



ICT1002

Digital Crime Analyser

Team 29 - User's Guide

SOFTWARE DESCRIPTION	3
Description	3
Benefits and Value	3
Importing of dataset	4
Filtering search data	6
Prediction of attacks	7
Generating graphical displays	8
Exporting of dataset	10

SOFTWARE DESCRIPTION

Description

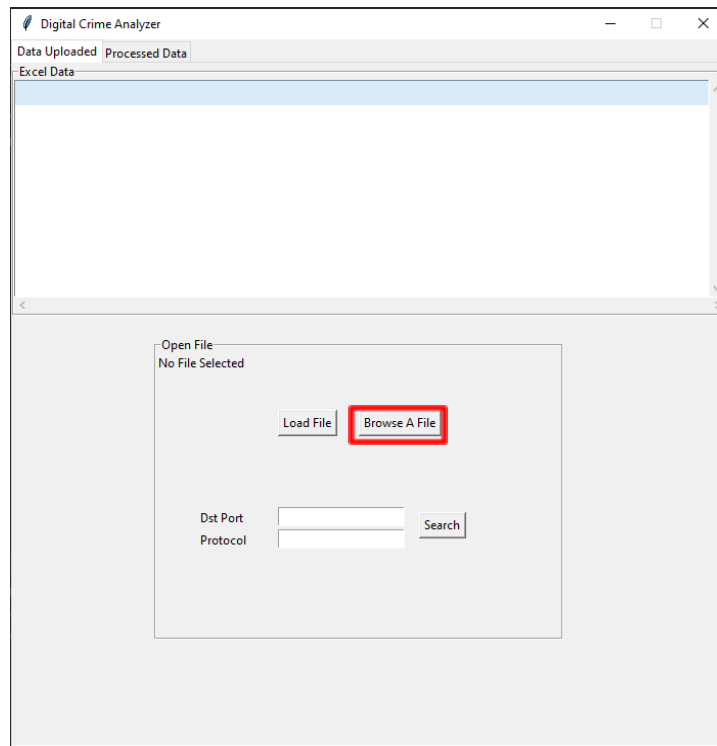
The software will analyse datasets as well as extract them into a new format that will better help crime investigators. It can also display statistical data which can give a better visualization for the user.

Benefits and Value

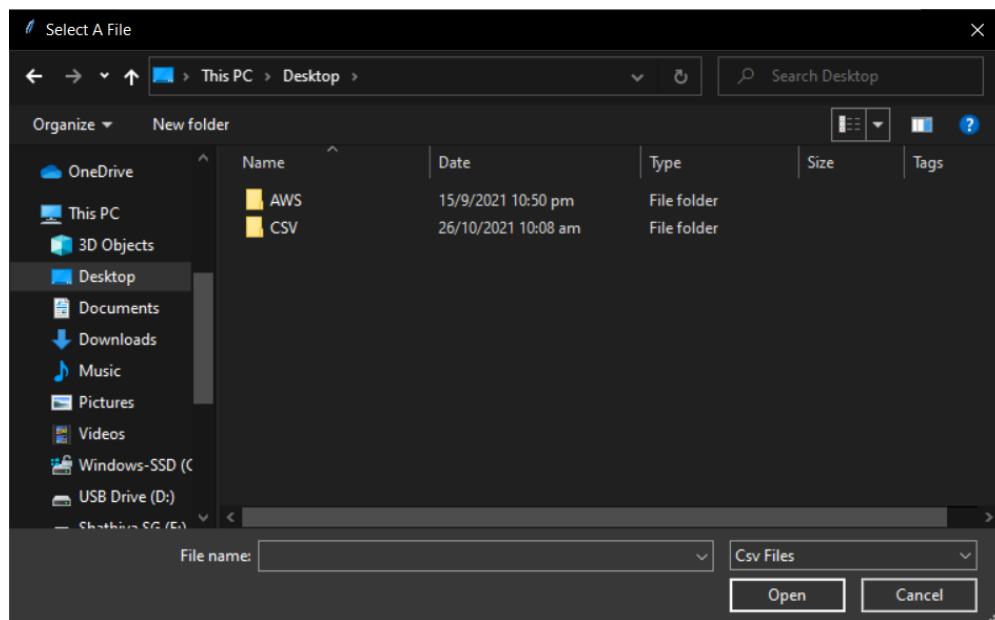
The investigators can better determine what attack has occurred according to the data. It can also give a better understanding of how and what preparation measures to take towards future attacks.

