DDOS-Detection

The PCAP files were first analysed in Wireshark and the important features we selected and extracted. Due to the large size of PCAP files we had to enhance our processing by multiprocessing for 6 hours approx. The extracted features were organised into a data frame and K-Nearest-Neighbours Classifier was used to classify the PCAP file as DDOS or Benign.

The following is the classification report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	22
1	1.00	1.00	1.00	58
accuracy			1.00	80
macro avg	1.00	1.00	1.00	80
weighted avg	1.00	1.00	1.00	80

Features Extracted:

1. Frequency of Packets:
    a. Mean
    b. Standard Deviation
2. Traffic of Packets:
    a. Bandwidth
    b. Mean
    c. Standard Deviation
3. Size of Packets:
    a. Mean
    b. Standard Deviation
    c. Maximum
    d. Minimum
    e. Total
4. IP Address:
    a. Unique Source Count
    b. Unique Destination Count
    c. Unique Destination Counter:
        i. Mean
        ii. Standard Deviation
5. UDP percentage