Detecting Malicious Twitter Bots Using Machine Learning

In this paper author is using machine learning algorithm such as Logistic Regression to detect BOTS from tweets and to implement this paper author has given 3 modules

Module 1: Tweet Extraction) Using this module we will extract tweets from online or offline and every time internet will not be available so we are using offline KAGGLE tweets dataset. By using this module we will read or extract all tweets from dataset. If we are downloading tweets online then we need WOEID from twitter but we are using dataset so WOEID not require.

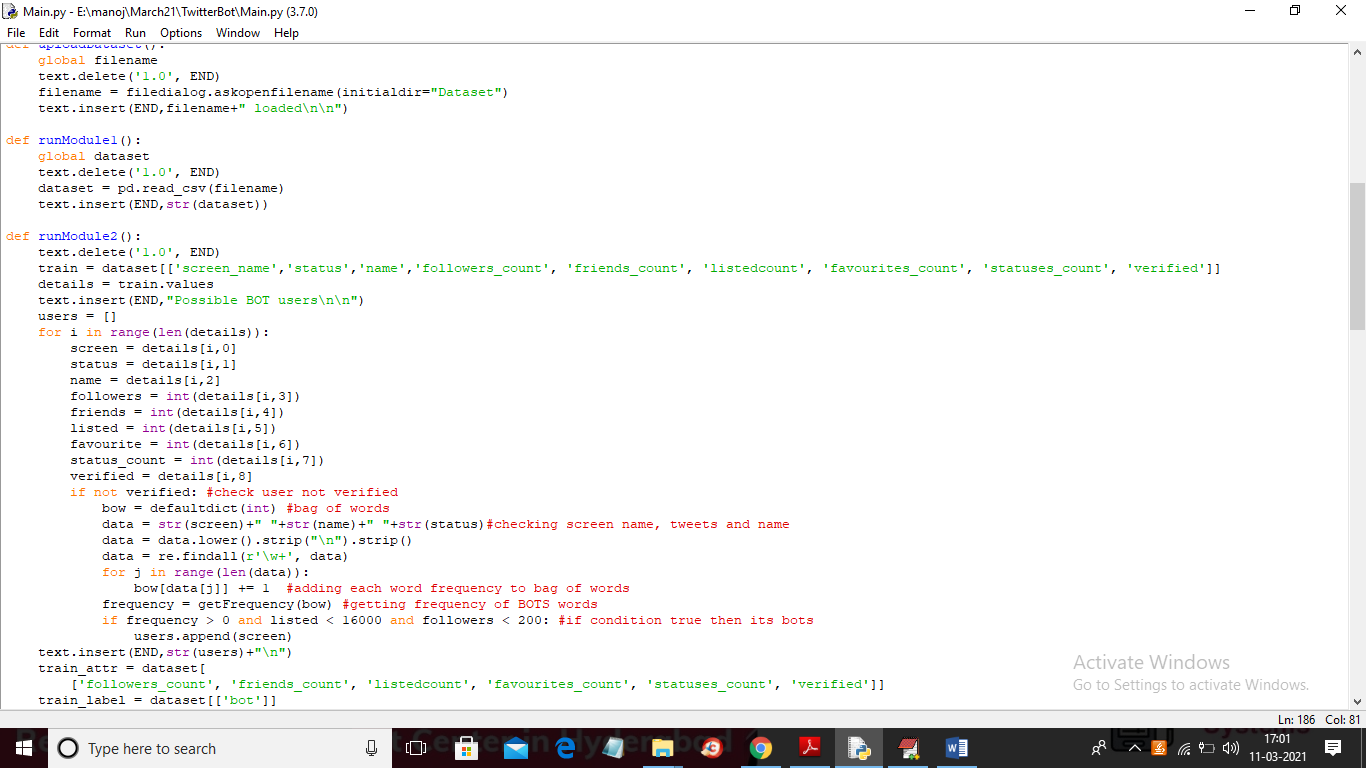
Module 2: (Recognize Twitter Bots using ML): In this module we are extracting features from tweets such as Activity, Anonymity and Amplification. Activity refers to finding tweet frequency and Anonymity refers to account information and Amplification refers to retweet count. By using above 3 concepts author is checking whether account is normal or bot.

