DDoS Attack Detection Algorithms Based on Entropy Computing

In this paper author is using entropy based calculation to detect DDOS attack as all existing techniques are based on signature and anomaly and this techniques are not reliable to detect attacks. Signature based technique will match predefine attack signature with new request signature and if signature matched then it will detect attack and if new signature arrived then this signature technique will not work and in anomaly also all know attacks will be trained and if new attacks arrived then anomaly technique will also not work.

In DDOS attack attackers will send continuous huge amount of request to server and server will keep busy on handling those requests and ignore genuine request and by processing such huge request server may get crash. To overcome from this attack author introducing cumulative entropy based calculation (CUSUM) to detect attacks. This technique can be initialize with WINDOW and this window will be filled with all IP addresses and once this window filled up then application will calculate CUSUM and if CUSUM has less number of values then requests will be consider as normal and when huge amount of request arrived then CUSUM value will increase and system will raise attack alarm.

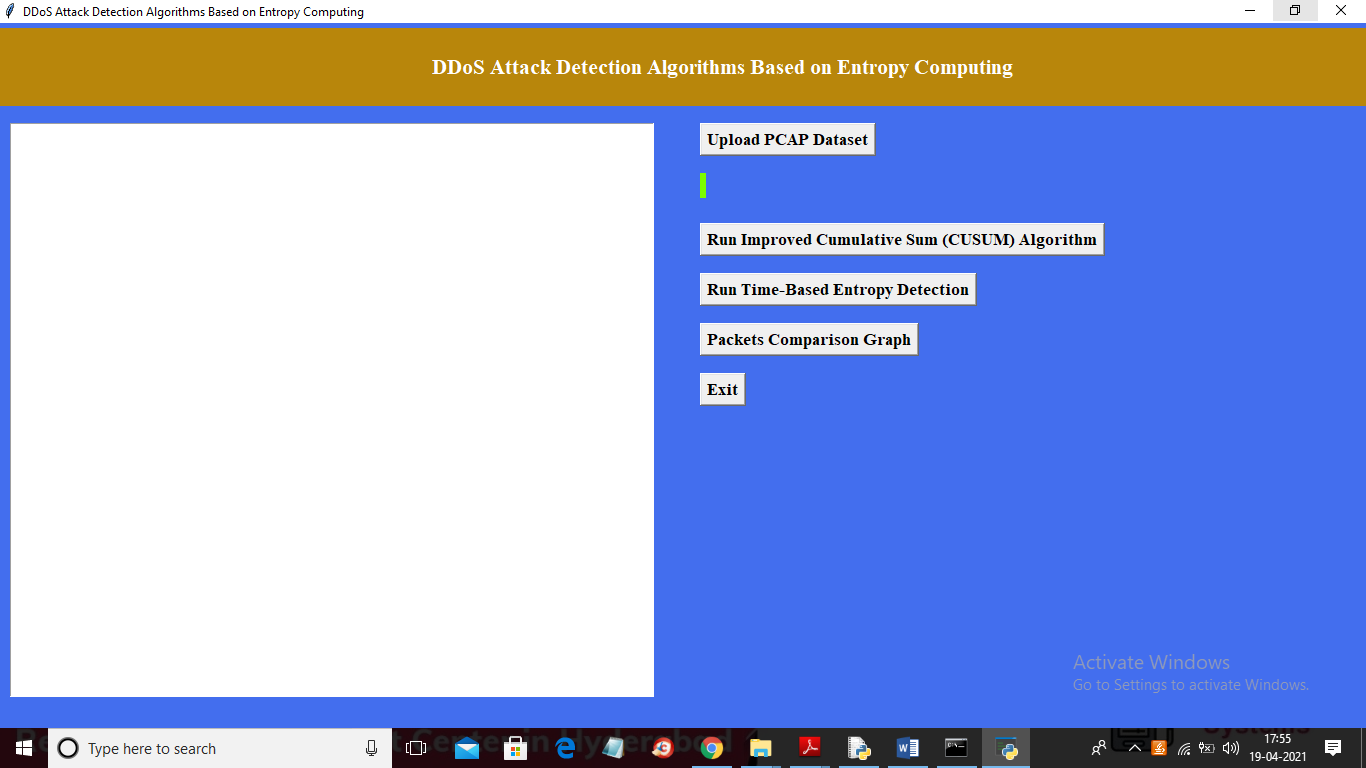
CUSUM is sliding window base technique and author saying we can use time based technique also where monitoring time will be set for request, for example application will monitor first packet and then keeps on capturing for next 10 seconds and store all packets in vector. After 10 seconds vector will be analysed using CUSUM formula to check request quantity and if more request arrive then vector will have more high values then system will raise alarm for attack.

