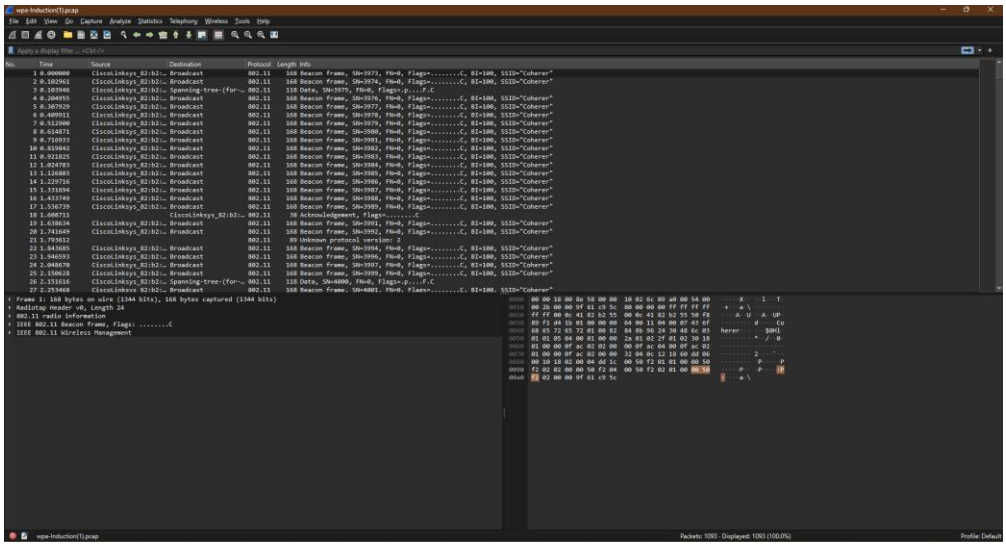
Lab 6 – Traffic Analysis using Wireshark

Joshua Ludolf
CSCI 4406_60L – Computer Networks Lab

Opening “lab6_wpa-Induction” in Wireshark

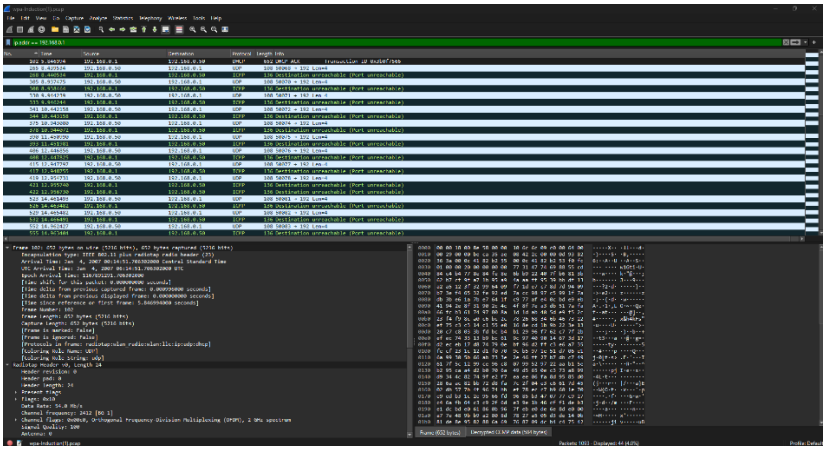
- Observations/issues: None. File downloaded and opened in Wireshark without any issues.



