Project approach:

1) Using tshark get all source IP addresses into a txt file from the pcap file.

2) Store IP addresses and there total count (+1 for every entry in txt file) in a dictionary (dict_pkt)

3) Run bash script to extract all blacklisted IP addresses into black_list.txt file from the users .txt file. This has been specifically done to extract only IP addresses and leave out all other text.

4) Store blacklisted IP addresses into a dictionary (dict_blist)

5) Compare the two dictionaries and check if any IP address is malicious. If yes add to blacklist list.

6) Parse PCAP file for source and destination port numbers. Count number of packets received by each port number.

7) Parse PCAP file to map source to destination stream flows. Count number of packets sent a particular flow.

8) Using the threshold and port number provided by the user check if that destination port receives more traffic than expected, If yes, interpret as possible DDOS attack and add source IP address to blacklist list.

9) Using D3.js, 6 html files are used for visualization.
Please refer to Synopsis for complete description

10) Use KML file to plot latitude and longitude on Google Earth.

Project Video Links:

Video 1: project demonstration

https://docs.google.com/file/d/0ByaQ_N-MXXinUVcyUXhfMzhGSjg/edit?usp=drivesdk

Video 2: Source files explanation

https://docs.google.com/file/d/0ByaQ_N-MXXinN2k2NmNfNEFSUmc/edit?usp=drivesdk

Video 3: Project Demo with extra work done

https://docs.google.com/file/d/0ByaQ_N-MXXinS2htWE51MHJ4MUE/edit?usp=drivesdk