To implement this project author using WINPCAP files which contains network packet data and we are also using same files to analyse packets and if huge requests arrive from same IP then CUSUM of that IP address will be high which indicate it as attack.

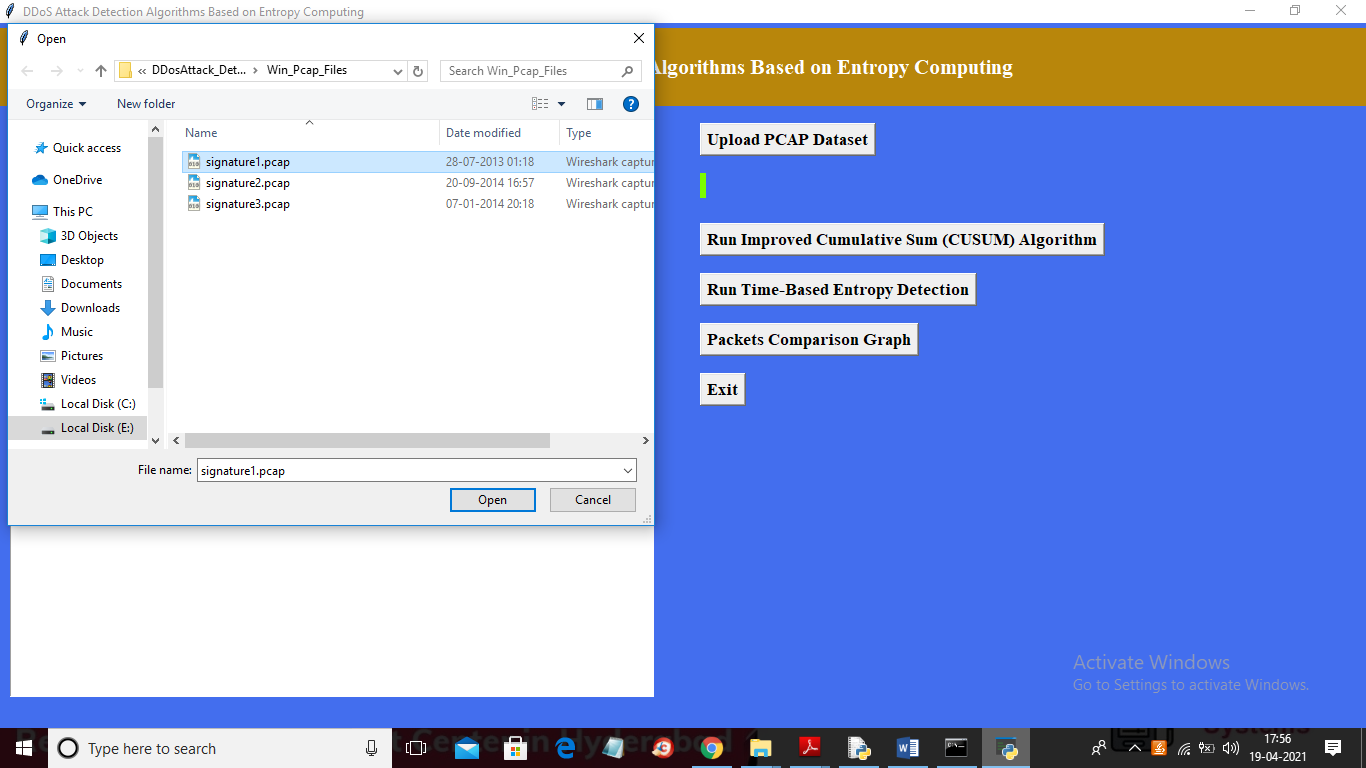
All WINPCAP file are stored inside ‘Win\_Pcap\_Files’ folder.

