**INTRODUCTION TO TCPFLOW**

TCPFlow is a software tool that analyzes offline and online packet traffic for the statistics of 5-tuple TCP flows. It has two versions written with C in Linux: TCPFlow-Offline and TCPFlow-Online.

1. **TCPFlow-Offline**

TCPFlow-Offline processes a traffic file in pcap format generated by WireShark and TCPDump. It outputs the statistics of TCP flows to a text file in the following format:

<local\_time>, <time\_stamp>, <src\_ip>, <src\_port>, <dst\_ip>, <dst\_port>, <tcp/udp>

In addition, it also outputs the ranking statistics of TCP flows including the Top 10 TCP flows in packets and in bytes, Top 10 source IP addresses, and Top 10 destination IP addresses.

TCPFlow\_Offline runs with the following parameters:

tcpflow-offline [-r <input\_pcap\_file>] [-w <output\_flow\_file>] [-s <output\_stat\_file>]

1. **TCPFlow-Online**

TCPFlow-Online captures online packet TCP flows with a promiscuous mode in a network device. It outputs 5-tuples of each TCP flow to a text file in the following format:

<local\_time>, <time\_stamp>, <src\_ip>, <src\_port>, <dst\_ip>, <dst\_port>, <tcp/udp>

TCPFlow-Online runs with the following parameters:

tcpflow-online [-i <netdevice\_num>] [-c <packet\_count>][-w <output\_flow\_file>] [-s <output\_stat\_file>]

**PREPARATION**

To run TCPFlow, please make sure of installing the libpcap libraries with the root permission.

**HOW TO USE IT**

You can compile and run TCPFlow in Linux as follows:

1. **TCPFlow-Offline**
2. Compile TCPFlow-Offline:

gcc -o tcpflow-offline tcpflow\_offline.c

1. Run TCPFlow-Offline

./tcpflow-offline -r test.pcap -w output\_tcpflow.txt -s output\_summary.txt

1. **TCPFlow-Online**
2. Compile TCPFlow-Online:

gcc -o tcpflow\_online tcpflow\_online.c -lpcap

1. Run TCPFlow-Online

./tcpflow\_online -i eth0 -c 2000 -w output\_tcpflow.txt -s output\_summary.txt