For example

Checking all tweets for BOTS words and then finding its frequency

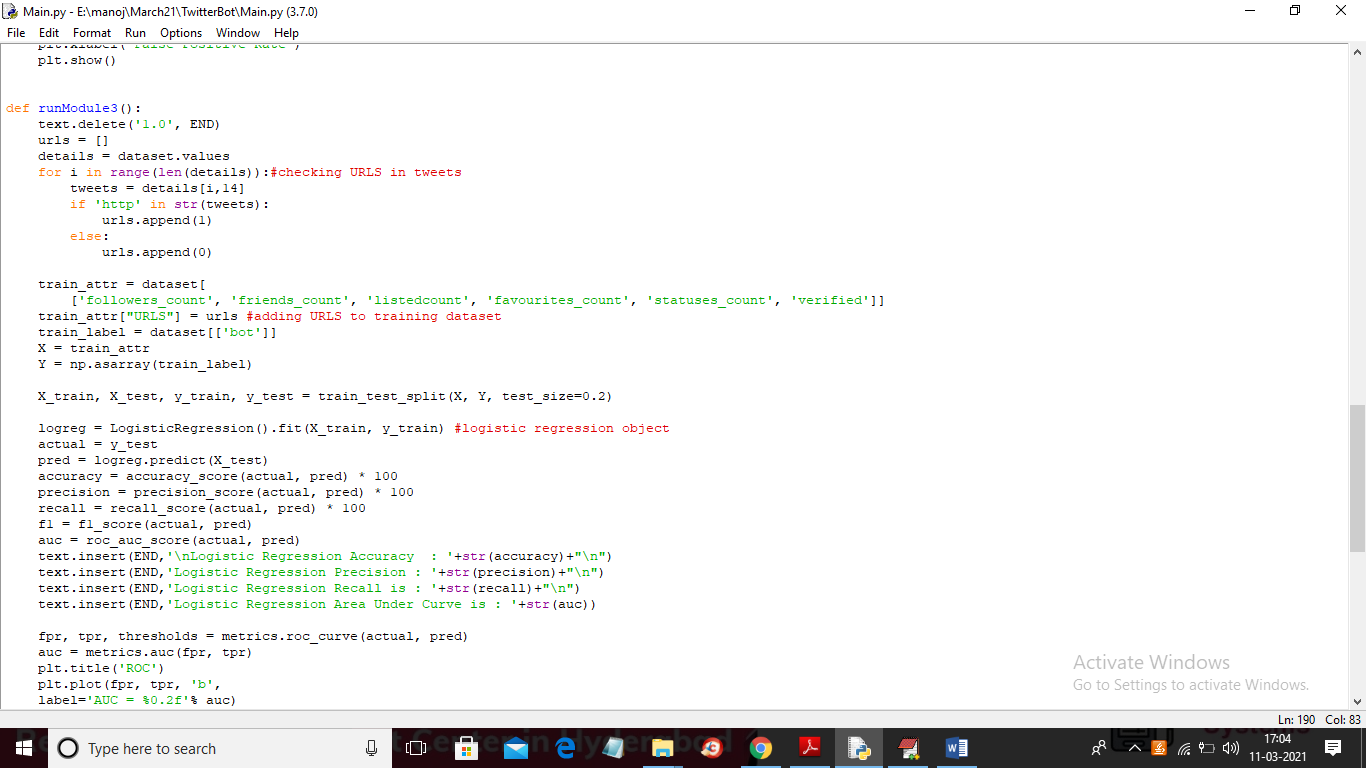
If account not verified and If listed count < 16000 and followers < 200 and retweet\_count > 10000 then account will be consider as BOT

By using above finding we will train Logistic regression and calculate bot prediction accuracy. Below screen shots showing code with comments about this methods