SCREEN SHOTS

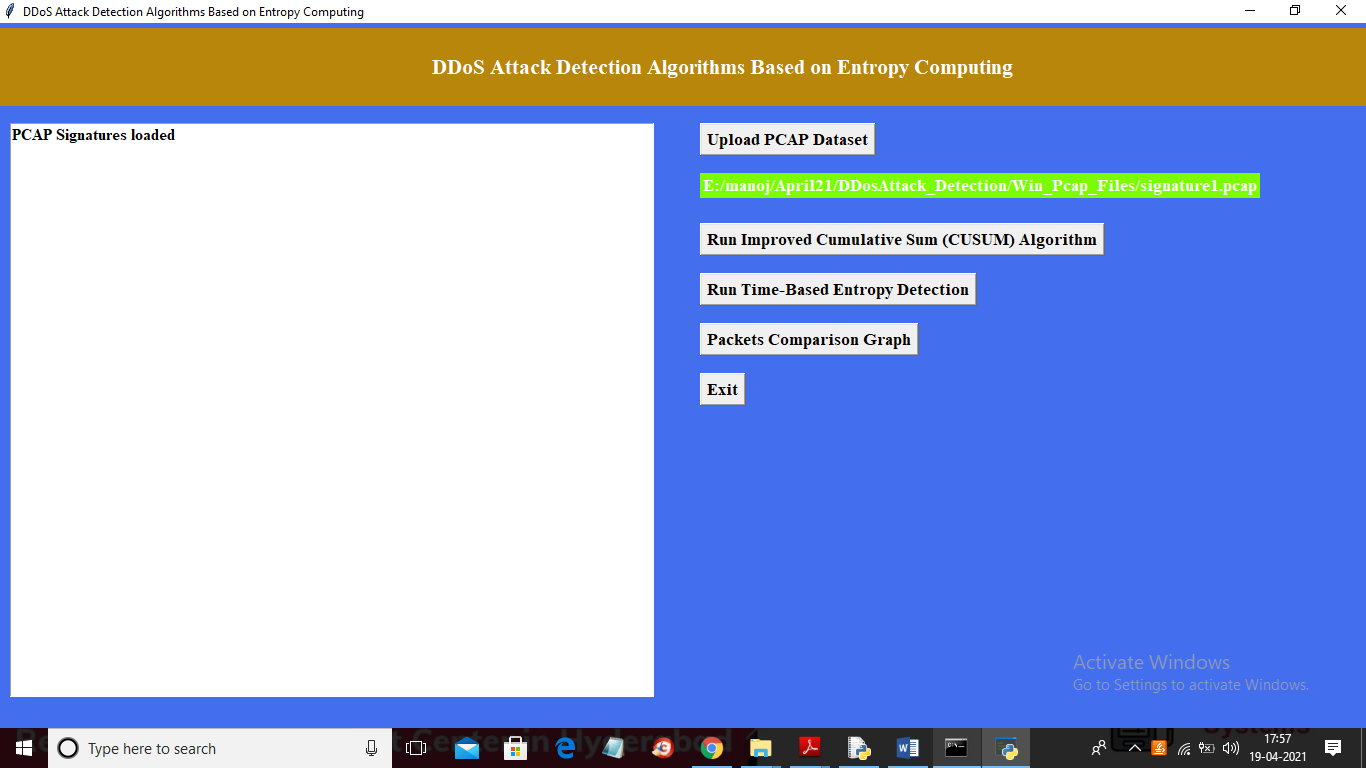
To run project double click on ‘run.bat’ file to get below screen



