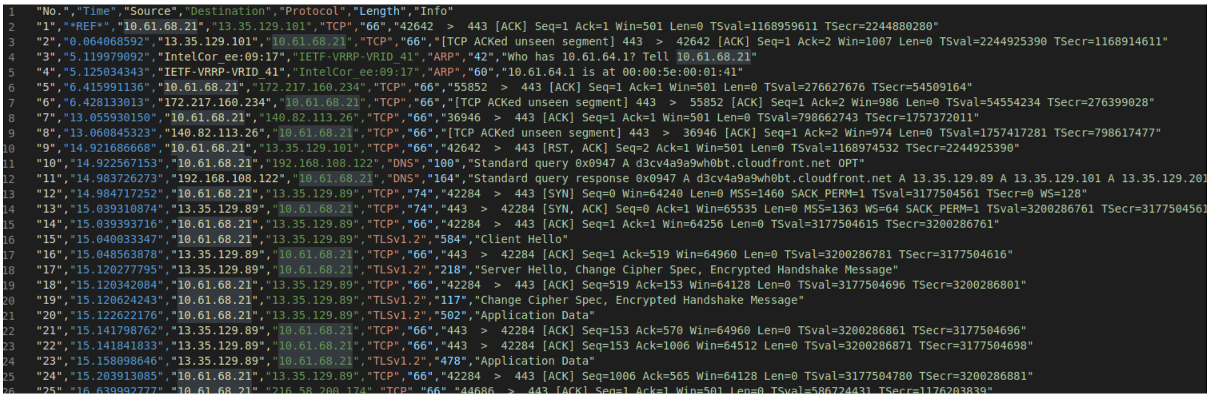
Name: Harshit Maurya
Enrollment No.: 17114037
Batch:CS-1

Class: B.Tech(III) CSE
Subject Code: CSN-361

Assignment L9

1. **Problem Statement 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.