Importing of dataset

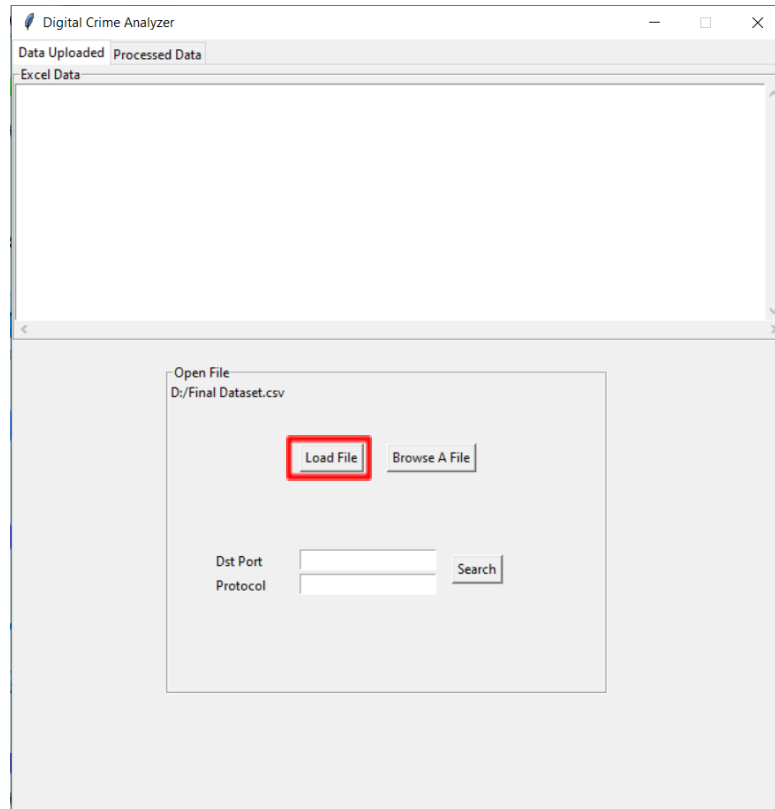
- 1) Click the "Browse A File" button.



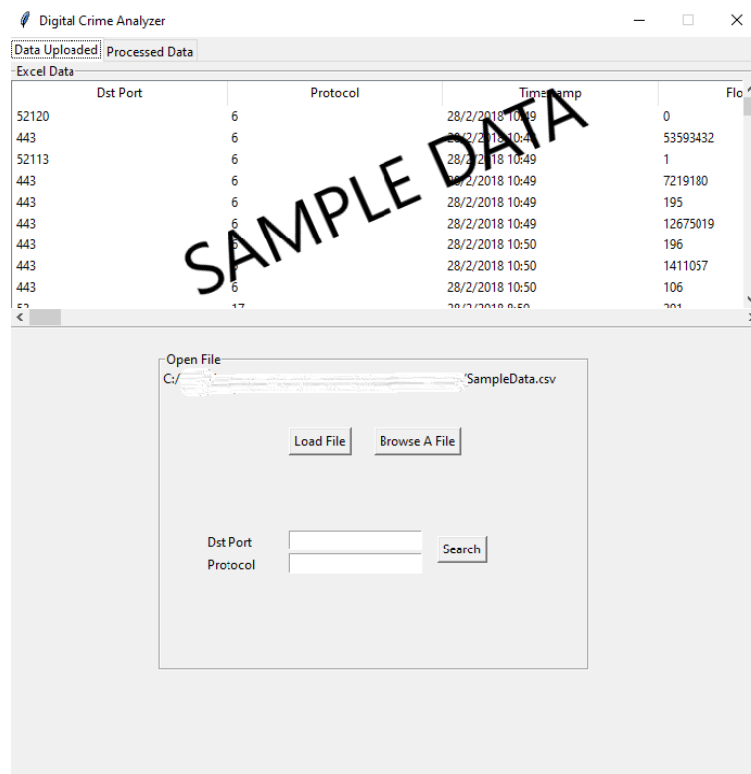
- 2) A prompt will appear for users to select their dataset. Only in .csv file format is allowed. Users will have to click on 'Open' once they have selected their file. **(Use provided dataset located in "Sample Data/Final Dataset.csv")**



3) Click the “Load File” button.

