Assignment 1

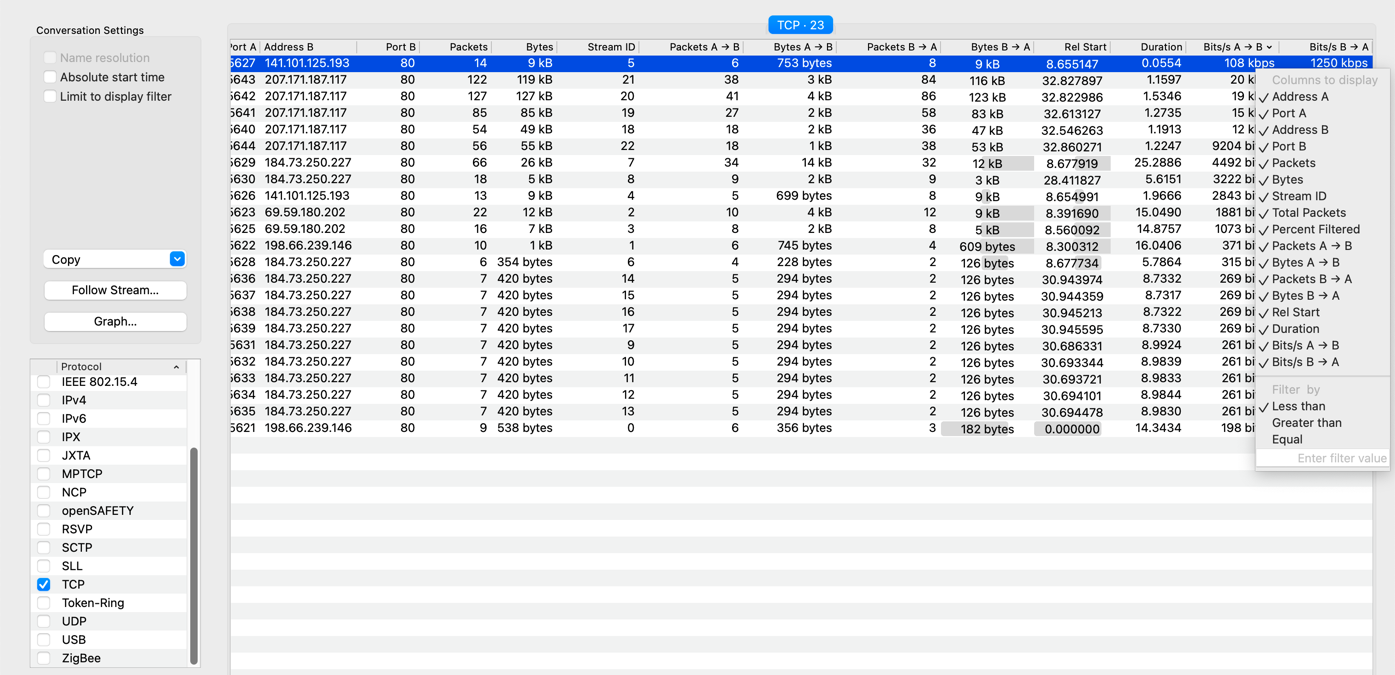
Wireshark Fundamentals