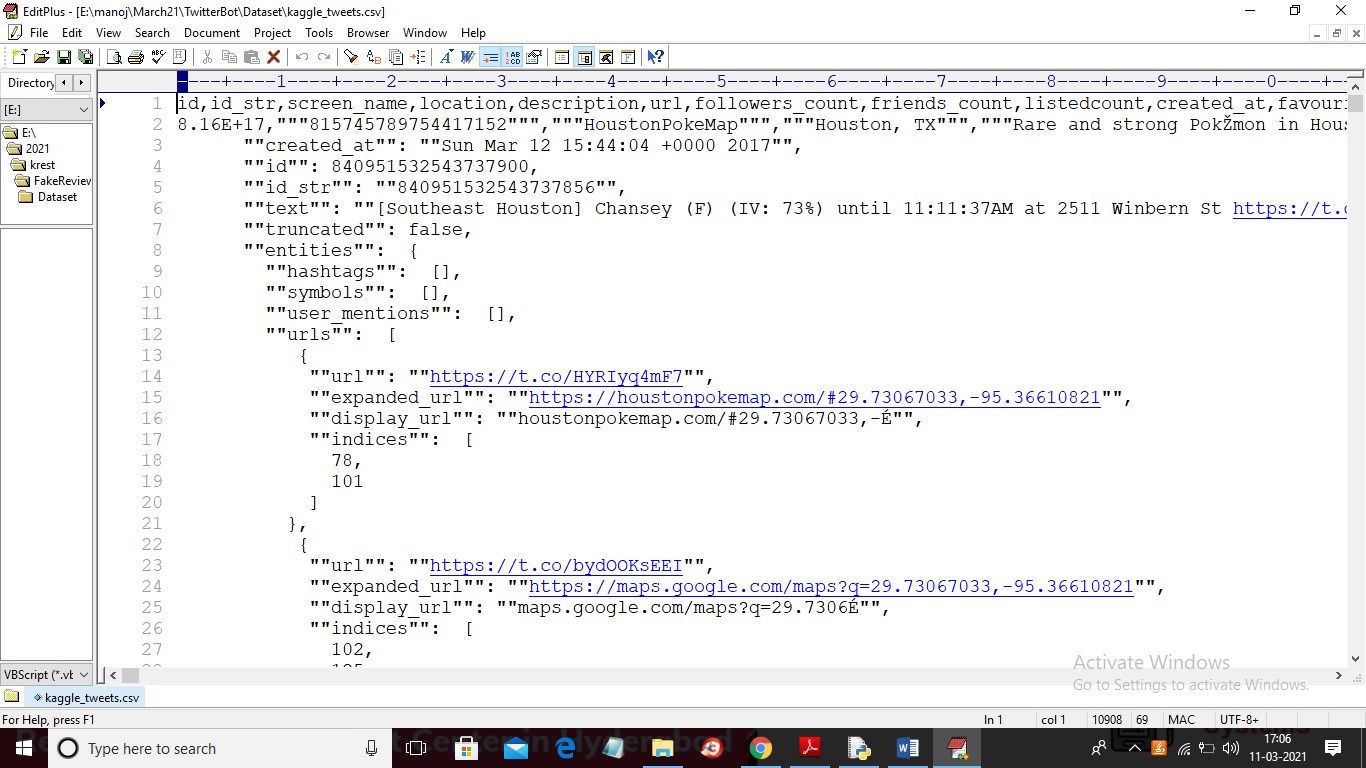


In above screen read red colour line comments to understand concept

Module 3: (Recognize Malicious URLS using ML): Using this module we analyse all tweets and check if tweet contains more number of URLs then it will consider as malicious URLS and below code with screen shots showing method3 checking for malicious URL



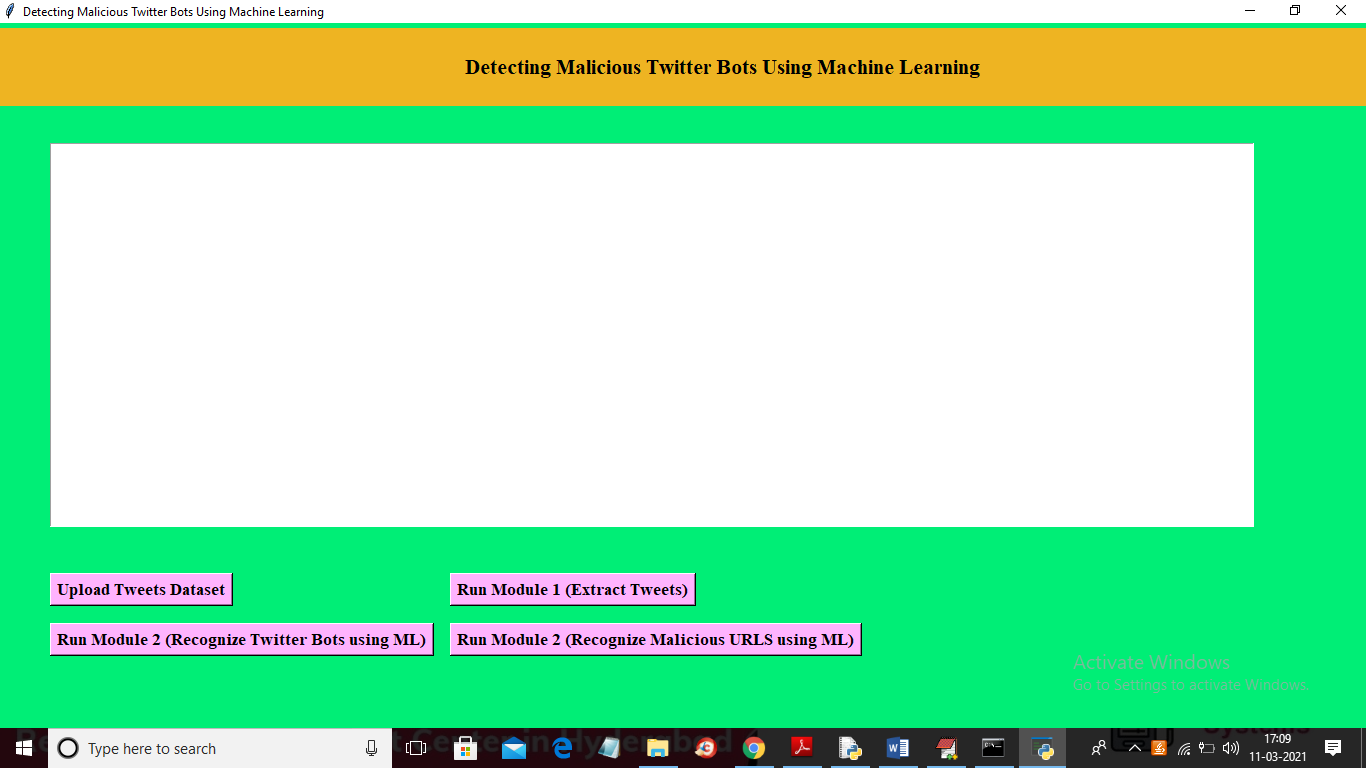
Dataset used in this project saved inside ‘Dataset’ folder and below screen shots showing all dataset details



