CS 39006: Networks Lab (Spring 2020)
Assignment 1: Using Wireshark for Analyzing Network Packet Traces
Report

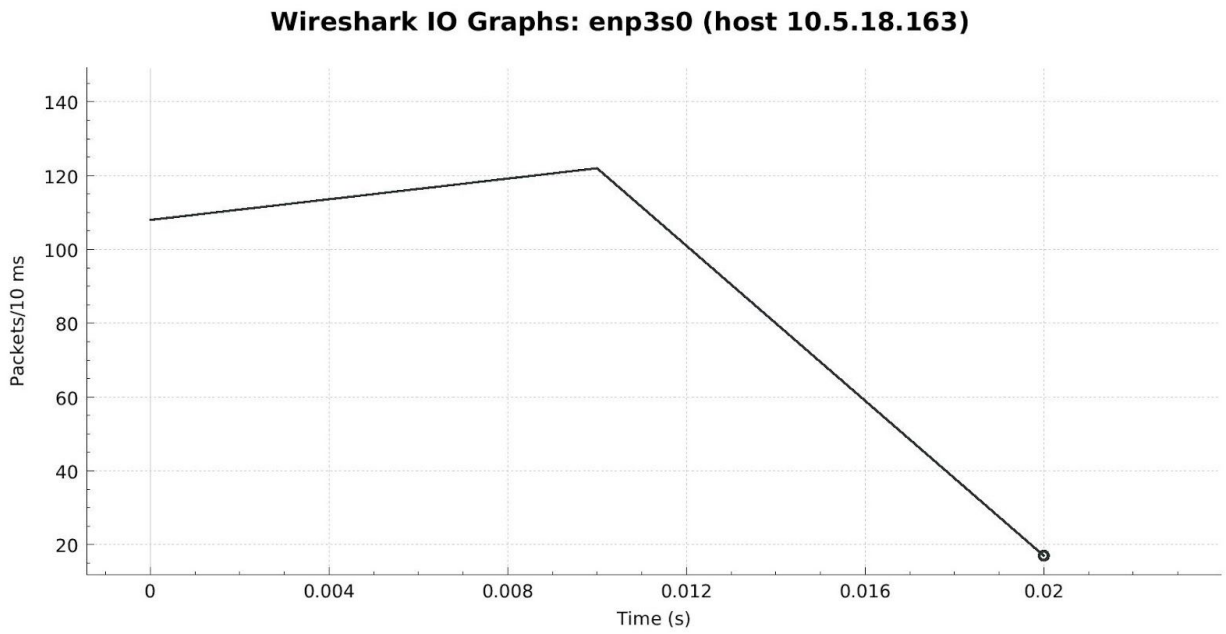
1. TCP :

Procedure :

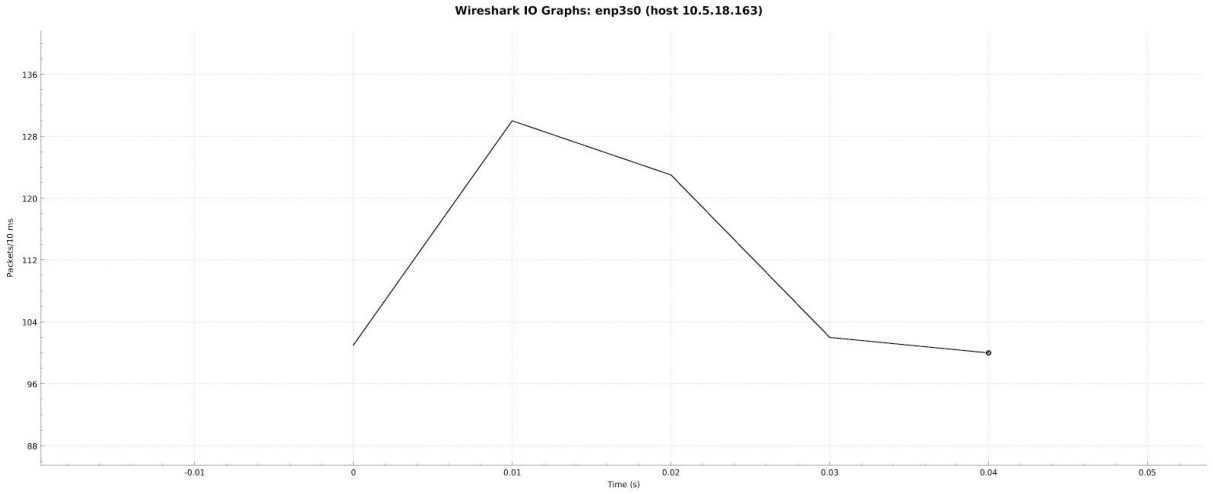
- Using **WireShark** tool captured the packets. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Applied **capture filter** for **host 10.5.18.163** . [corresponding to connection enp3s0]
- Applied **display filter** for **TCP && !IPV4 && ip.addr == client_ip** .
- "wget --no-proxy http://10.5.18.163:8000/i.jpg" Used above wget command which employs HTTP protocol to download the image file i.jpg from the web server running at 10.5.18.163.
- Recorded different types of protocols observed, number of TCP packets, total number of packets and size range of packets.
- Observed packets/s vs time plot by following path Statistics-> I/O Graphs.
- Measured throughput through the following path Statistics->capture file properties. [row : Average bits/s = throughput].
- Repeated above steps for all i in [2,7].

