congestion which might lead to packets being dropped. The other pics' sizes are not too large and hence, no dropping and retransmission occurs.

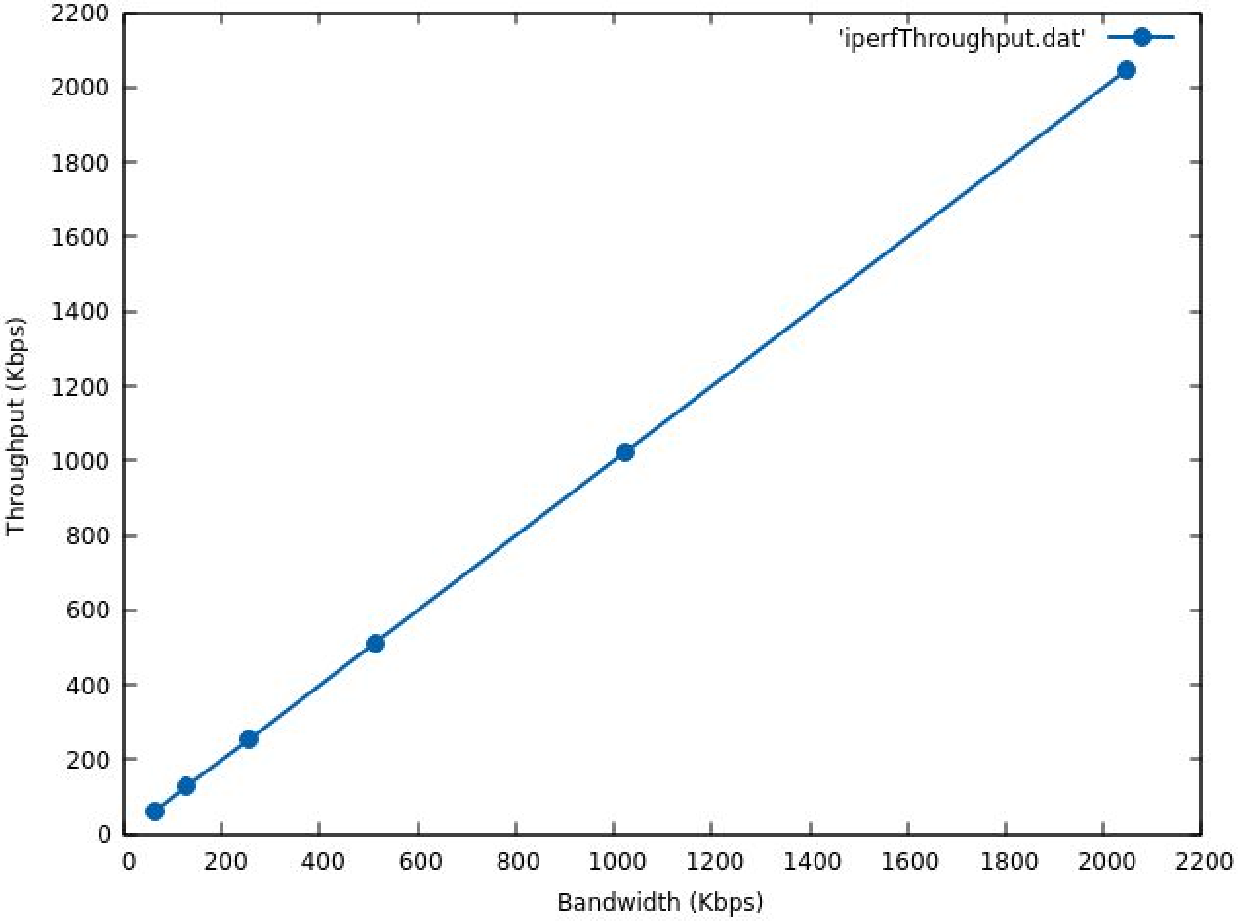
4. Plot the following.

a) UDP throughput with respect to the UDP Bandwidth.