Filtering traffic using display filters

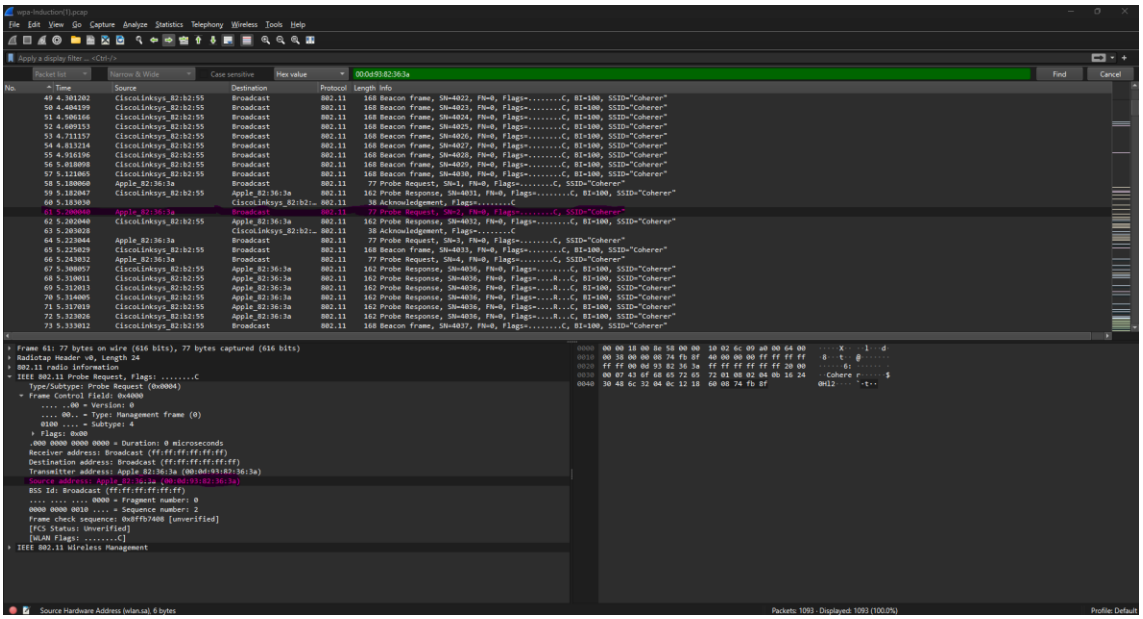
Applying display filter to filter by IP address – I filtered using ip.addr == 192.168.0.1

- Reusing instructions from lab 2, I was able to filter for the IP address 192.168.0.1 without any issues.



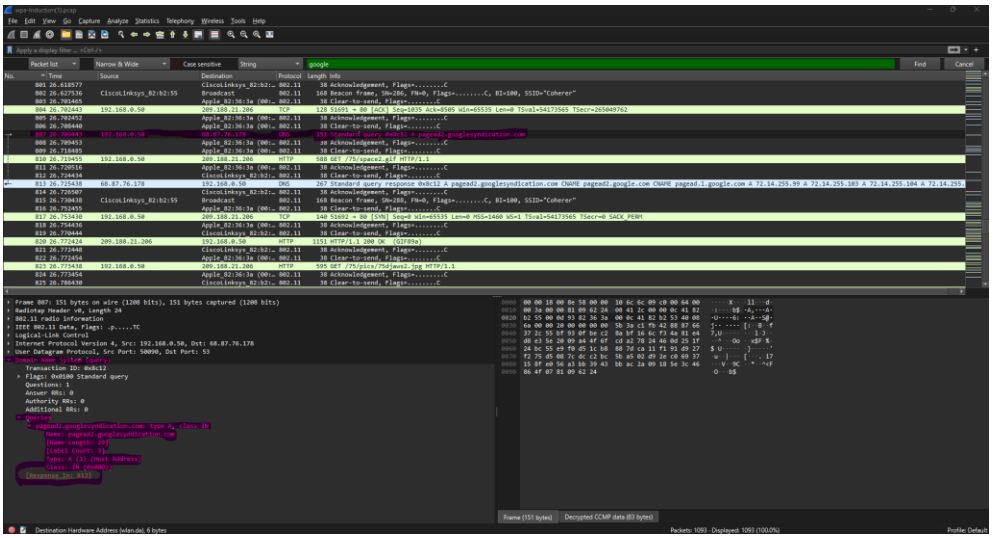
Applying display filter to filter by Hex value – I filtered using 00:0d:93:82:36:3a

- Filtering by Hex value wasn't as simple as filtering by IP address. I eventually found it in the edit menu bar, the find packet option allows additional search options to select from. I noticed that when filtering by packet you must continuously click the "Find" button to see the next applicable result instead of all the applicable results displaying after applying the filter. After that I checked the Source address as shown (everything highlighted in the pink).



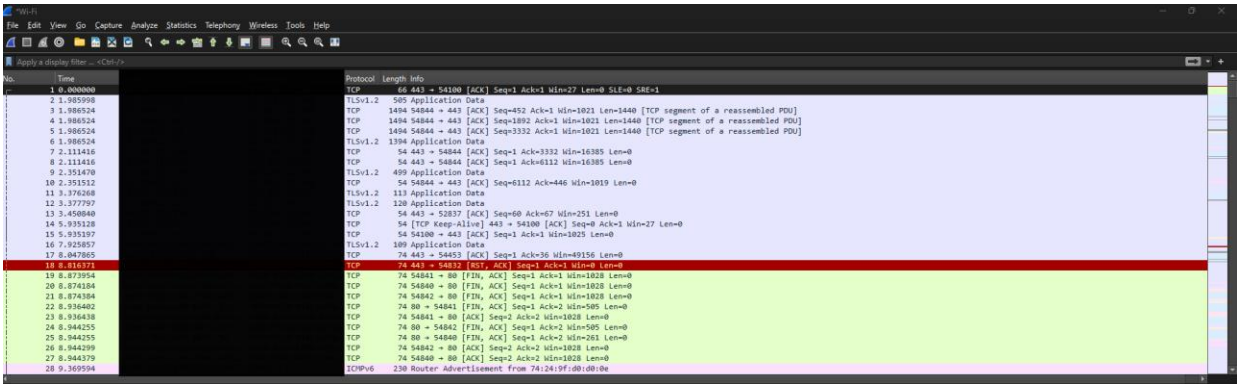
Applying display filter to filter by String – I filtered using google

