Lab 3 Exercise

Bonus points for submission:

Submission of this lab exercise is not required.
Successful submissions before 6:00 PM ET on Monday, 10/1/2018 will be graded with up to 10 bonus points towards your final course grade.

NO bonus points for late submission.

Submission format: .ipynb

Note that, the total number of points of this final course is 100. The bonus points does not add points to the total number of points possible, i.e., the total points is still 100, not 110. So it is designed to give credit to students who complete the lab exercise without negatively affecting the Final Grades of students who do not complete the lab exercise.

Example #1:
If you get total 100 points from all homework assignments, quizzes, and final project, winning the 10 bonus points will not affect your final grade. Your final course grade is still 100 points, not 110 points.

Example #2:
If you get 85 points from all homework assignments, quizzes, and final project, winning 10 bonus points will increase your final grade from 85 points to 95 points.

Data Set:

The same data set (traffic_dump.pcap) we used in our last class. Please download it from Blackboard.

Task 1: Query function - 2 points

Write a function, given an ip address, output information of all TCP streams that involve this ip address, including stream's starting time, ending time, the other ip address, and stream's size in bytes

Task 2: Plot the query results - 2 points

Use your function from task 1, get all streams of a given ip address (e.g., 192.168.1.64). Then Generate a time series plot of stream size over the starting time.

Task 3: Restore the content of streams - 2 points

Use the tool tcpflow (http://www.forensicswiki.org/wiki/Tcpflow) to save all stream content to external files. Submit the list of files generated by your tcpflow command.

Task 4: Explore and analyze the dataset - 4 points

This is an open ended question, intended for you to explore the dataset and implement any kind of analysis and/or visualization on the dataset. Answers to this task will be assessed with considerations of analysis logic/reasoning and creativity.

For example, you could use the pcap data to do some analysis on HTTP traffic, e.g., find out how much HTTP resources are successfully fetched along the time. To do so, you can leverage the packet payload data from the pcap. Standard response for successful HTTP requests carry a status code “200 OK”. This status code can be used to filter out the successful HTTP requests.