**IP Blocker**

**IP Blocker** is an independent research project and the main intension behind the project is play with raw packet capture. The project takes input as a raw pcap (packet capture) file and gives output file in CSV format which consist of score from the IP Data API.

The project is divided into two modules:

1. Take input as pcap file and gives output as csv file which has source and destination IP address from pcap file, after extracting source IP and destination IP remove duplicate IP’s and after removing duplicate IP’s remove private IP’s
2. Second module calls API which take input of CSV consist of all public IP’s and calls API for each IP and gets score. After getting score then check which score is above 8 copiesIP address and score in another csv file.

Pre-requisite:

1. Install Python 3.7
2. Add folder path "C:\Program Files\Wireshark" to Path environment
3. Create folder named “IP Blocker” in C:/ drive copy paste the python script

Run:

1. Reopen VS Code in administrator privilege after setting environmental path
2. ipScoreUtil.py is main script run command “python ipScoreUtil.py<pcap\_file.pcap>”

Result:

1. In C: drive IP Blocker folder there will be one latest folder created with IP\_Score\_#
2. In this folder after running script successfully at the end you will get 4 CSV files
3. Ip\_list\_from\_pcap.csv: which consist of source ip and destination ip
4. Unique\_ip\_list.csv: consist of removed duplicate IP and private IP’s
5. IP\_score.csv: consist of unique public IP address with score of IP Data API.
6. High\_threat\_ip\_score.csv consists of IP’s whose score is 8+.