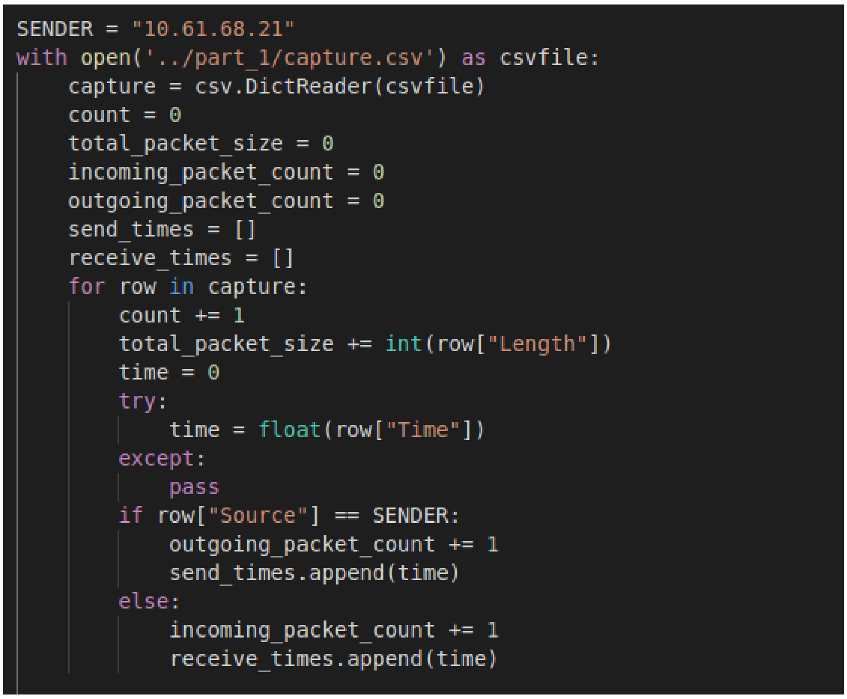
```
"No.","Time","Source","Destination","Protocol","Length","Info"
"1","*REF*","10.61.68.21","13.35.129.101","TCP","66","42642  >  443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1168959611 TSecr=2244880280"
"2","0.064068592","13.35.129.101","10.61.68.21","TCP","66","[TCP ACKed unseen segment] 443  >  42642 [ACK] Seq=1 Ack=2 Win=1007 Len=0 TSval=2244925390 TSecr=1168914611"
"3","5.119979092","IntelCor_ee:09:17","IETF-VRRP-VRID_41","ARP","42","Who has 10.61.64.1? Tell 10.61.68.21"
"4","5.125034343","IETF-VRRP-VRID_41","IntelCor_ee:09:17","ARP","60","10.61.64.1 is at 00:00:5e:00:01:41"
"5","6.415991136","10.61.68.21","172.217.160.234","TCP","66","55852  >  443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=276627676 TSecr=54509164"
"6","6.428133013","172.217.160.234","10.61.68.21","TCP","66","[TCP ACKed unseen segment] 443  >  55852 [ACK] Seq=1 Ack=2 Win=986 Len=0 TSval=54554234 TSecr=276399028"
"7","13.055930150","10.61.68.21","140.82.113.26","TCP","66","36946  >  443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=798662743 TSecr=1757372011"
"8","13.060845323","140.82.113.26","10.61.68.21","TCP","66","[TCP ACKed unseen segment] 443  >  36946 [ACK] Seq=1 Ack=2 Win=974 Len=0 TSval=1757417281 TSecr=798617477"
"9","14.921686668","10.61.68.21","13.35.129.101","TCP","66","42642  >  443 [RST, ACK] Seq=2 Ack=1 Win=501 Len=0 TSval=1168974532 TSecr=2244925390"
"10","14.922567153","10.61.68.21","192.168.108.122","DNS","100","Standard query 0x0947 A d3cv4a9a9wh0bt.cloudfront.net OPT"
"11","14.983726273","192.168.108.122","10.61.68.21","DNS","164","Standard query response 0x0947 A d3cv4a9a9wh0bt.cloudfront.net A 13.35.129.89 A 13.35.129.101 A 13.35.129.201
"12","14.984717252","10.61.68.21","13.35.129.89","TCP","74","42284  >  443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3177504561 TSecr=0 WS=128"
"13","15.039310874","13.35.129.89","10.61.68.21","TCP","74","443  >  42284 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1363 WS=64 SACK_PERM=1 TSval=3200286761 TSecr=3177504561
"14","15.039393716","10.61.68.21","13.35.129.89","TCP","66","42284  >  443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3177504615 TSecr=3200286761"
"15","15.040033347","10.61.68.21","13.35.129.89","TLSv1.2","584","Client Hello"
"16","15.048563878","13.35.129.89","10.61.68.21","TCP","66","443  >  42284 [ACK] Seq=1 Ack=519 Win=64960 Len=0 TSval=3200286781 TSecr=3177504616"
"17","15.120277795","13.35.129.89","10.61.68.21","TLSv1.2","218","Server Hello, Change Cipher Spec, Encrypted Handshake Message"
"18","15.120342084","10.61.68.21","13.35.129.89","TCP","66","42284  >  443 [ACK] Seq=519 Ack=153 Win=64128 Len=0 TSval=3177504696 TSecr=3200286801"
"19","15.120624243","10.61.68.21","13.35.129.89","TLSv1.2","117","Change Cipher Spec, Encrypted Handshake Message"
"20","15.122622176","10.61.68.21","13.35.129.89","TLSv1.2","502","Application Data"
"21","15.141798762","13.35.129.89","10.61.68.21","TCP","66","443  >  42284 [ACK] Seq=153 Ack=570 Win=64960 Len=0 TSval=3200286861 TSecr=3177504696"
"22","15.141841833","13.35.129.89","10.61.68.21","TCP","66","443  >  42284 [ACK] Seq=153 Ack=1006 Win=64512 Len=0 TSval=3200286871 TSecr=3177504698"
"23","15.158098646","13.35.129.89","10.61.68.21","TLSv1.2","478","Application Data"
"24","15.203913085","10.61.68.21","13.35.129.89","TCP","66","42284  >  443 [ACK] Seq=1006 Ack=565 Win=64128 Len=0 TSval=3177504780 TSecr=3200286881"
"25","16.639992777","10.61.68.21","216.58.200.174","TCP","66","44686  >  443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=586724431 TSecr=1176203839"
```

2. **Problem Statement 2:**

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

Average Packet Size	Average Flow Duration
Average no of packets Sent per Flow	Average no of Packets Received per Flow
Average amount of Bytes Sent per Flow	Average amount of Bytes Received per Flow
Average Ratio of Incoming to Outgoing Packets	Average Ratio of Incoming to OutgoingBytes
Average Time Interval b/w Packets Sent	Average Time Interval b/w Packets REceived
Average Ratio of Connections to Number of Destination IPs	

Results:



```python
SENDER = "10.61.68.21"
with open('../part_1/capture.csv') as csvfile:
    capture = csv.DictReader(csvfile)
    count = 0
    total_packet_size = 0
    incoming_packet_count = 0
    outgoing_packet_count = 0
    send_times = []
    receive_times = []
    for row in capture:
        count += 1
        total_packet_size += int(row["Length"])
        time = 0
        try:
            time = float(row["Time"])
        except:
            pass
        if row["Source"] == SENDER:
            outgoing_packet_count += 1
            send_times.append(time)
        else:
            incoming_packet_count += 1
            receive_times.append(time)
```

3. Doc in respective folder.