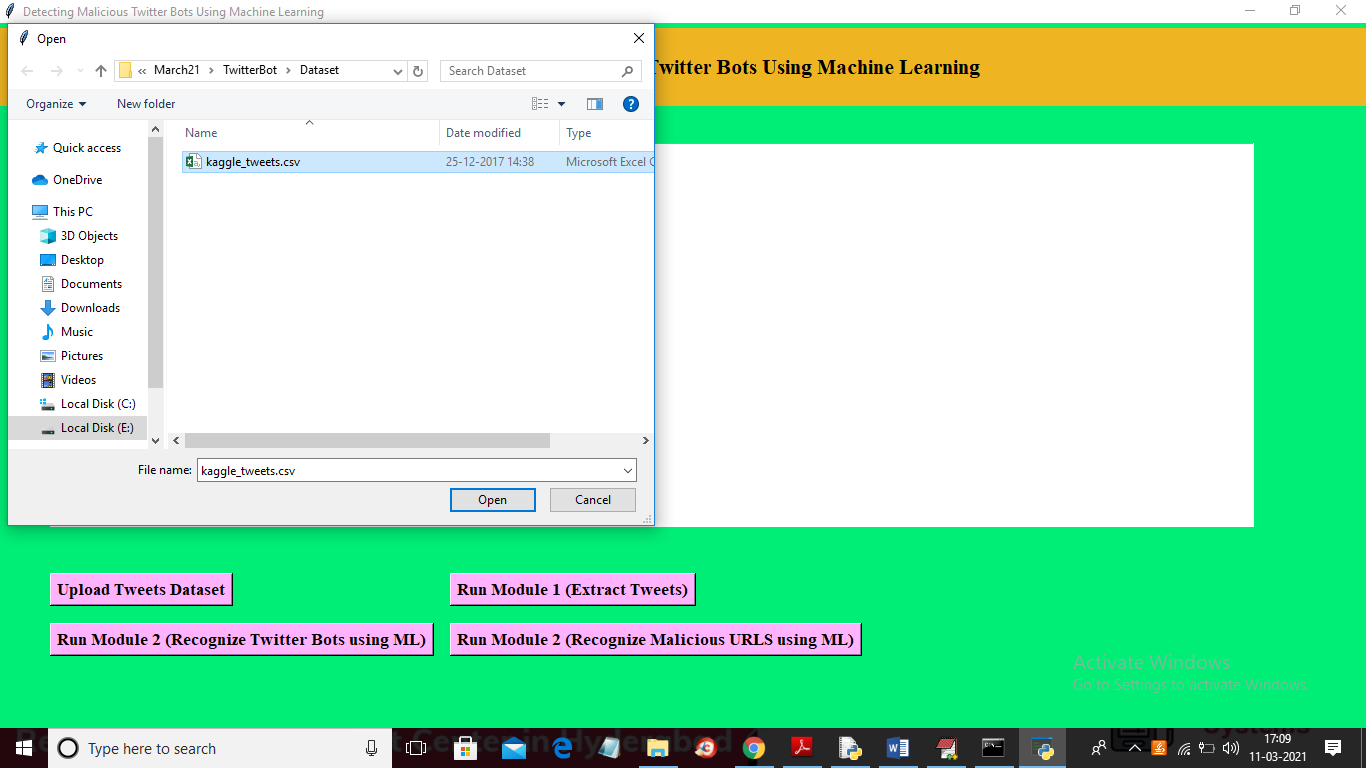
In above dataset screen in first line we can see all dataset column names and from second lines we can see dataset values.