- Filtering using google string was like filtering by hex code, I used the same Find packet function but changed the Hex Code value option to String. That was the only real diference from Hex Code filtering.



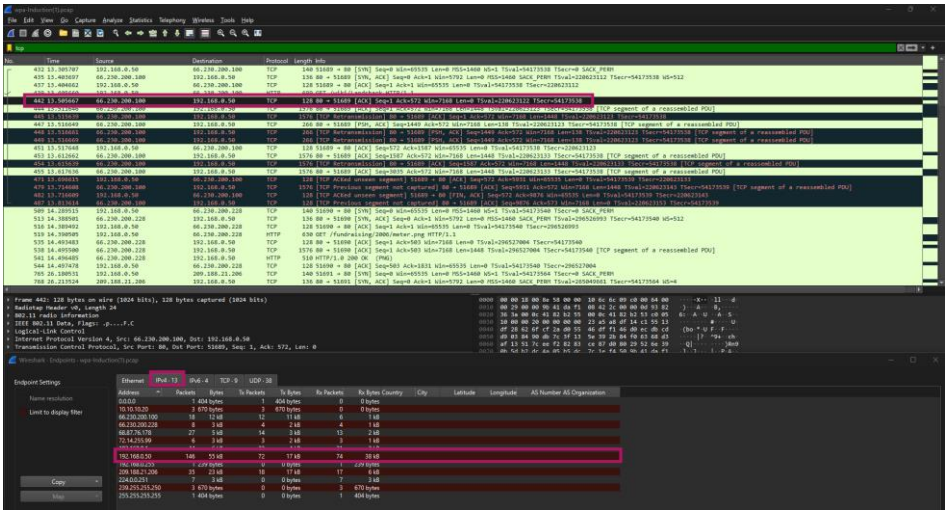
- I read through the section “How to use capture filters” which I thought was something we were supposed to do with the pcap file provided but researched some more and realized that those are the filters you apply when you want to capture traffic which in turn would become your pcap file. I applied a capture filter and ran it on my home network just to see what I captured (pictured below). I was bombarded with a message pop up asking me if I wanted to run this is admin mode, I clicked yes and it kept asking, but eventually I clicked no several times and Wireshark started to behave. After that I selected wifi in the home (file selection option after closing previous .pngcap file)

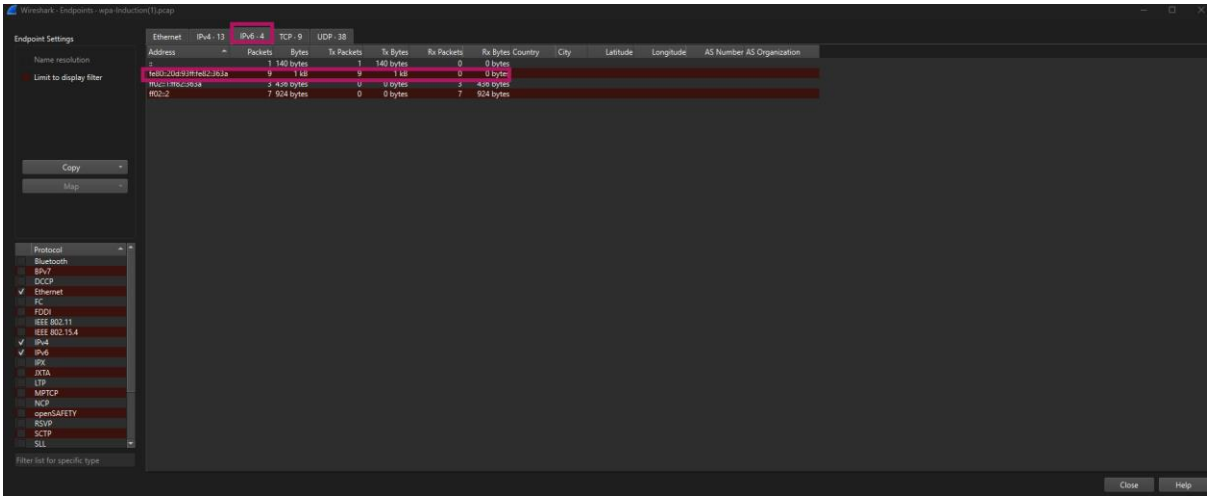
Using capture filters and capturing traffic on my home network via Wireshark