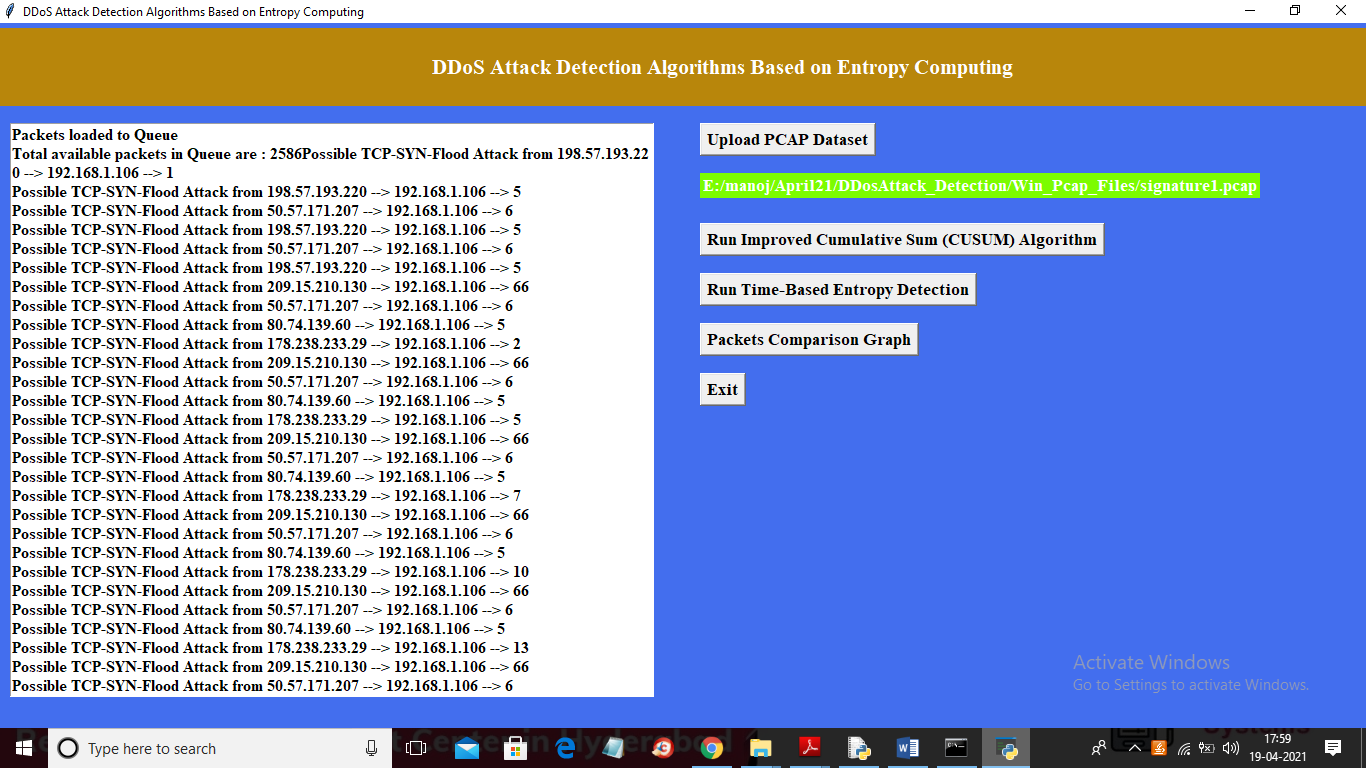
In above screen click on ‘Upload PCAP Dataset’ button to upload PCAP file and to get below screen