SCREEN SHOTS

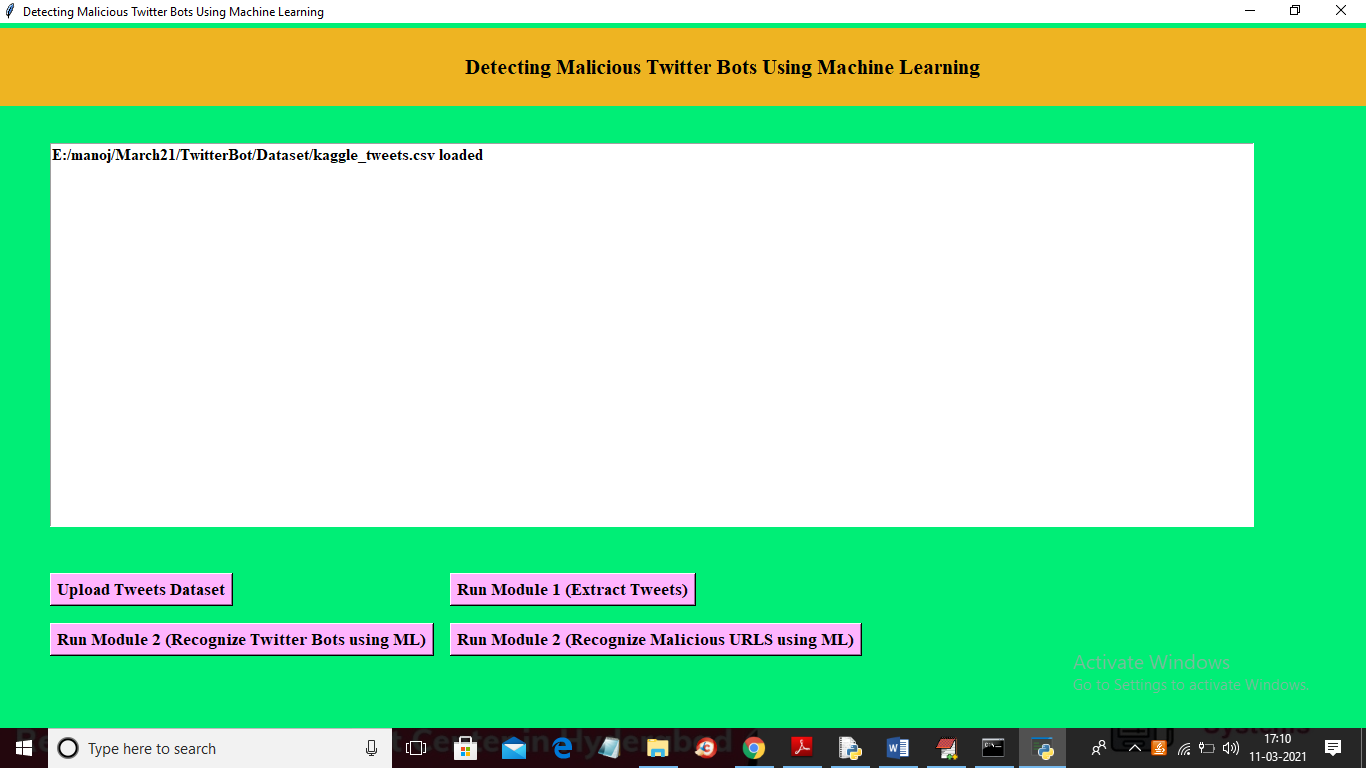
To run project double click on ‘run.bat’ file to get below screen