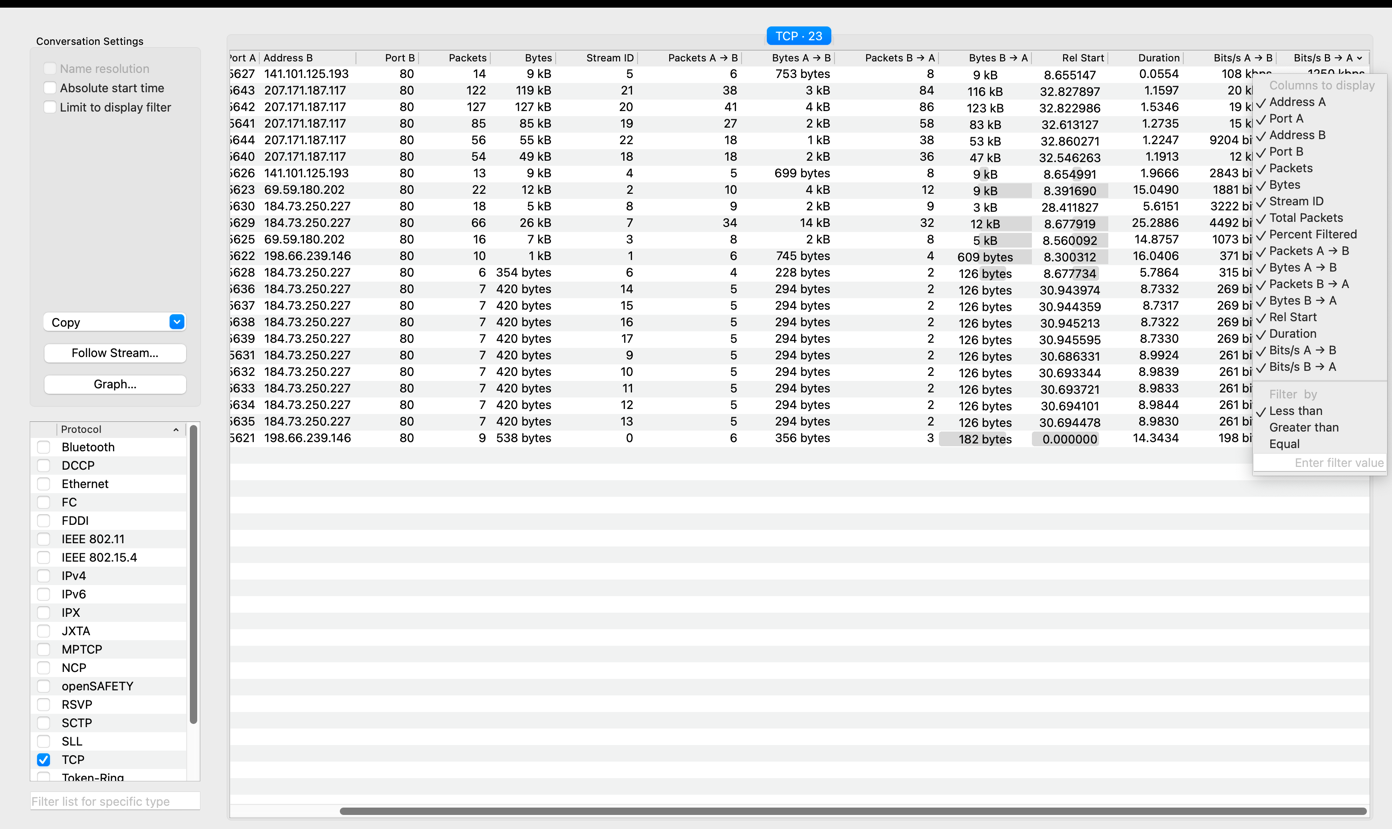
By Ziming Song

[zs2815@nyu.edu](mailto:zs2815@nyu.edu)