Analyzing Endpoints

- I selected package #442 and noticed that under the IPv4 tab end point 192.168.0.50 had the most traffic at 146 packets and traffic under for IPv6 was subpar to IPv4 traffic (most intensive endpoint was at 9 packets).

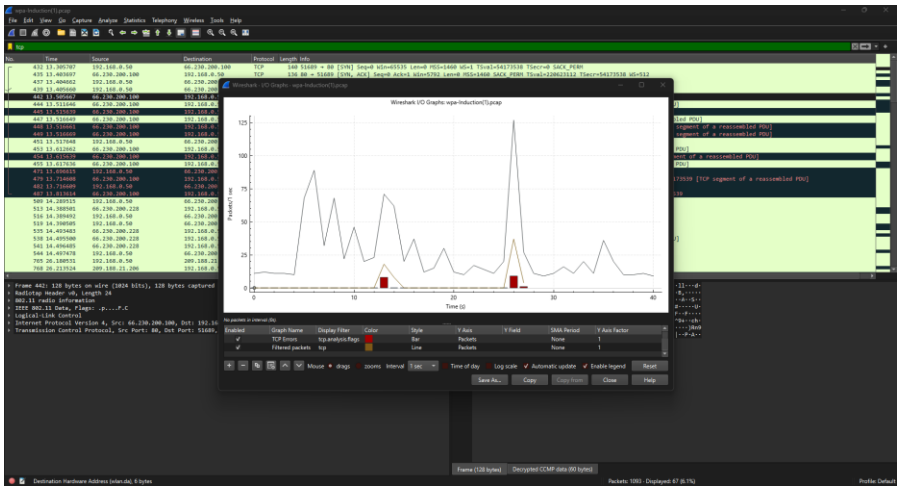




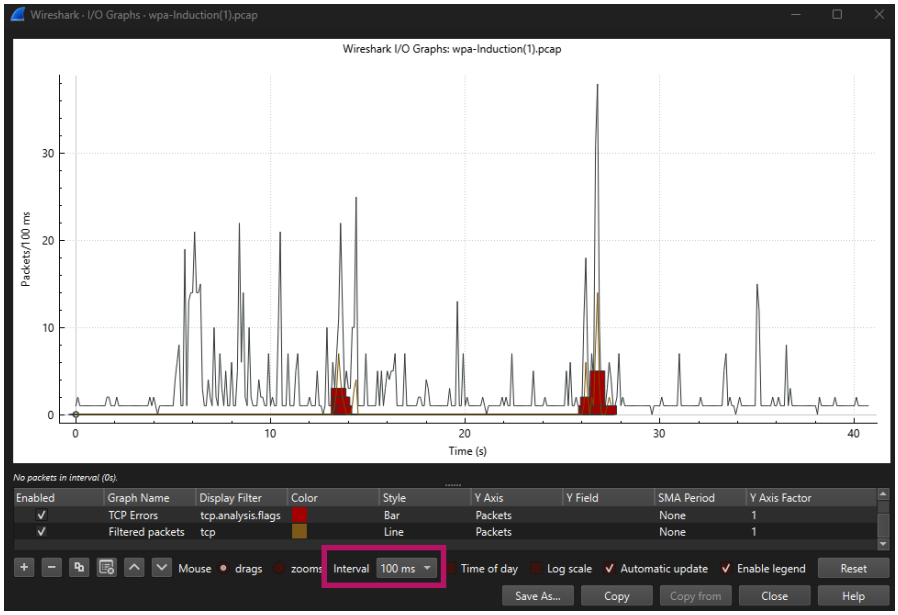
Analyzing Graphs for Traffic

IO Graphs

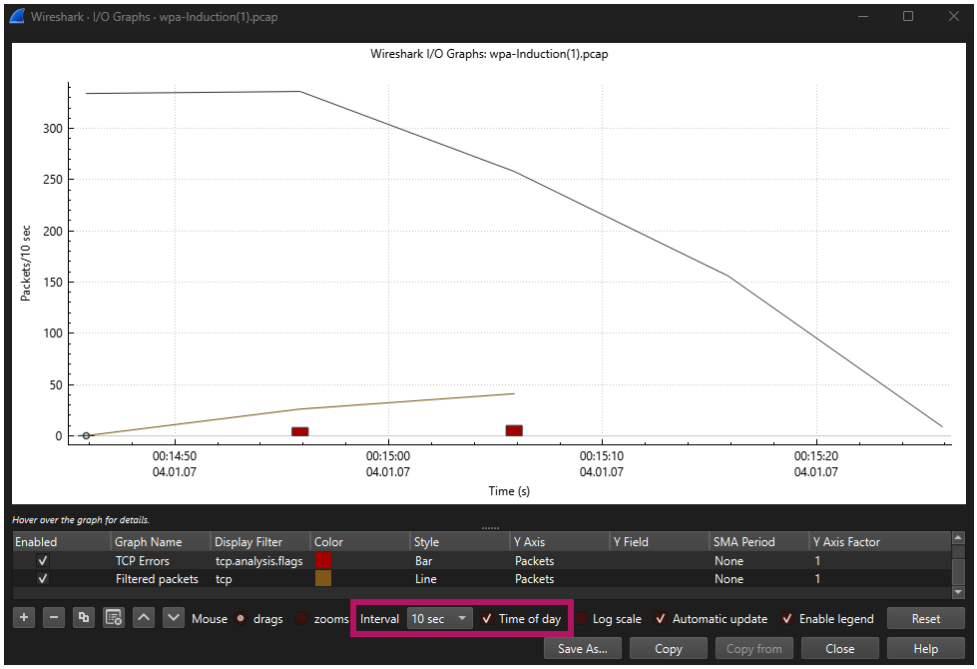
- No issues. I went to statistics in menu bar and selected IO graphs. I played around with the IO graph and