In above screen click on ‘Upload Tweets Dataset’ button and then upload dataset



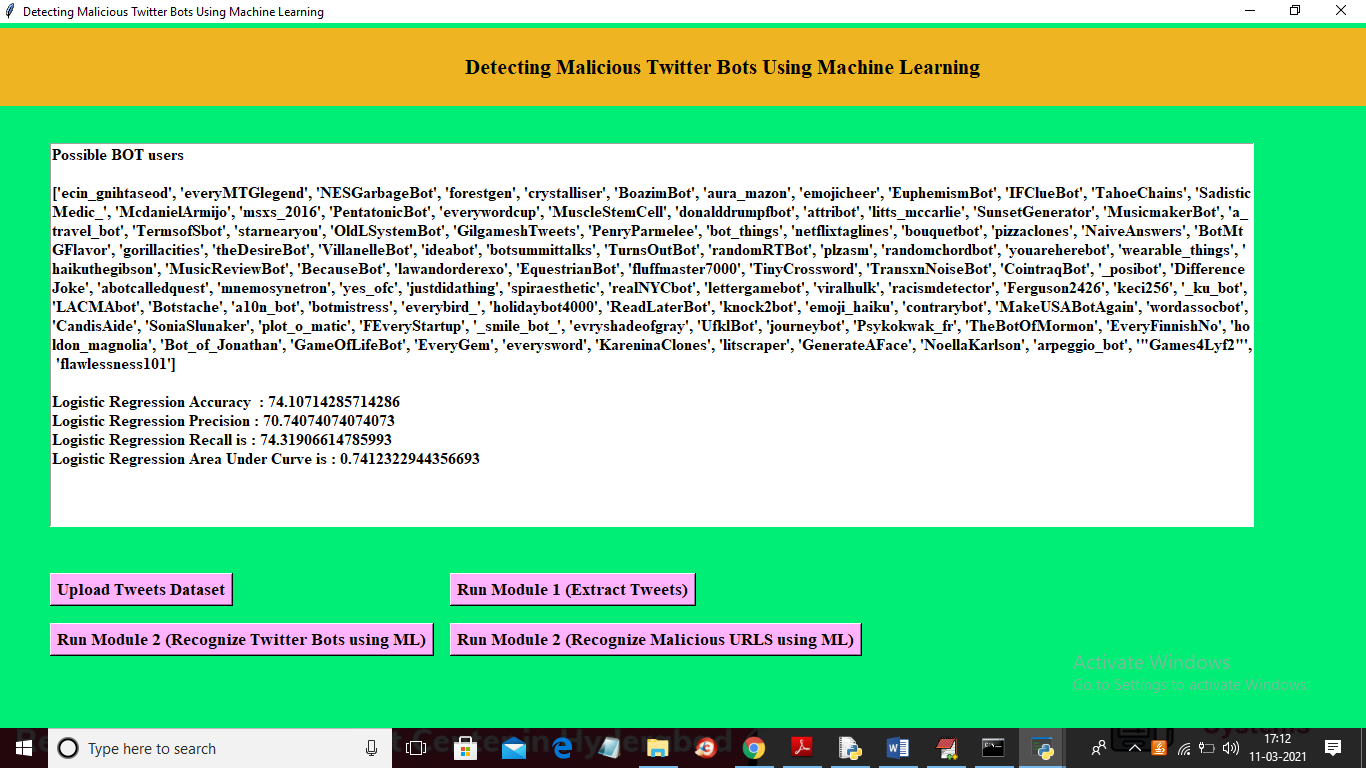
In above screen selecting and uploading ‘kaggle\_tweets.csv’ file and then click on ‘Open’ button to load dataset and to get below screen



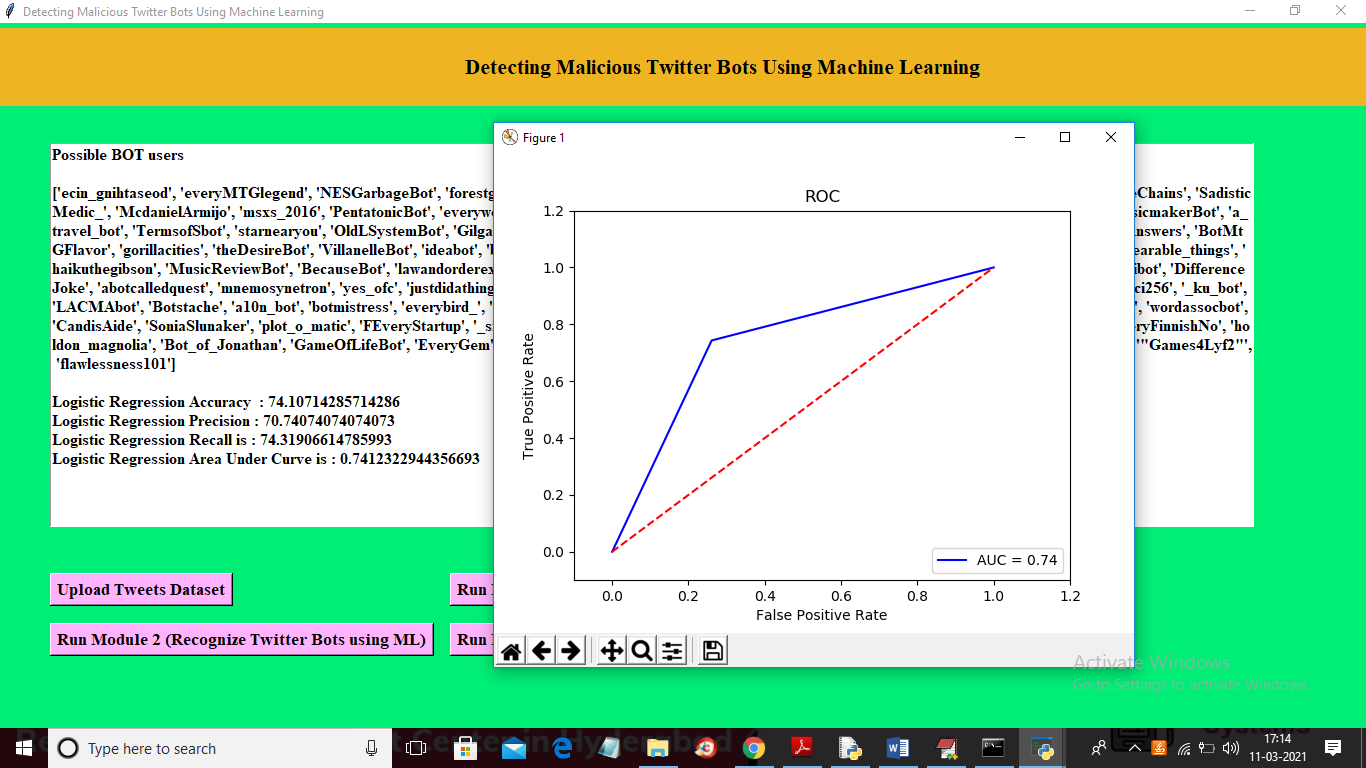
In above screen dataset loaded and now click on ‘Run Module 1 (Extract Tweets)’ button to read all tweets from dataset and to get below screen