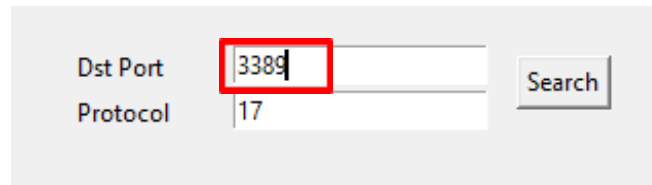


4) The file will be loaded and values will appear under ‘Excel Data’



Filtering search data

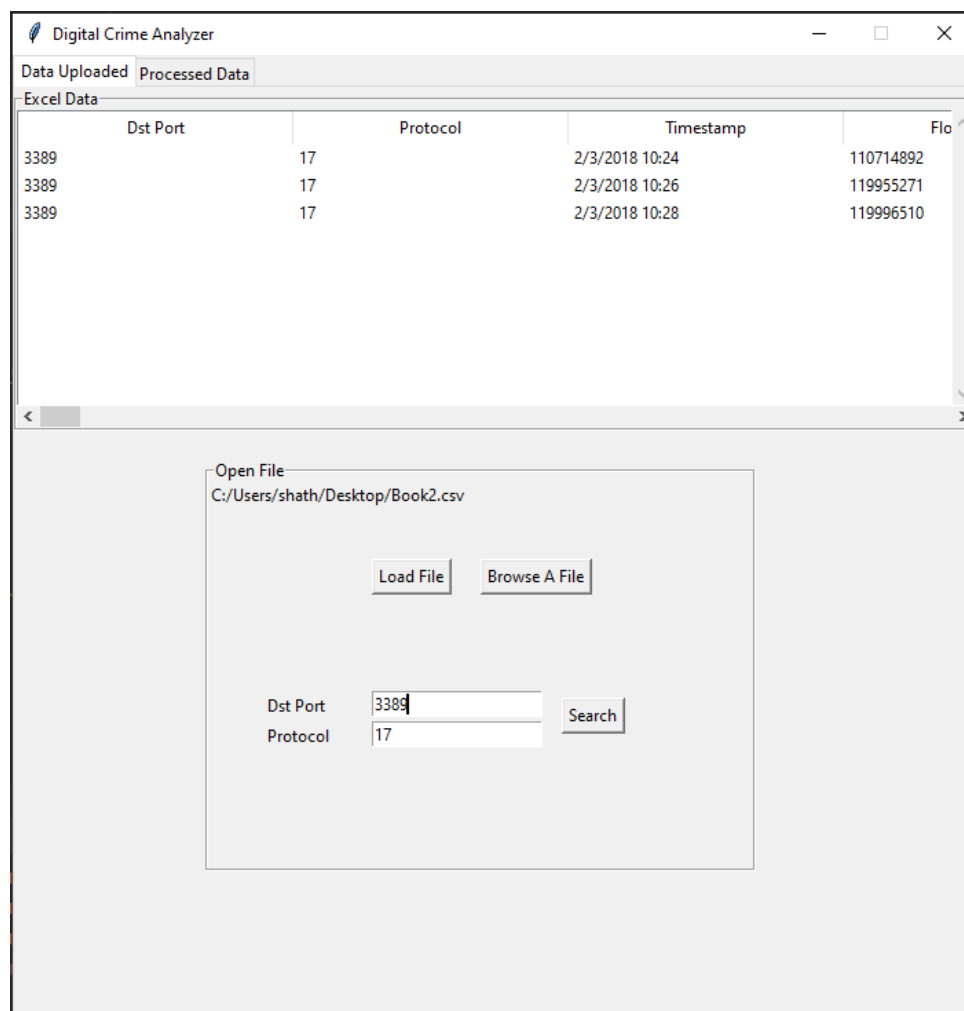
- 1) The user can enter a value for "Destination port", "Protocol" or both



A search filter form with two input fields and a search button. The first field is labeled "Dst Port" and contains the value "3389", which is highlighted with a red rectangle. The second field is labeled "Protocol" and contains the value "17". A "Search" button is located to the right of the fields.

Dst Port	3389
Protocol	17
<input type="button" value="Search"/>	

- 2) The values in the 'Excel Data' table will be updated when the search button is clicked