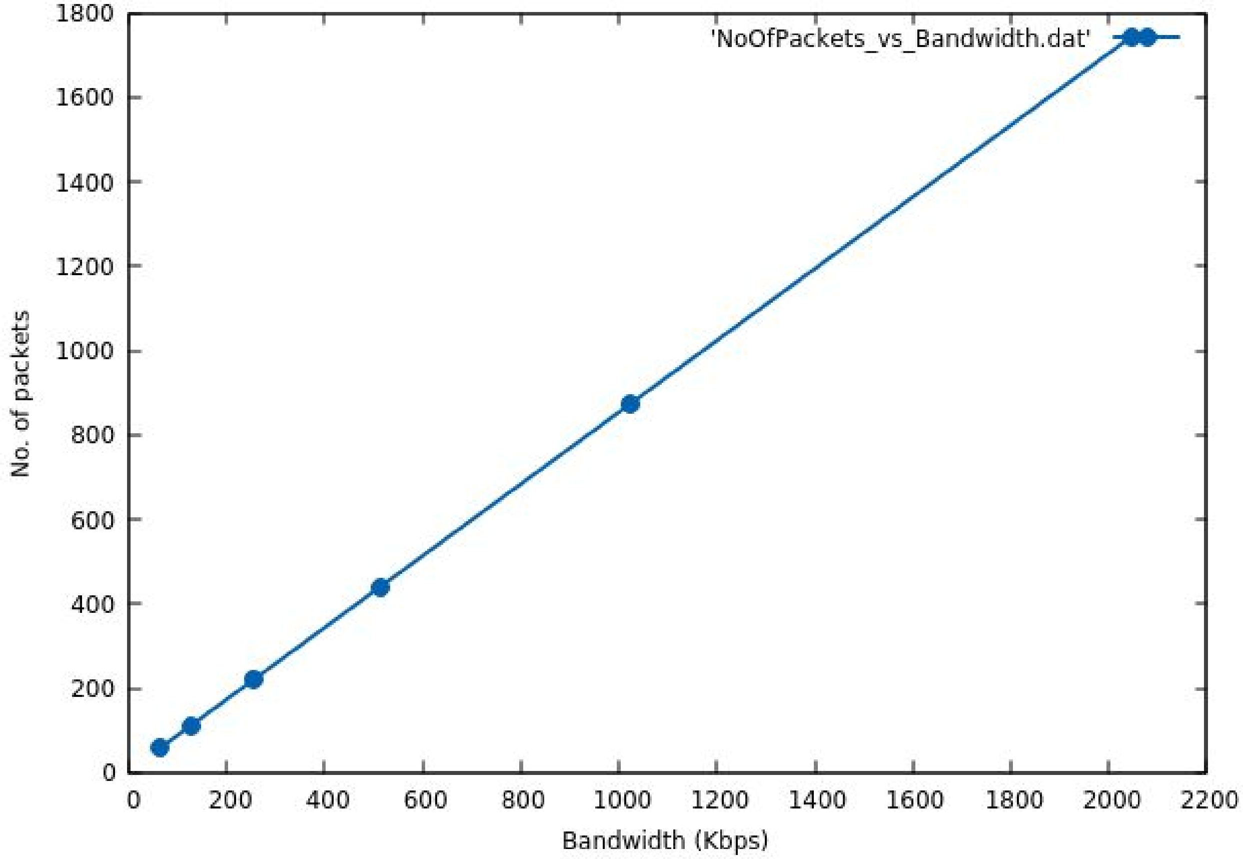
Data rate vs Bandwidth(As captured by wireshark)



Throughput vs Bandwidth(As reported by iperf)



b) Number of UDP packets transmitted vs UDP Bandwidth



The UDP throughput increases linearly with the Bandwidth and their values are almost equal.

The number of UDP packets transmitted also increase linearly with the bandwidth.(Since all the packets are of the same size)