Assignment 4 (marks: 2 + 3 + 3 + 4 + 3 = 15)

Consider the pcap file shared with you in Google Classroom.

1. Identify unique IP addresses and label them as public IP address or private IP address. And, count the number of packets and number of bytes for each IP addresses. Store the information of each IP address in a table called “IPStat”, having column names “IP”, ”isPublic”, ”nPkt”, and “nBytes”.
2. Find all the pairs IP addresses such that for each pair of IP addresses there exists at least one packet in the pcap file. And, Count the number of packets, the number of bytes and the number of unique transport ports for each pair of IP addresses. Store the information of each pair of IP addresses in a table called “IPPairStat”, having column names “IP1”, “IP2”, “nPkts”, “nBytes”, “nPorts”.
3. Find all the 4-tuples of 2 IP addresses and 2 transport port numbers such that for each of the 4-tuples there exists at least one packet in the pcap file. And, find the time gap between first and the last packet in the group of a 4-tuple and call it as “SessionLen”. Store the information in a table called “sessionLen” having column names “IP1”, “IP2”, “Port1”, “Port2”, “SessionLen”.
4. Group all the packets based on the 4-tuples identified in Step 3. Find the number of packets transferred in each direction. Store this information in a table called “tupleStat” having column names “IP1”, “IP2”, “Port1”, “Port2”, “nPktFromIP1”, “nBytesFromIP1”, “nPktsFromIP2”, “nBytesFromIP2”, “nPktTotal”, “nByteTotal”.
5. Find time gap between a pair of successive send and receive packets for each of the 4-tuples, call this as TimeGap. Let say, pkt1 is sent from IP1, pkt2 is received by IP1, pkt3 is send by IP1 and pkt4 is received by IP1 in sequence in a group of packets in a 4-tuple. Then compute two RTT values like RTT1 = time(pkt2) – time(pkt1) and RTT2 = time(pkt3) – time(pkt4). Store the time gap and the RTT values in a table called “tupleRTT” with column names “IP1”, “IP2”, “port1”, “port2”, “TimeGap”, “RTT”. If the successive packets are not in opposite directions, then consider RTT as 0.