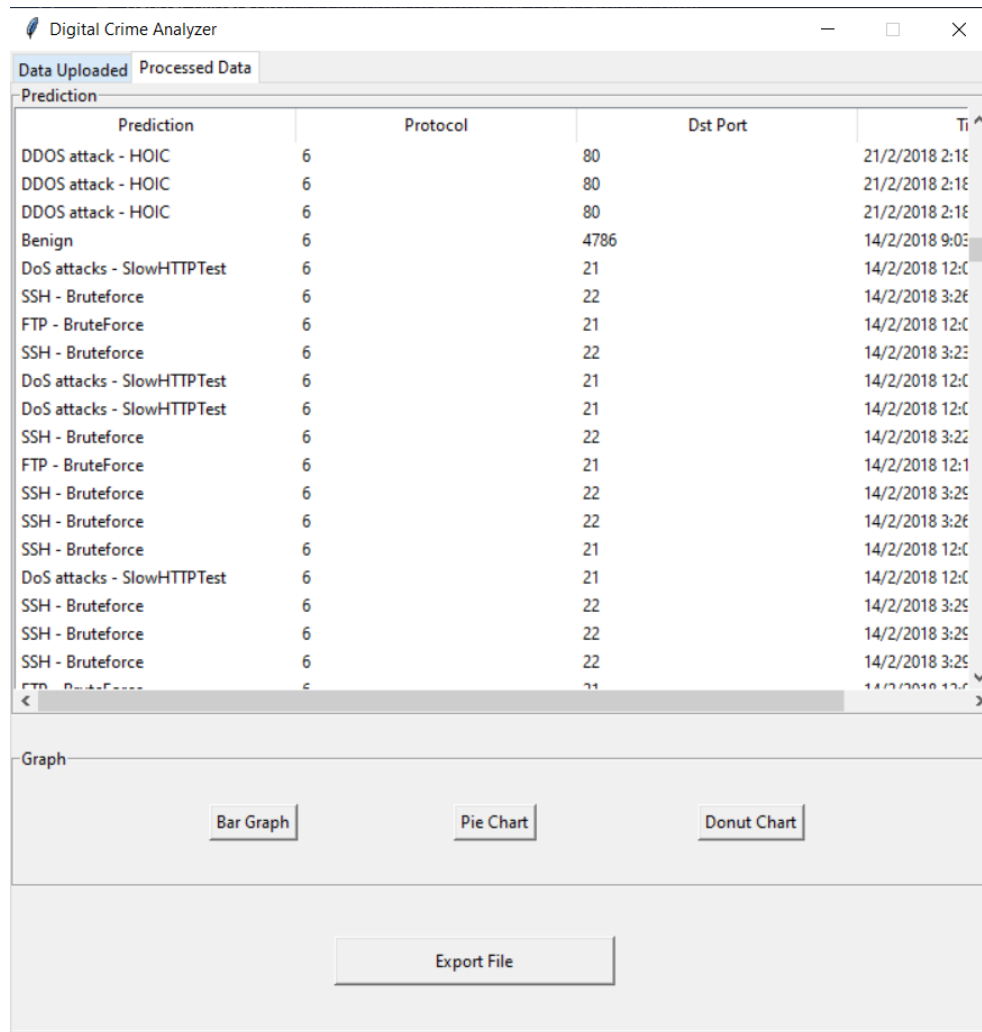


The screenshot shows the "Digital Crime Analyzer" application window. It has two tabs: "Data Uploaded" and "Processed Data". The "Processed Data" tab is active, showing an "Excel Data" table. The table has five columns: "Dst Port", "Protocol", "Timestamp", and "Flo". It contains three rows of data, all with "Dst Port" value 3389 and "Protocol" value 17. Below the table, there is a section titled "Open File" with the path "C:/Users/shath/Desktop/Book2.csv". It includes "Load File" and "Browse A File" buttons. At the bottom, there is a search filter form identical to the one in the first image, with "Dst Port" set to 3389 and "Protocol" set to 17.

Dst Port	Protocol	Timestamp	Flo
3389	17	2/3/2018 10:24	110714892
3389	17	2/3/2018 10:26	119955271
3389	17	2/3/2018 10:28	119996510

Prediction of attacks

The prediction model is created using machine learning, and it predicts the type of attack based on the dataset.