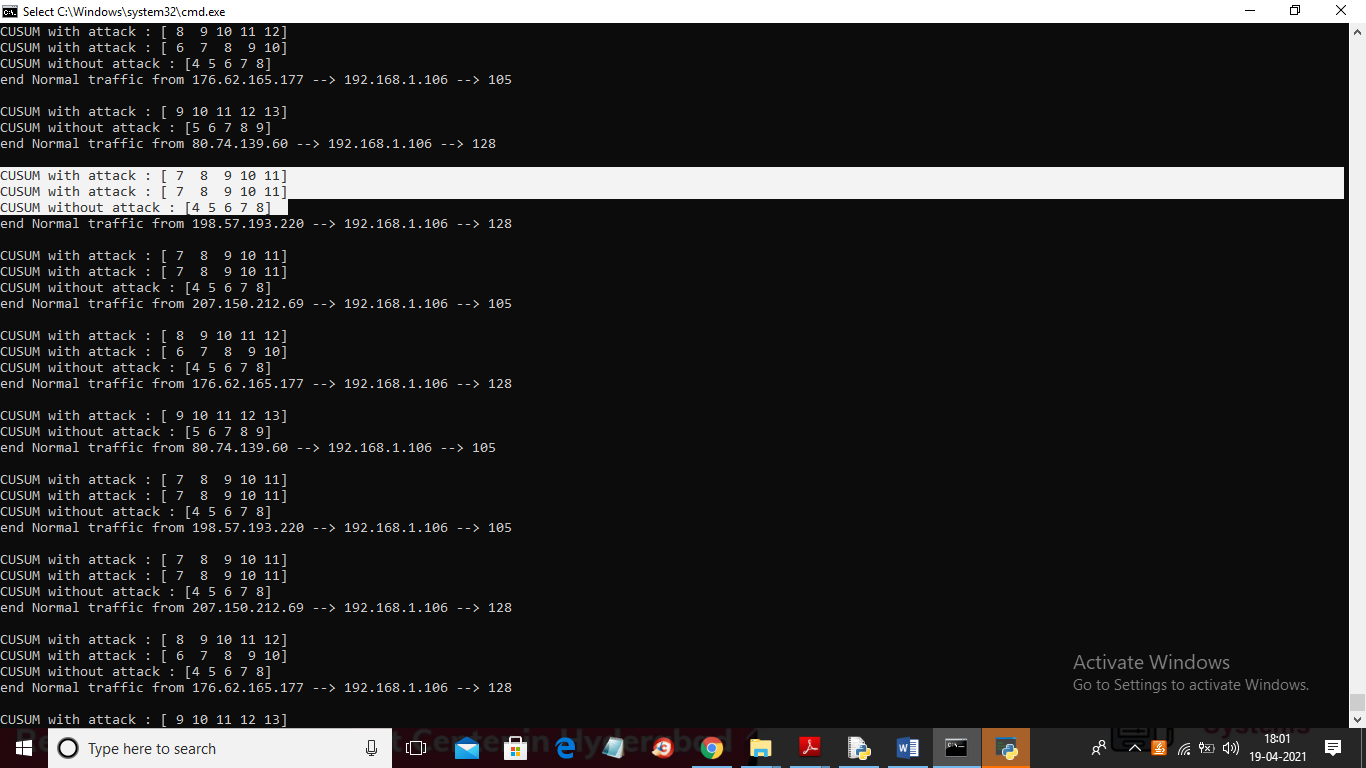
In above screen selecting and uploading ‘signature.pcap’ file and then click on ‘Open’ button to get below screen



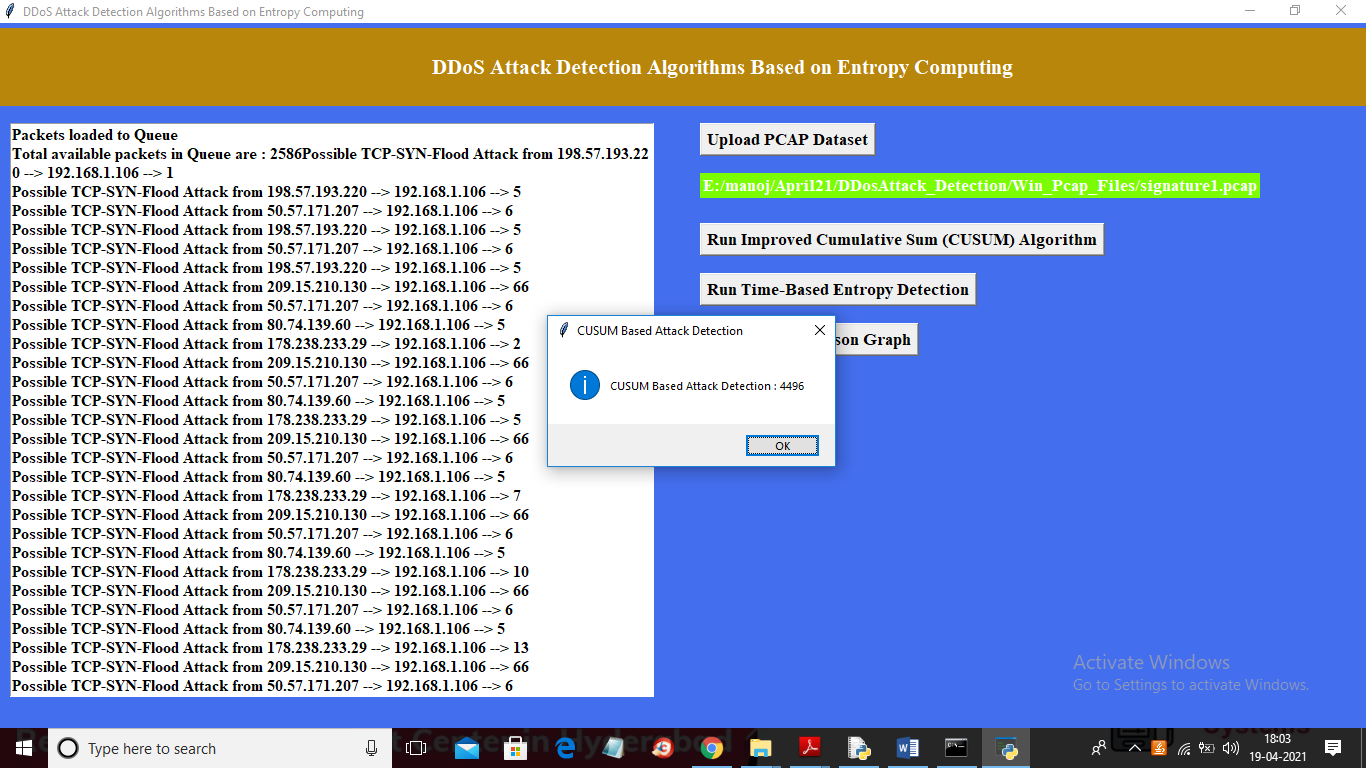
In above screen pcap file loaded and now click on ‘Run Improved Cumulative Sum (CUSUM) Algorithm’ button to analyse pcap file with CUSUM technique