Protocols : TCP (Transport Layer) , HTTP (Application Layer).

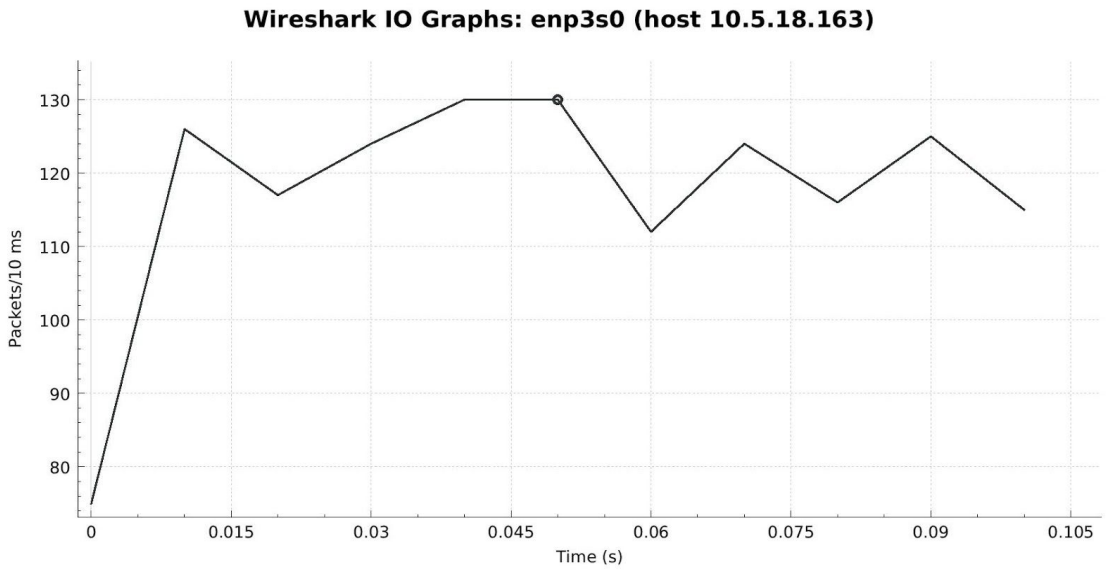
a. Image 1 :
   i. Total = 247
   ii. TCP = 245
   iii. HTTP = 2
   iv. No packets aren't of same sizes in [66,18890] bytes
   v. TCP packets retransmitted : 0