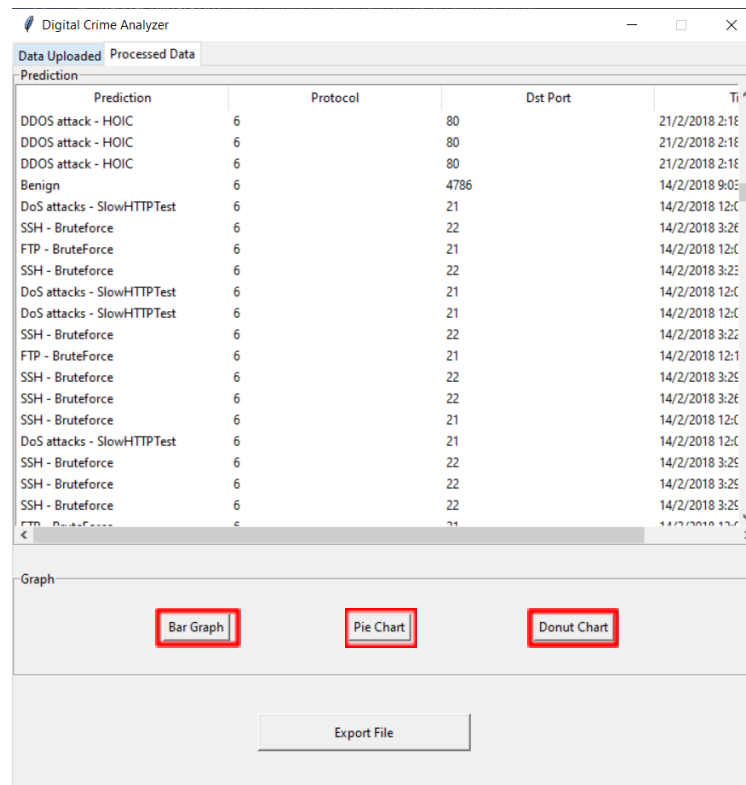
The screenshot shows the 'Digital Crime Analyzer' application window. It has two tabs: 'Data Uploaded' and 'Processed Data'. The 'Processed Data' tab is active, displaying a table of prediction results. The table has four columns: 'Prediction', 'Protocol', 'Dst Port', and 'Time'. Below the table, there is a 'Graph' section with three buttons: 'Bar Graph', 'Pie Chart', and 'Donut Chart'. At the bottom, there is an 'Export File' button.

Prediction	Protocol	Dst Port	Time
DDOS attack - HOIC	6	80	21/2/2018 2:16
DDOS attack - HOIC	6	80	21/2/2018 2:16
DDOS attack - HOIC	6	80	21/2/2018 2:16
Benign	6	4786	14/2/2018 9:03
DoS attacks - SlowHTTPTest	6	21	14/2/2018 12:0
SSH - BruteForce	6	22	14/2/2018 3:26
FTP - BruteForce	6	21	14/2/2018 12:0
SSH - BruteForce	6	22	14/2/2018 3:23
DoS attacks - SlowHTTPTest	6	21	14/2/2018 12:0
DoS attacks - SlowHTTPTest	6	21	14/2/2018 12:0
SSH - BruteForce	6	22	14/2/2018 3:22
FTP - BruteForce	6	21	14/2/2018 12:1
SSH - BruteForce	6	22	14/2/2018 3:25
SSH - BruteForce	6	22	14/2/2018 3:26
SSH - BruteForce	6	21	14/2/2018 12:0
DoS attacks - SlowHTTPTest	6	21	14/2/2018 12:0
SSH - BruteForce	6	22	14/2/2018 3:25
SSH - BruteForce	6	22	14/2/2018 3:25
SSH - BruteForce	6	22	14/2/2018 3:25
FTP - BruteForce	6	21	14/2/2018 12:0