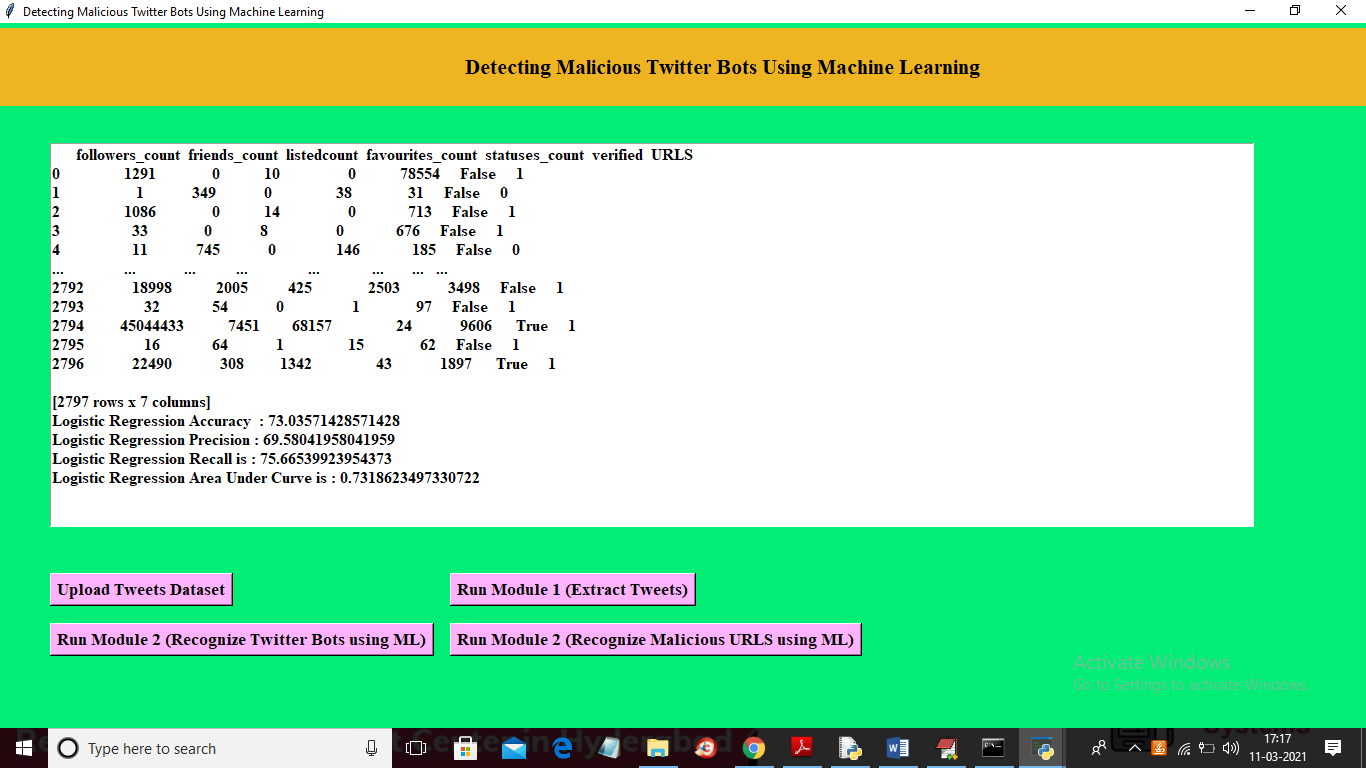
In above screen application read all tweets and displaying few tweets in above screen and now click on ‘Run Module 2 (Recognize Twitter Bots using ML)’ button to recognize BOTS user and then apply logistic regression ML to calculate BOT prediction accuracy