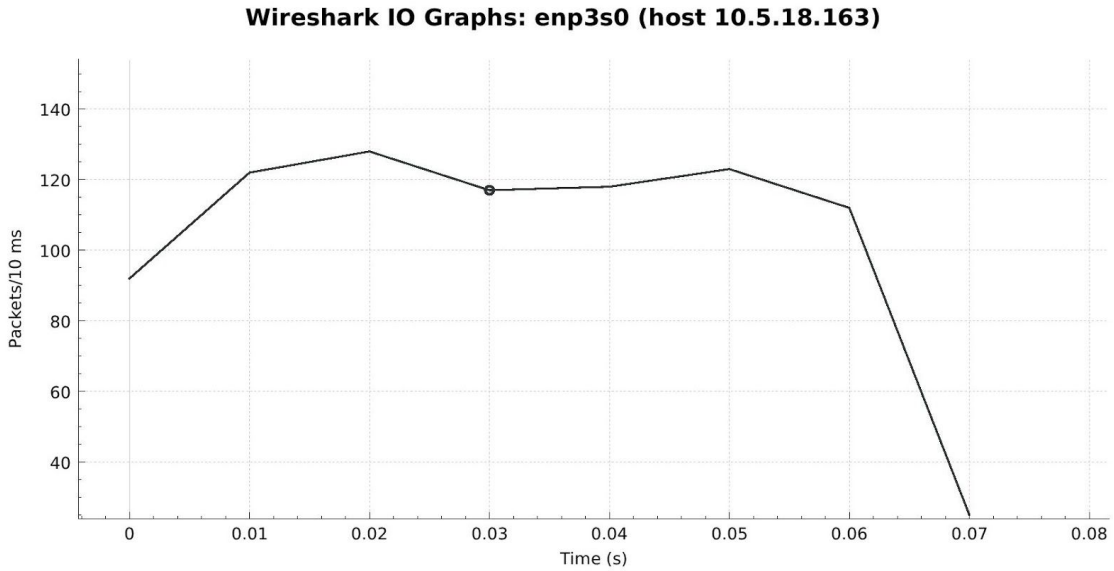
b. Image 2:
   i. Total = 556
   ii. TCP = 554
   iii. HTTP = 2
   iv. No packets aren't of same sizes in [66,26130] bytes
   v. TCP packets retransmitted 4



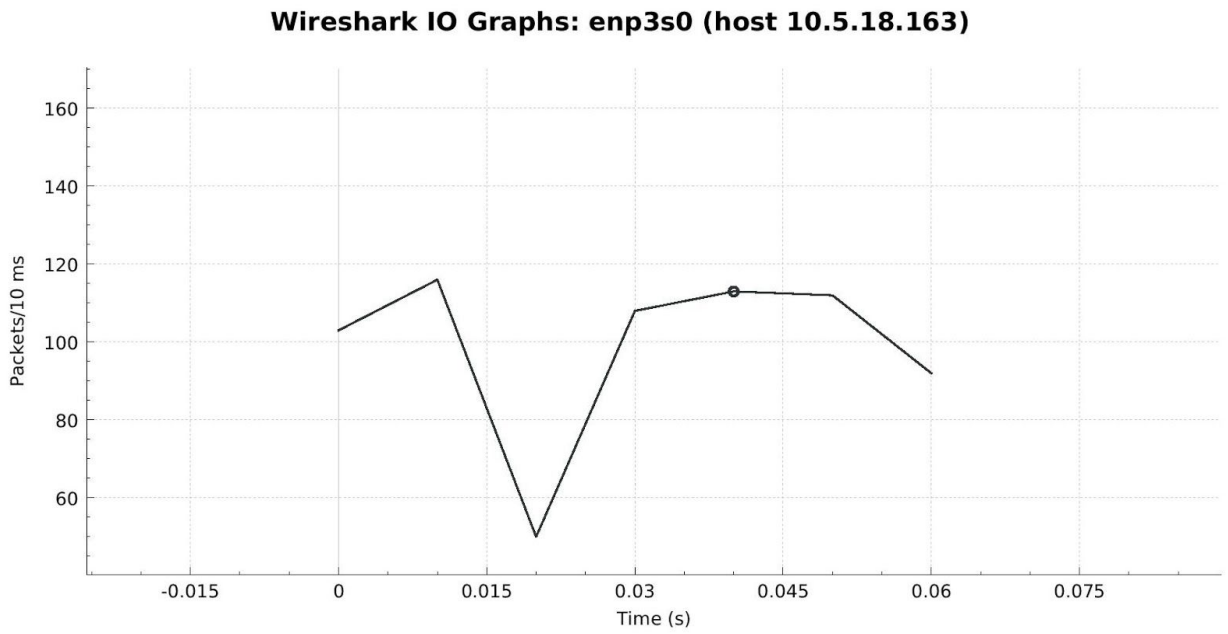
c. Image 3:
   i. Total = 1294
   ii. TCP = 1292
   iii. HTTP = 2
   iv. No packets aren't of same sizes in [66,29026] bytes
   v. TCP packets retransmitted 9