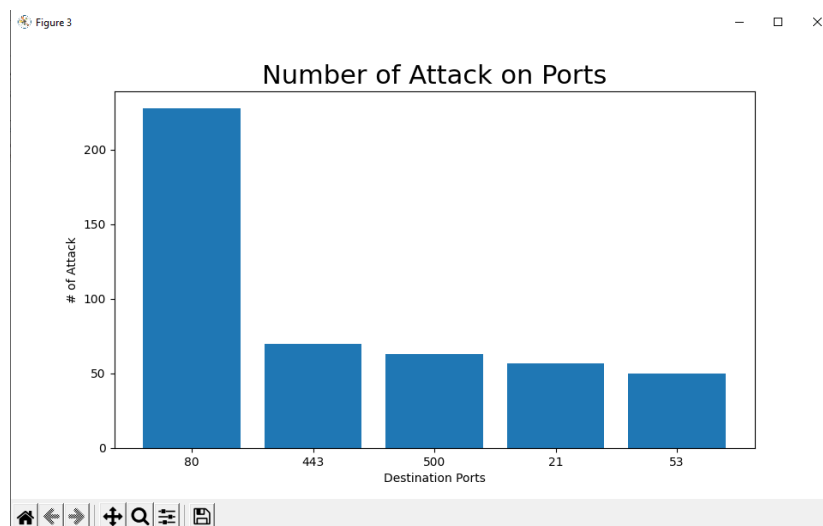
Prediction Output

Generating graphical displays

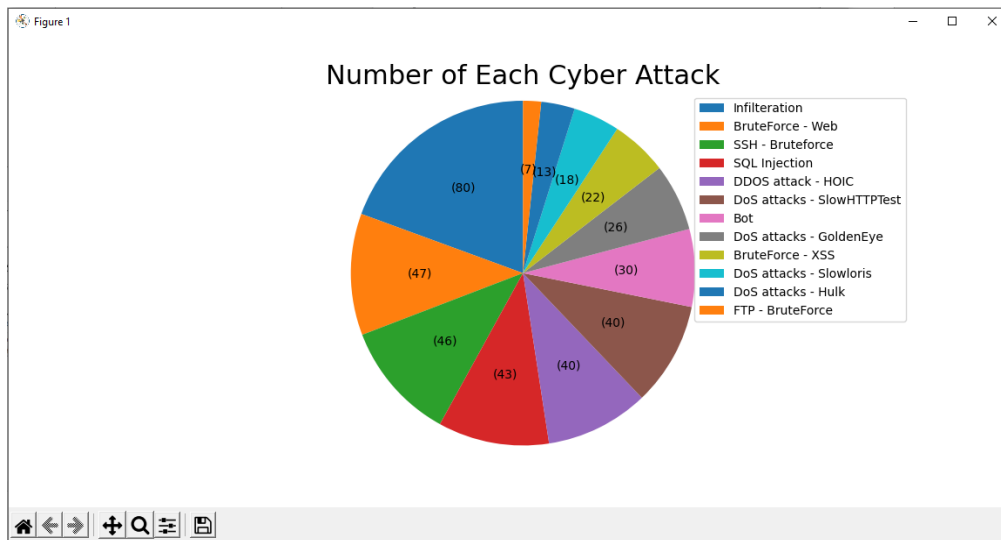
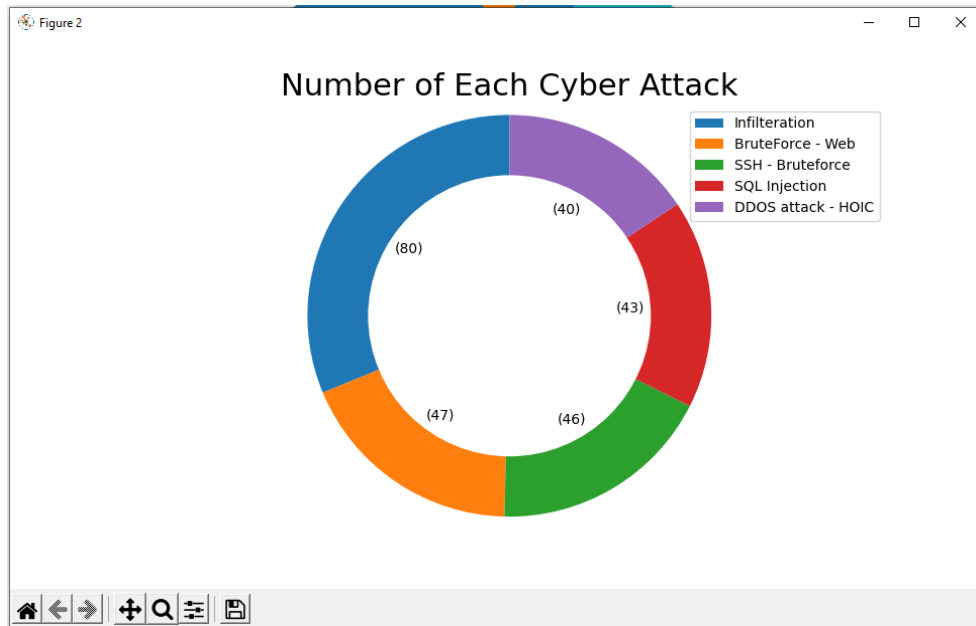
- 1) Users can click on Bar Graph, Pie Chart, and Donut