applied different filters – screen shots below. The options are pretty cool and I can see the benefits of having the ability to filter. I noticed in the Interval filter that the graph for all units smaller than 100ms were hard to read and understand. I'm sure there's a good use case for these graphs and I'm just not aware of it but it was quite difficult to understand the graph and made me just not want to look at it.
    - No Filter:



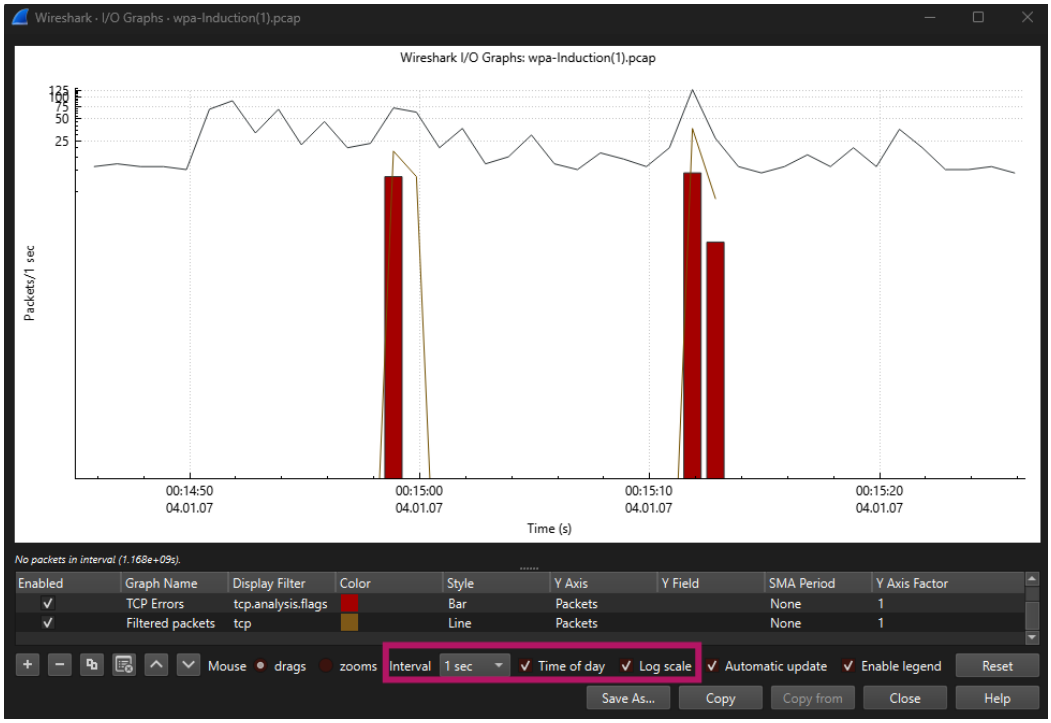
- Filter - time interval 100 ms:



