Ayush Agarwal
[17114017]

Assignment 9

17th October 2019

1. Install Wireshark and explore its uses to capture network traffic. You have to capture normal internet traffic for 20-30 minutes from your system using Wireshark. You need to copy this data in CSV / TXT file.

   Answer: Captured the normal internet traffic for 20 minutes from the system using Wireshark and export the packet data in the file named `***analysis.csv***`.

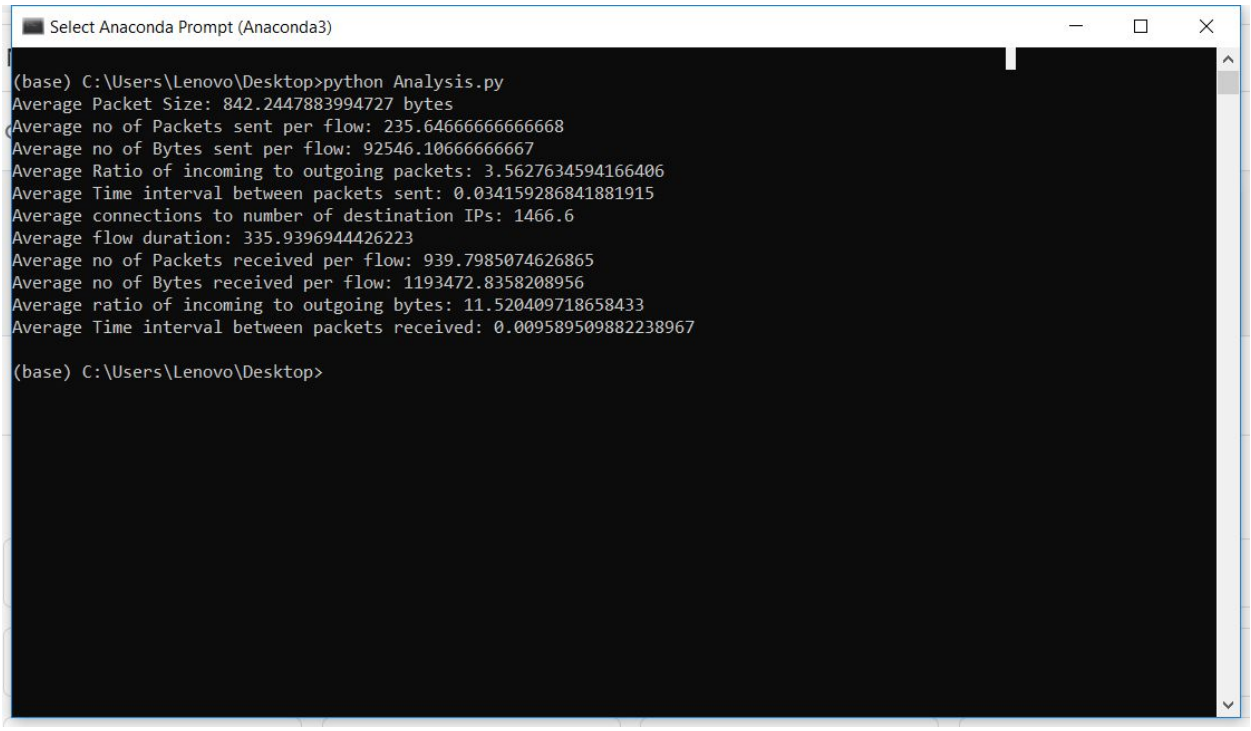
2. Take the CSV / TXT, which is generated in Problem Statement 1 as an input. Write code (in any programming language of your choice) to extract the following 11 features given below in the table:

   Answer: The python code for the above question is written below:

```
import pandas as pd

output = pd.read_csv('analysis.csv')

IP = '10.21.2.75'

print("Average Packet Size: {} bytes".format(sum(output['Length'])/len(output['Length'])))

print('Average no of Packets sent per flow:
{}'.format(output[output['Source']==IP].groupby(['Source','Destination'])['Length'].count(
).mean()))

print('Average no of Bytes sent per flow:
{}'.format(output[output['Source']==IP].groupby(['Source','Destination'])['Length'].sum().
mean()))

x =
len(output[output['Destination']==IP]['Length'])/len(output[output['Source']==IP]['Length'
])
print('Average Ratio of incoming to outgoing packets: {}'.format(x))

x = (output[output['Source']==IP]['Time'])
ans = (x.iloc[len(x)-1] - x.iloc[0])/len(x)
print('Average Time interval between packets sent: {}'.format(ans))

n_destinations = len(set(output[output['Source']==IP]['Destination']))
print('Average connections to number of destination IPs:
{}'.format(len(output)/n_destinations))
```

```
avg_duration = (output.groupby(['Source','Destination'])['Time'].max() -
output.groupby(['Source','Destination'])['Time'].min()).mean()
print('Average flow duration: {}'.format(avg_duration))

print('Average no of Packets received per flow:
{}'.format(output[output['Destination']==IP].groupby(['Source','Destination'])['Length'].c
ount().mean()))

print('Average no of Bytes received per flow:
{}'.format(output[output['Destination']==IP].groupby(['Source','Destination'])['Length'].s
um().mean()))

ans =
sum(output[output['Destination']==IP]['Length'])/sum(output[output['Source']==IP]['Length'
])
print('Average ratio of incoming to outgoing bytes: {}'.format(ans))

x = (output[output['Destination']==IP]['Time'])
ans = (x.iloc[len(x)-1] - x.iloc[0])/len(x)
print('Average Time interval between packets received: {}'.format(ans))
```

Output:



3. In this problem, the behavior of TCP protocol will be studied using Wireshark. For this assignment download the Wireshark captured trace file named as **tcpethe-trace** from Piazza, which is a packet trace of TCP transfer of a file from a client system to a remote server (named as ser1), obtained by running Wireshark on the client machine. Open **tcpethe-trace**

file in Wireshark and answer the following question:

a. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to server (ser1)?

Answer: 1st handshake (the packet) would be by the client. So source ip=client ip = 192.168.1.102. Click on tcp info, find the source port = 1161.

b. What is the IP address of server (ser1)? On what port number it is sending and receiving the TCP segments for this connection?

Answer: The 1st packet will be sent to server only. Find the IP and port in the same way. IP=128.119.245.12, port = 80.

c. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and ser1? What is it in the segment that identifies the segment as a SYN segment?

Answer: Sequence number of first SYN packet. Here it is 0. In the segment, there is a flag 0x002. Which signifies SYN as set and rest as NOT SET.

d. What is the sequence number of the SYNACK segment sent by ser1 to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did ser1 determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Answer: Check the sequence number of the second packet = 0. Go to TCP details, and see ack number there=1. Flag here is 0x012 signifying syn=set and ack=set and rest are not set.

e. 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.

Answer: The segment No.6 contains the HTTP POST command, the sequence number of this segment is 1.

f. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgment was received, what is the Round Trip Time (RTT) value for each of the six segments? What is the Estimated RTT value after the receipt of each ACK? Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment, and then is computed using the following Estimated RTT equation for all subsequent segments. Estimated RTT = (1 – α) * Estimated RTT + α * SampleRTT where the new value of Estimated RTT is a weighted combination of the previous value of Estimated RTT and the new value for SampleRTT. The recommended value of α = 0.125.

Answer: The 4th packet is the first TCP segment (with seq. number 1) having the HTTP POST in its data field.

- 1 sent on 0.026477 length = 619
- 566 sent on 0.041737 ack received at 0.053937 length = 1514
- 2026 sent on 0.054026 ack received at 0.077294 length = 1514
- 3486 sent on 0.054690 ack received at 0.124085 length = 1514
- 4946 sent on 0.077405 ack received at 0.169118 length = 1514
- 6406 sent on 0.078157 ack received at 0.217299 length = 1514
- 7866 sent on 0.124185 ack received at 0.267802 length = 1201

g. What is the length of each of the first six TCP segments?

Answer: The length of the first TCP segment is 578 bytes, the length of the second TCP segment is 137 bytes. The length of each of the following five TCP segments is 1448 bytes.

h. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

Answer: Min avail. Buffer (shown in syn ack packet as window size value) = 5840. The reviver window grows until it reaches the maximum receiver buffer size of 62780 bytes. According to the trace, the sender is never throttled due to lacking of receiver buffer space.

i. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Answer: Total time = 5.624664 sec. Total data = 1771851-(62=62=54=175*8=62) = 176273. Therefore throughput is equal to 176273/5.62 = **31365.3** bytes per second.