- 2) A bar graph data will be shown

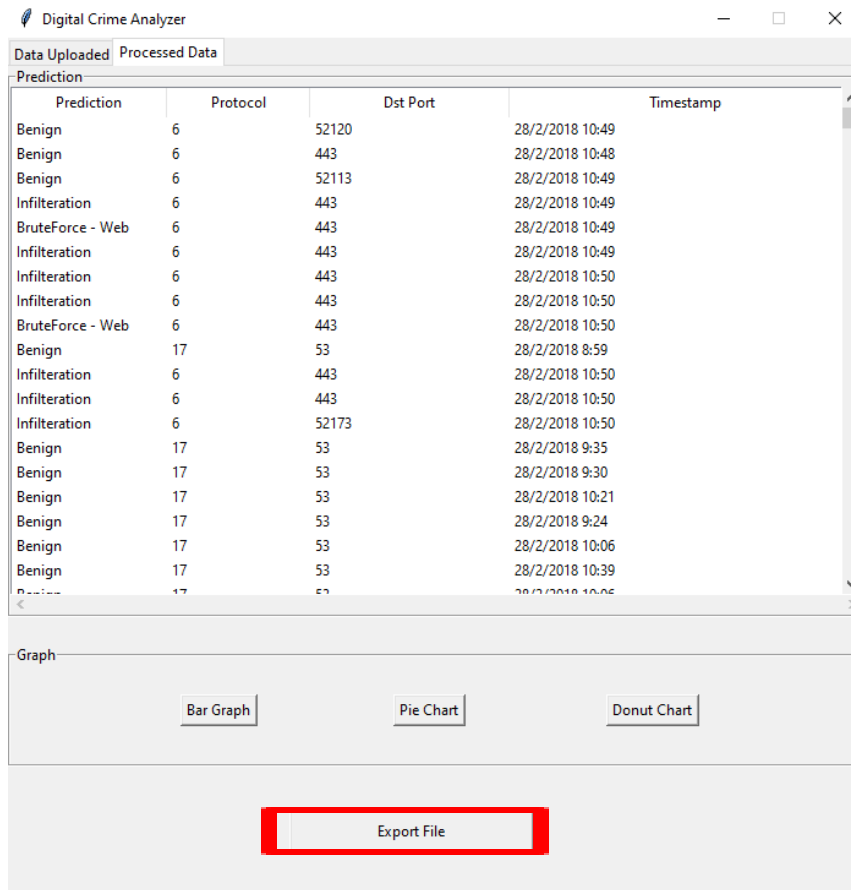


Bar Graph

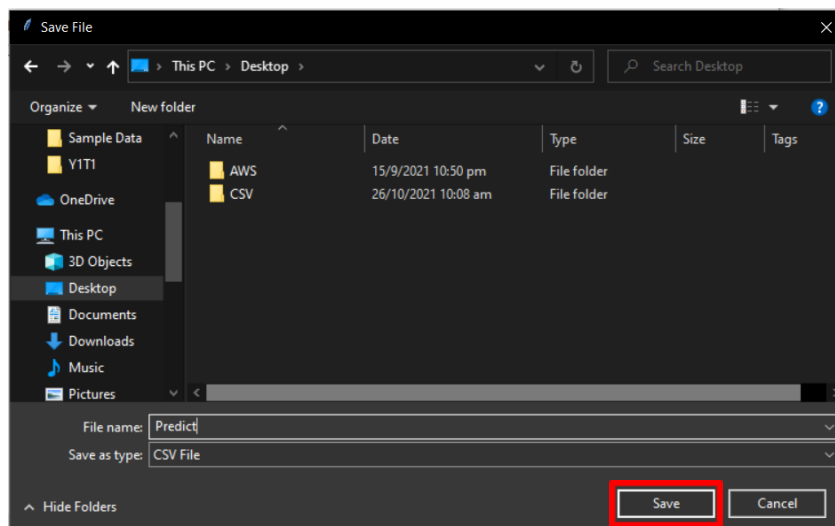


Exporting of dataset

1) From the Processed Data tab, click the “Export File” button.



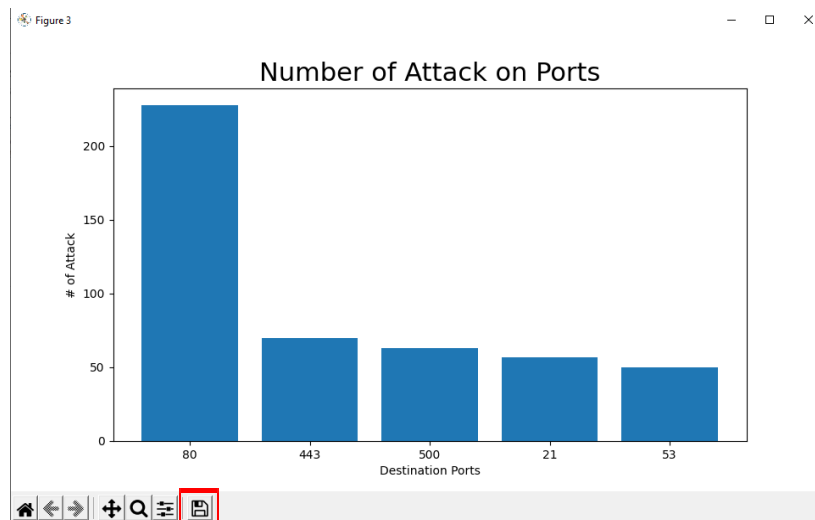
2) Input file name and save file at the desired location.



