Assignment 2 – Part A

Your task is to write a program “analysis_pcap_tcp” that analyzes a Wireshark/TCPdump trace to characterize the TCP flows in the trace. A TCP flow starts with a TCP "SYN” and ends at a TCP “FIN”

Building:
gcc -lm analysis_pcap_tcp.c -o analysis_pcap_tcp

Only external library used is the math library (-lm). All other APIs are intrinsic to gcc.

Running:
./analysis_pcap_tcp

Note – The program will read **assignment2.pcap** as default pcap file from the current location. The file must be present there.

Output:
For the given pcap file the output is as follows

```
neha:Part A$ ./a.out
Part A
1. Total Number of TCP Flows initiated by the Sender - 3

2 (a) First 2 transactions per Flow
Flow       Ports      Seq_Num     Ack_Num     Dest_Seq_Num   Dest_Ack_Num  Recv_Window   Length
  1     43498->80   705669103  1921750144    1921750144      705669127     49152          90
  1     43498->80   705669127  1921750144    1921750144      705670575     49152        1514
  2     43500->80  3636173852  2335809728    2335809728     3636173876     49152          90
  2     43500->80  3636173876  2335809728    2335809728     3636175324     49152        1514
  3     43502->80  2558634630  3429921723    3429921723     2558634654     49152          90
  3     43502->80  2558634654  3429921723    3429921723     2558636102     49152        1514

2 (b) Throughput
Flow       Ports        Sent(B)  Time(s)     Throughput(Mbps)
  1     43498->80     10552802  2.010401       41.992824
  2     43500->80     10552802  8.320370       10.146474
  3     43502->80      1096664  0.740275       11.851423

2 (c) Loss Rate
Flow       Ports     Packets Sent  Packets Lost  Loss Rate
  1     43498->80        6976            3       0.00043005
  2     43500->80        7067           94       0.01330126
  3     43502->80         728            0       0.00000000

2 (d) Average RTT
Flow       Ports     Average RTT  Theoretical Throughput  Empirical Throughput
  1     43498->80     0.073518            6.317771            41.992824
  2     43500->80     0.088418            0.944563            10.146474
  3     43502->80     0.073290                 inf            11.851423
neha:Part A$
```

EXPLANATIONS

2(a). The program outputs the first two transactions for each flow after the TCP connection is setup (handshake is complete). The columns in the output represent the Flow number, Ports (Sender->Receiver), Sequence Number of the sent packet, Acknowledgment Number of the sent packet, Sequence Number of the received acknowledgment, Acknowledgment Number of the received acknowledgment, Receive Window Size and Total Length of packet in bytes respectively.

2(b). Here I calculate the empirical throughput of each flow. It is calculated as the total number of bits successfully sent over the total time taken to sent the packet. The output is in Megabits per second (Mbps)

2(c). Here I calculate the loss rate for each flow. It is calculated as the total number of packets lost during transmission compared to the total number of packets sent.

2(d). Here I calculate the average RTT of each flow. An RTT of a packet is considered as the time duration between the sent packet and the received acknowledgment of the packet. I am ignoring the time for any packet which were lost during transmission.

Here I also print the theoretical throughput of each flow and compare it with the empirical throughput as calculated by the program. As seen there is a huge difference between the two throughputs. The reasons for this difference could be anything like network overhead, external performance limiters, and network configuration problems. When assessing the performance of networks, there is always a difference between theoretical throughput and “real-world” throughput. There is no option for the difference between theoretical and practical performance being “negligible”!