README

The python code extracts data from network communications and identifies edges that have 'bot-like' behavior due to repeated communication at equal time intervals.
The code is : *bot_detection.py*
Read the document "*Botnet Detection Algorithm.docx.pdf*" in the folder for insights on how the algorithm works.

Change the paths of input data in the following functions:
@ get_Data(day)

- The day input can take ['a','b','c']
- Change this path to point to your input data - *'/Users/emugambi/botnet_traffic/Data/lanl_nflow_a%s'*
- See this folder for all input data files with daily connections between source and destination computers in the LANL network - *'/Users/emugambi/botnet_traffic/Data/'*

To run the code:
Call this function:
@run_detection_methods(which_day)

- *Which_day* : select from this list - ['a','b','c']
- Change the path to where you want the results saved
- Results are the edges that show high repetivity and have bot-like behavior

@ edge_traffic_dist(which_day,src,dst)

- Inputs are : [day,source_computer,destination_computer]
- Output is a plot of distribution of time intervals between connections.