- Filter - time interval 10 seconds and Time of day:

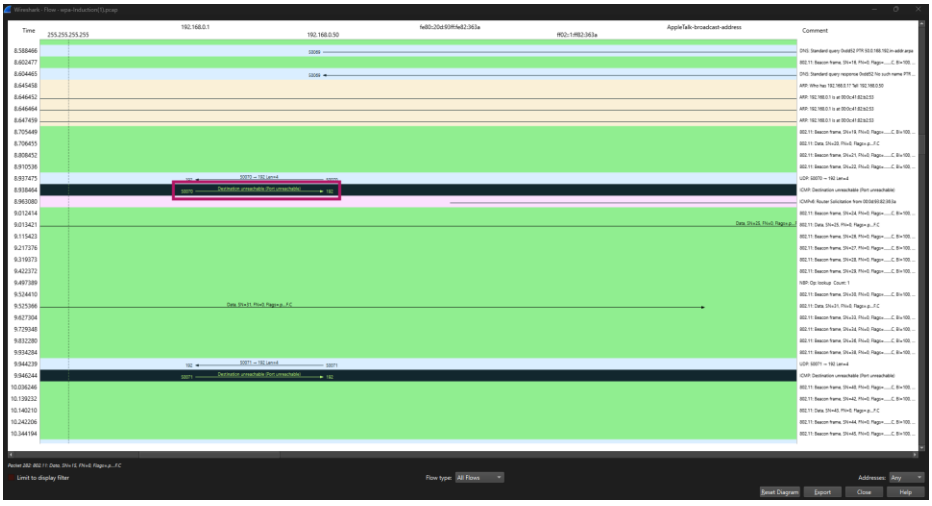


- Filter - time interval 1 second, Time of day, and Log Scale:



Flow Graphs

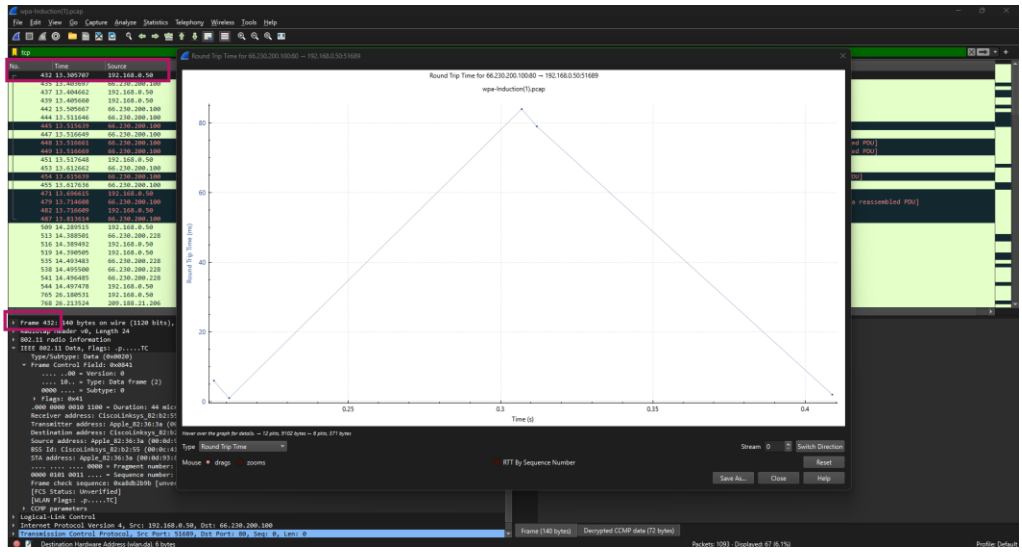
- I think my favorite chart in this lab is this one. When a connection drops or slows down, I always wonder why it happens, especially if it's a dubiously portrayed website. As I moved through the graph, I came across a black bar that said, "Destination unreachable (Port unreachable)," at 8.440534 seconds. If I could alter this graph, I would enlarge the remark area or make it a field that expands at the bottom when a line item is clicked. Though I was unable to read the entire comment or figure out how to enlarge that data.