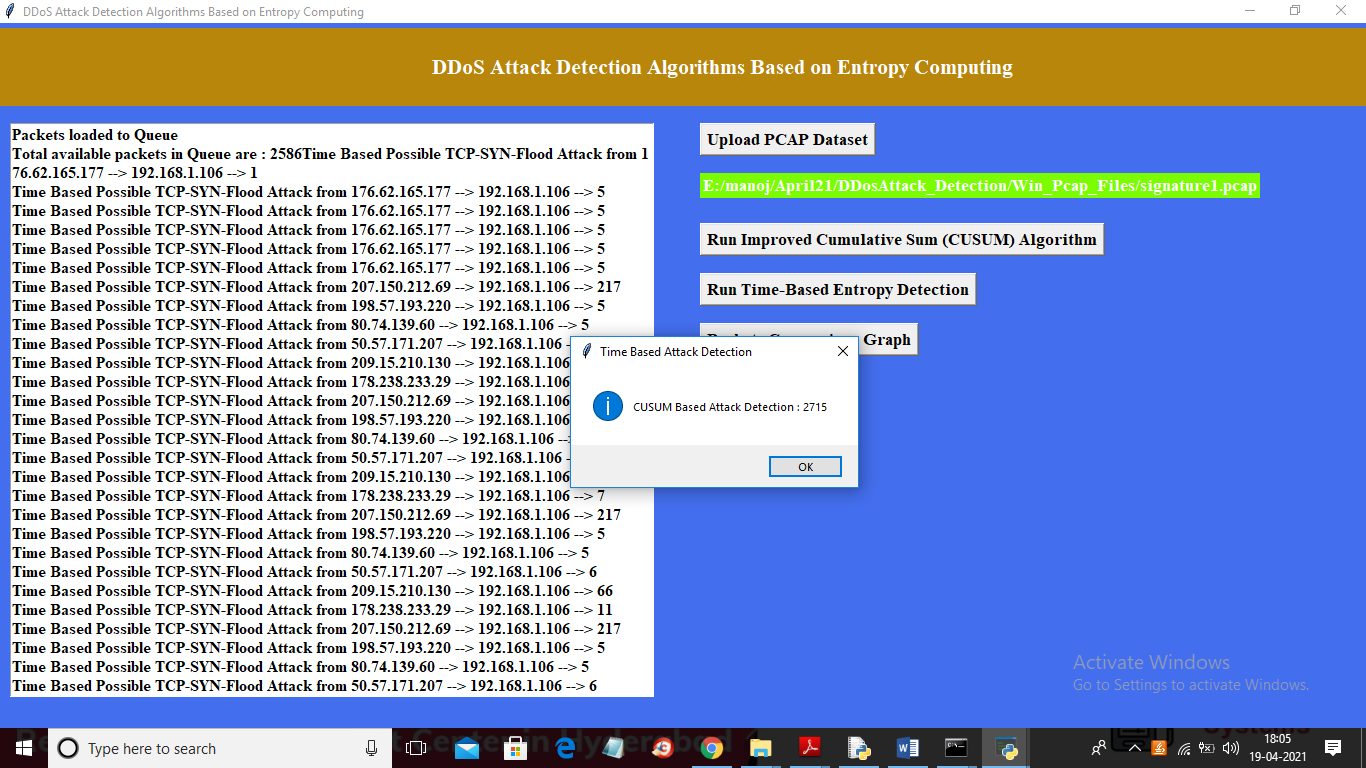
In above screen each packet analyse and we can see source and destination port number and we can see CUSUM values for each packet in below screen