d. Image 4:
   i. Total = 837
   ii. TCP = 835
   iii. HTTP = 2
   iv. No packets aren't of same sizes in [66,23234] bytes
   v. TCP packets retransmitted 4



e. Image 5:
   i. Total = 694
   ii. TCP = 693
   iii. HTTP = 1
   iv. No packets aren't of same sizes in [66,26130] bytes
   v. TCP packets retransmitted : 6



Justification for Observations :

- **WGET** is a tool which employs HTTP protocol to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.
- Number of TCP packets captured varies absurdly with images : The number of TCP packets transferred is related to the data used to download the specific image.
- Packets aren't of the same size and the range of sizes observed is mentioned as in the observations.
- We observed seven peaks in the I/O Plot. Also individual I/O graphs can be seen as increasing initially and then dropping afterwards as a peak is observed when an image is downloaded using the wget command.

2. UDP :

Procedure:

1. Run wireshark with capture filter 'host 10.5.18.163'
2. Run command 'iperf -c 10.5.18.163 -u -b bandwidth' with the required bandwidth.
3. Apply display filter to 'ip.src == ip_client && udp' this shall give the total udp packets among the lot.
4. Throughput can be measured through the following path Statistics->capture file properties.

Protocols : UDP (Transport Layer) , IPv4 (Network Layer).

a. 28Kbps :
   i. Total Packets : 72
   ii. UDP Packets : 11
   iii. Yes each packet is of same size 834 bytes
   iv. Throughput : 37 Kb/sec

v. Data per packet = 8192 bytes

b. 64 Kbps:
   i. Total Packets : 102
   ii. UDP Packets : 16
   iii. No packets aren't of same sizes i.e. 46, 60*, 834 bytes
   iv. Throughput : 71 Kb/sec
   v. Data per packet = 8192 bytes

c. 128 Kbps:
   i. Total Packets : 172
   ii. UDP Packets : 28
   iii. No packets aren't of same sizes i.e. 46, 60*, 834 bytes
   iv. Throughput : 156 Kb/sec
   v. Data per packet = 8192 bytes

d. 256 Kbps:
   i. Total Packets : 279
   ii. UDP Packets : 45
   iii. No packets aren't of same sizes i.e. 46, 60*, 834 bytes
   iv. Throughput : 265 Kb/sec
   v. Data per packet = 8192 bytes

e. 512 Kbps:
   i. Total Packets : 493
   ii. UDP Packets : 81
   iii. No packets aren't of same sizes i.e. 46, 60*, 834 bytes
   iv. Throughput : 545 Kb/sec
   v. Data per packet = 8192 bytes

f. 1024 Kbps:
   i. Total Packets : 969
   ii. UDP Packets : 158
   iii. No packets aren't of same sizes i.e. 46, 60*, 834 bytes
   iv. Throughput : 1062 Kb/sec
   v. Data per packet = 8192 bytes