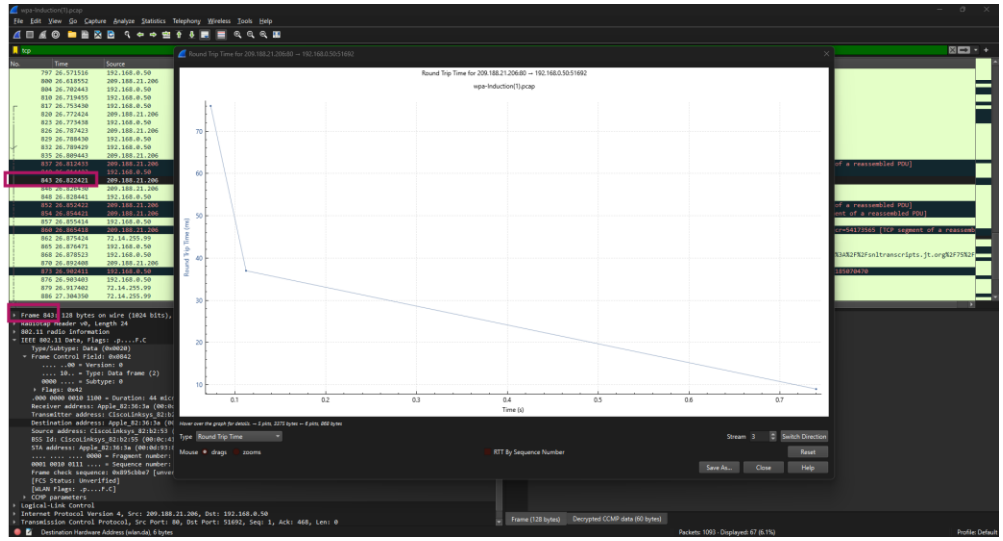
TCP Stream Graphs

Round-trip time graphs

- I filtered the results by TCP and selected the first TCP packet (# 432) to see what the traffic looked like as it started up, see graphs below. This graph looks like what I expected it would look like with a high peak point.