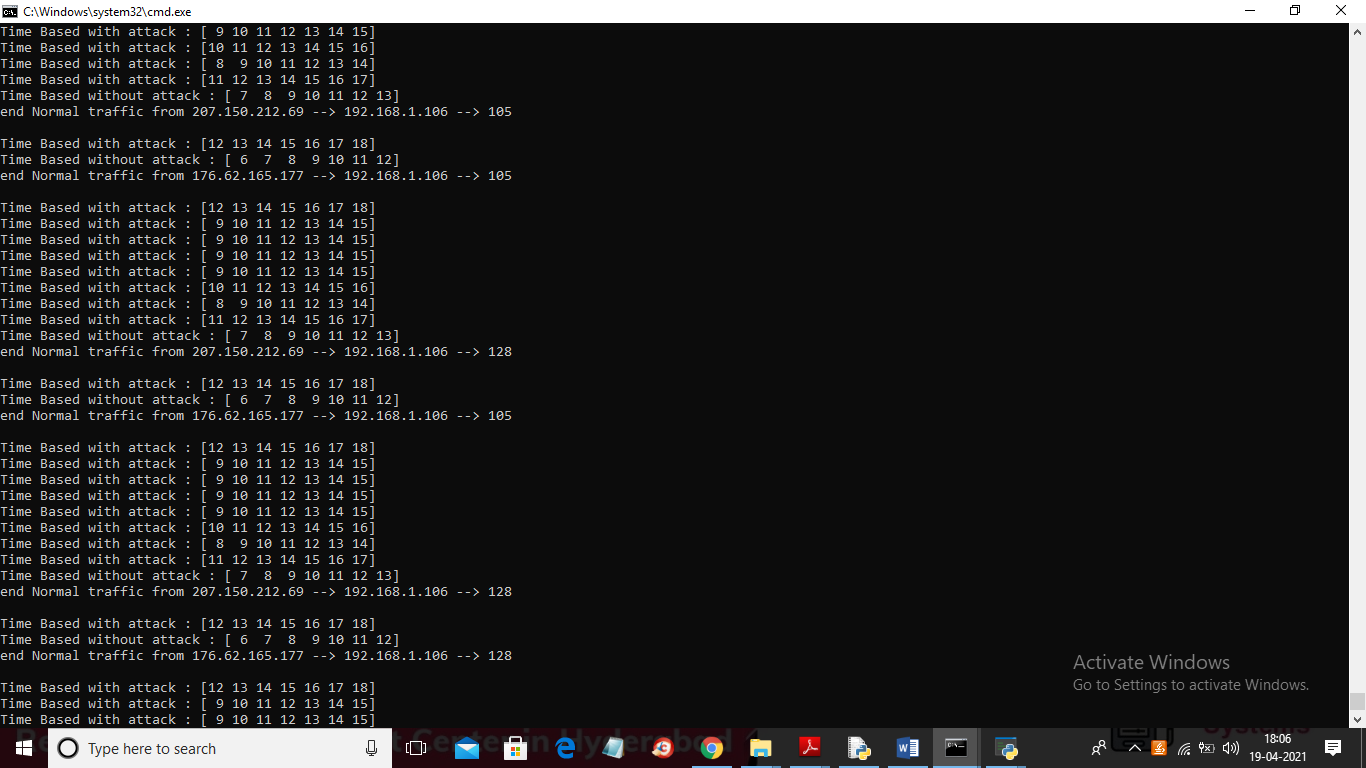
In above screen for each packet we got CUSUM array and we can see CUSUM array with less values has no attack and when attack occur then CUSUM array contains more values and in above screen without attack CUSUM value is [4 5 6 7 8] and when attack occur then CUSUM values changed to [7 8 9 10 11]. So by analysing this CUSUM array we can detect whether request is normal or attack.