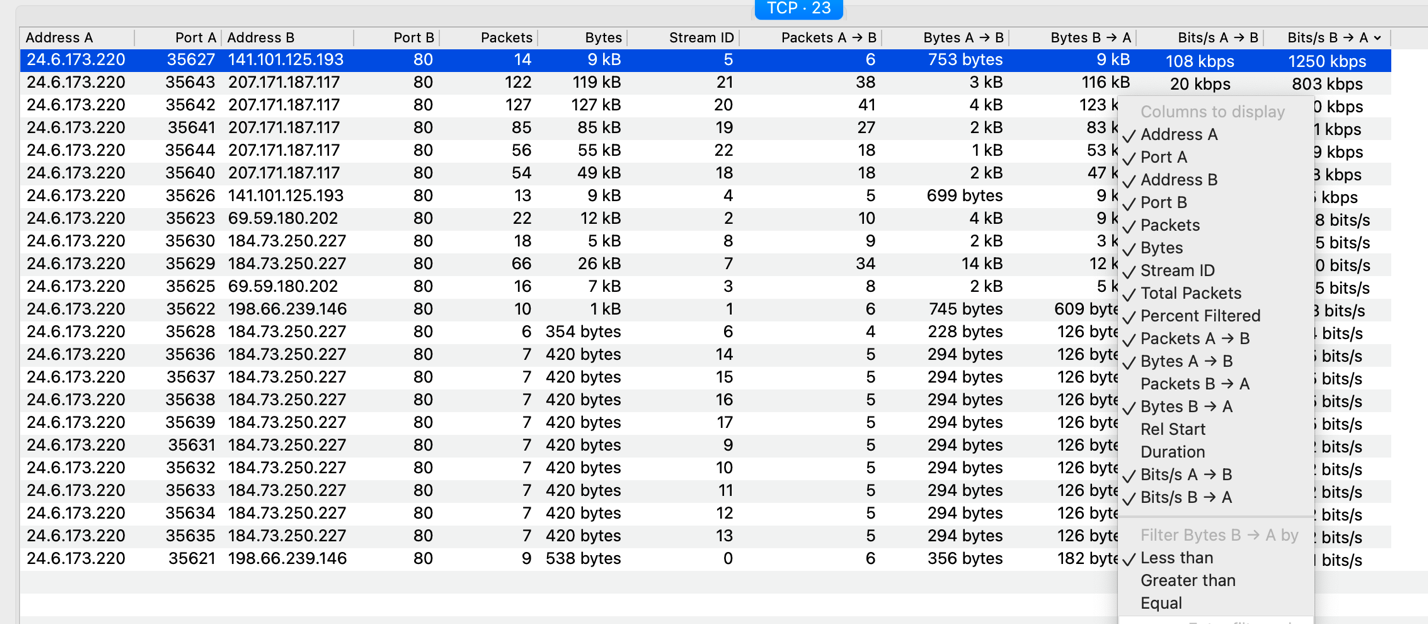
# **Part 1: tr-chappellu.pcapng**

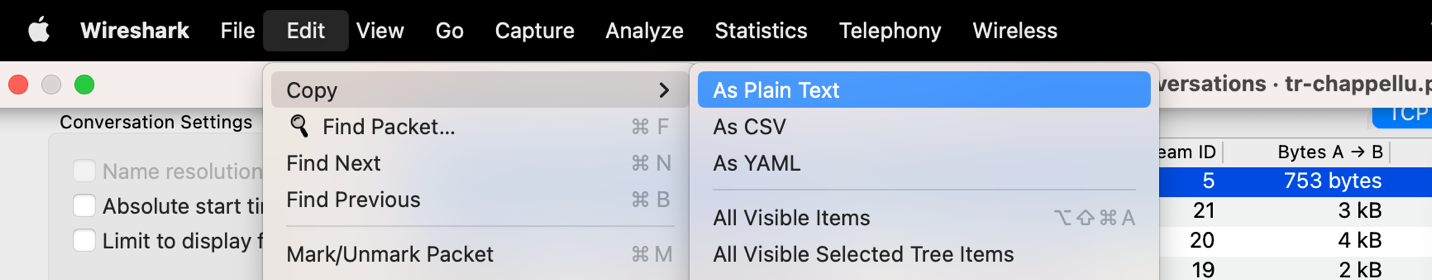
## **Find the most active TCP conversation in the file (by bits per second)**

The most active TCP conversation is the first one marked as blue. The bits/s from A to B at 108kbps and the bits/s from B to A at 1250kbps.The filter method is marked with red boxes.



## **What is the total amount of bytes transferred from A to B and from B to A in the most active TCP conversation? (Hint: right-click on the conversation, select Apply as Filter > Selected > A → B. Save the packets once the filter is applied)**

*753* bytes transferred from A to B. 9000 bytes transferred from B to A. The filter method is marked with red boxes. The result is marked with yellow boxes.

****

## **Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP**

## **Handshake.**

# **Reference**

1. Wireshark User’s Guide: Version 3.5.1