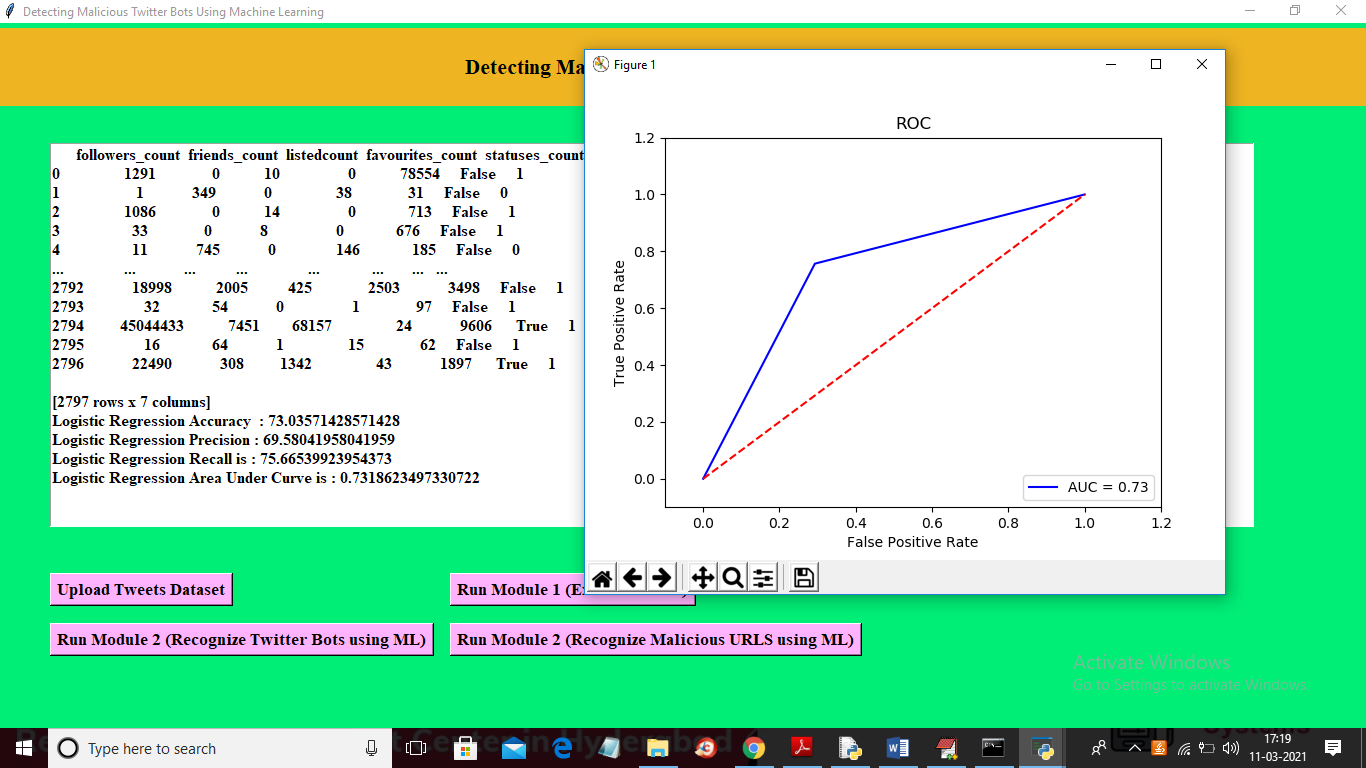
In above screen in square brackets we can see SCREEN NAME of all BOTS account and then we got ML accuracy of Logistic Regression is 74% and in below screen we can see ROC graph



In above graph x-axis represents False Positive Rate (wrong prediction) and y-axis represents True Positive Rate (Correct Prediction) and red line represents False Rate and blue line represents True prediction Rate and from above graph we can conclude that True rate is higher than false prediction rate. Now click on ‘Run Module 2 (Recognize Malicious URLS using ML)’ button to find malicious URLS and then calculate malicious URL prediction rate.



In above screen in last column we find URL as malicious or non-malicious and in above screen in last column 1 indicates Non-Malicious URL and 0 indicate Malicious URL and in above screen we can see URL prediction accuracy as 73% and below is URL prediction ROC graph



Above screen represents malicious URL ROC graph and blue line rate is higher than red colour false prediction rate