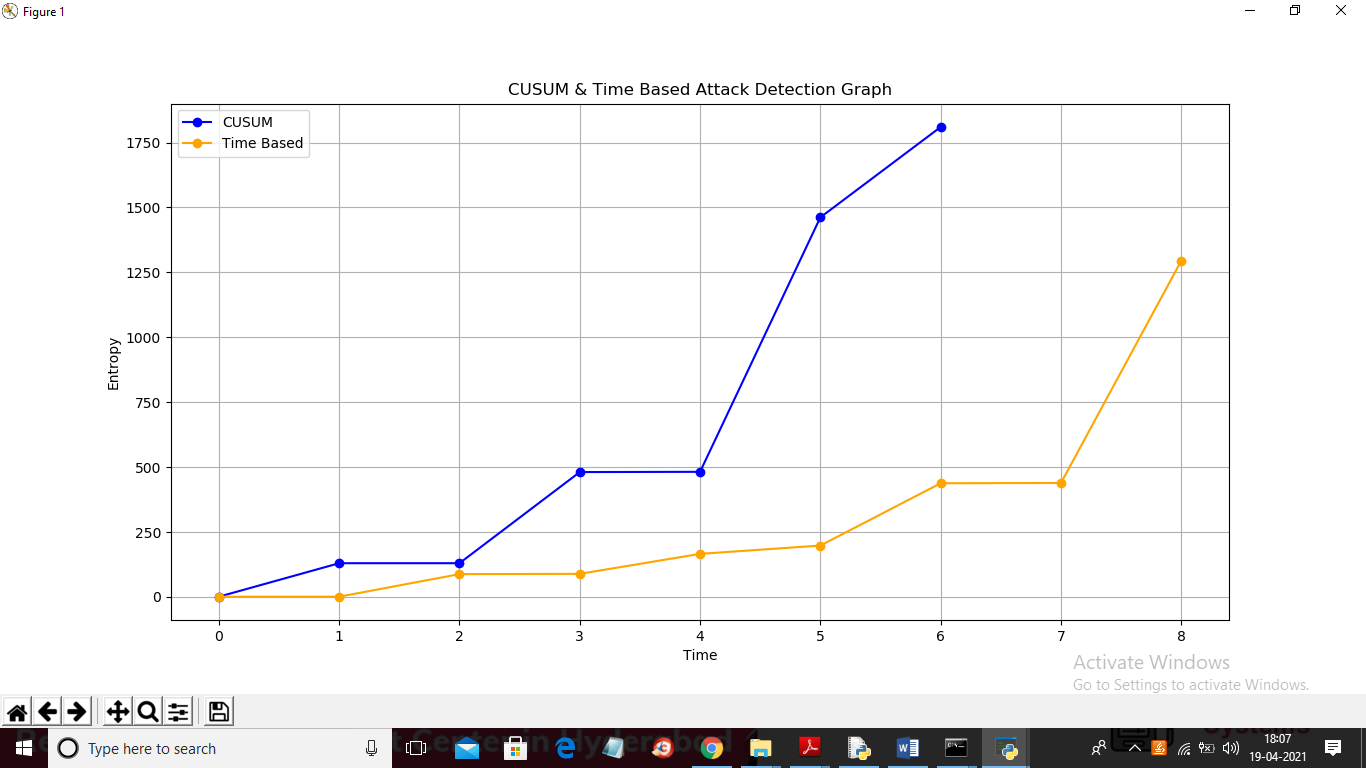
In above screen we can see PCAP file contains total 4496 attacks and now click on ‘Run Time-Based Entropy Detection’ button to run Time Based technique



In above screen with time based application detected 2715 attacks as this technique monitors once in 10 seconds so its detection rate will be less and in below black console we can see Time Based CUSUM values



In above screen with Time Based also we can see more request variation in attack scenario compare to normal scenario and now click on ‘Packets Comparison Graph’ button to get below graph



In above graph x-axis represents time and y-axis represents entropy values and in above graph blue is for Window Based CUSUM and orange line is for Time Based CUSUM and in both technique we can see entropy values increases heavily when attack occurred. In above graph up to 5 seconds in x-axis both technique has low entropy values and after application received more request from same IP which causes growth in entropy value