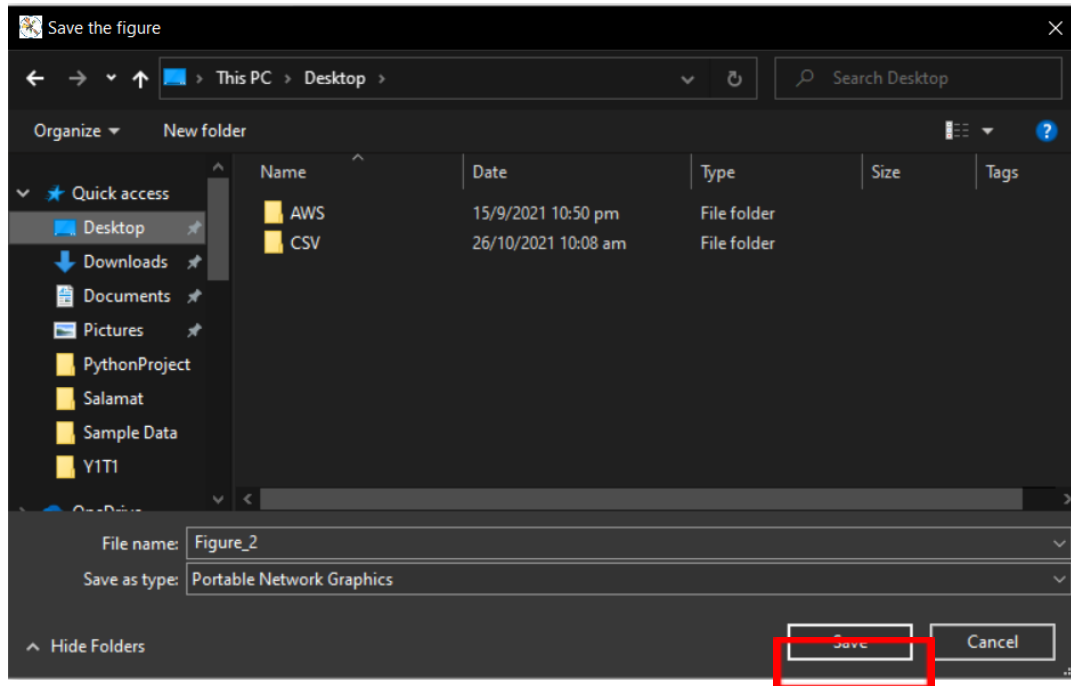
3) CSV file has been created and the data is shown below

	A	B	C	D
1	Prediction	Protocol	Dst Port	Timestamp
2				
3	Benign	6	52120	28/2/2018 10:49
4				
5	Benign	6	443	28/2/2018 10:48
6				
7	Benign	6	52113	28/2/2018 10:49
8				
9	Infiltration	6	443	28/2/2018 10:49
10				
11	BruteForce - Web	6	443	28/2/2018 10:49
12				
13	Infiltration	6	443	28/2/2018 10:49
14				
15	Infiltration	6	443	28/2/2018 10:50
16				
17	Infiltration	6	443	28/2/2018 10:50
18				
19	BruteForce - Web	6	443	28/2/2018 10:50
20				
21	Benign	17	53	28/2/2018 8:59
22				
23	Infiltration	6	443	28/2/2018 10:50
24				
25	Infiltration	6	443	28/2/2018 10:50
26				
27	Infiltration	6	52173	28/2/2018 10:50
28				
29	Benign	17	53	28/2/2018 9:35
30				
31	Benign	17	53	28/2/2018 9:30
32				
33	Benign	17	53	28/2/2018 10:21
34				
35	Benign	17	53	28/2/2018 9:24
36				
37	Benign	17	53	28/2/2018 10:06
38				
39	Benign	17	53	28/2/2018 10:39

4) The User can save the graphical displays by clicking on the save icon at the bottom



5) The user can select the location they want to save the file



6) The user can view it in their own photo viewer software