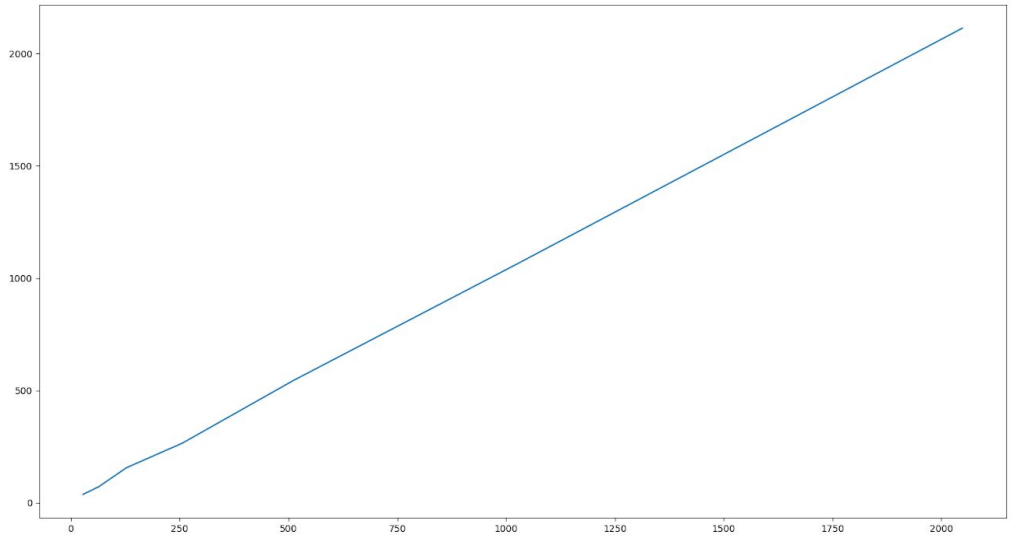
g. 2048 Kbps:
   i. Total Packets : 1898
   ii. UDP Packets : 313
   iii. No packets aren't of same sizes i.e. 46, 60*, 834 bytes
   iv. Throughput : 2113 Kb/sec
   v. Data per packet = 8192 bytes

Justification:

- The readings are in consensus with the fact that theoretically throughput is bounded by bandwidth. The network is also capable to provide throughput equivalent to bandwidth.

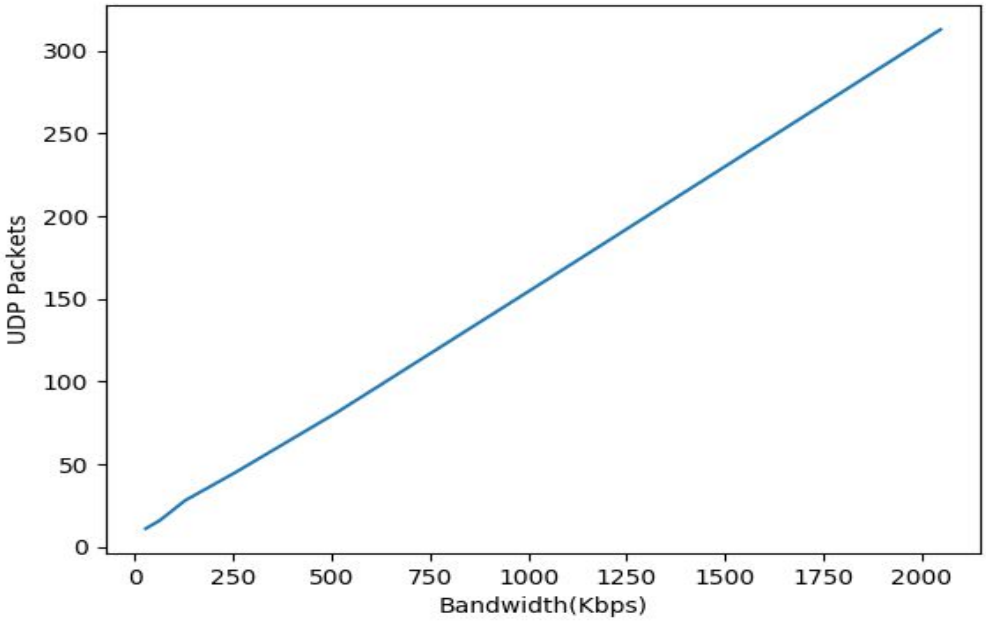
- **iPerf** is a command-line tool used in diagnosing network speed issues by measuring the maximum network throughput a server can handle. We used **-c** <host> to run in client mode, connecting to <host>; **-u** to use UDP rather than TCP and **-b** to specify bandwidth to send at in bits/sec.

Fig. UDP throughput with respect to the UDP bandwidth



- With increasing bandwidth, throughput increases this shows that network is able to sustain required throughput.

Fig. Number of UDP packets transmitted with respect to UDP bandwidth



- The number of udp packets transferred increases with bandwidth because of the high throughput.