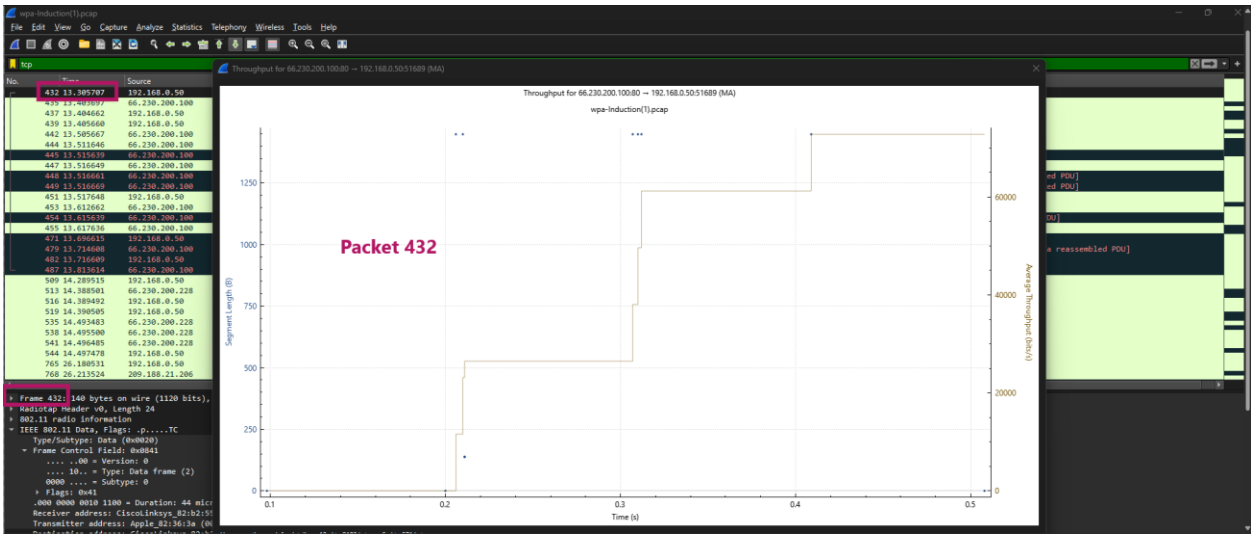


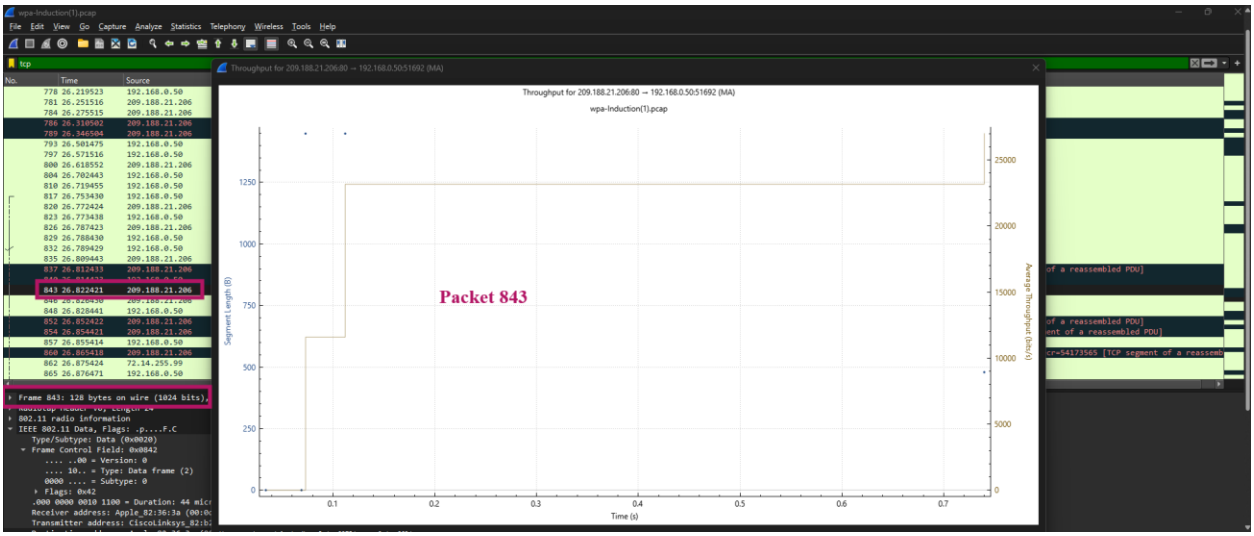
- I also selected a secondary packet (# 843) to see if there was any difference in the graphs and there was. For this packet it looks like the traffic is already coming to an end so the graph is making it's way back down to 0.



Throughput Graphs

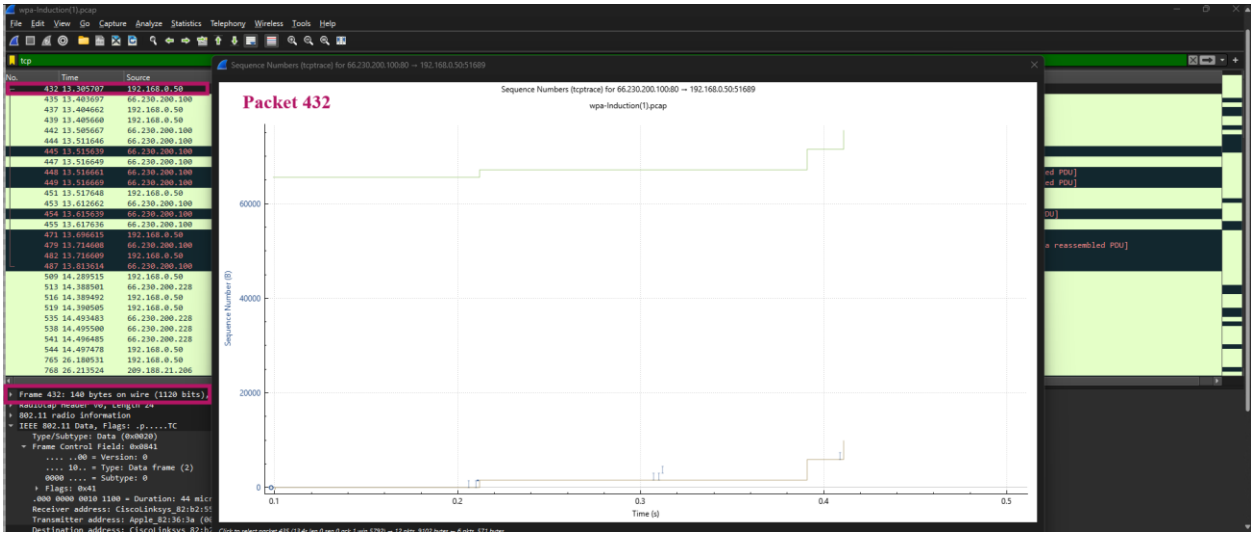
- I again selected two packets to compare, packet # 432 and packet # 843, images below. My graphs didn't quite look like the examples in the guide provided and I played around with the filter options available in the Throughput graph but still wasn't able to get it to look much like the throughput graph example in the guide. I figured that it may just be because the pcap being used is not the same. What I did notice in the graphs is that while packet 432 seems to be climbing up packet 843 ends up reaching a point where it just flattens out and peaks again at the end.

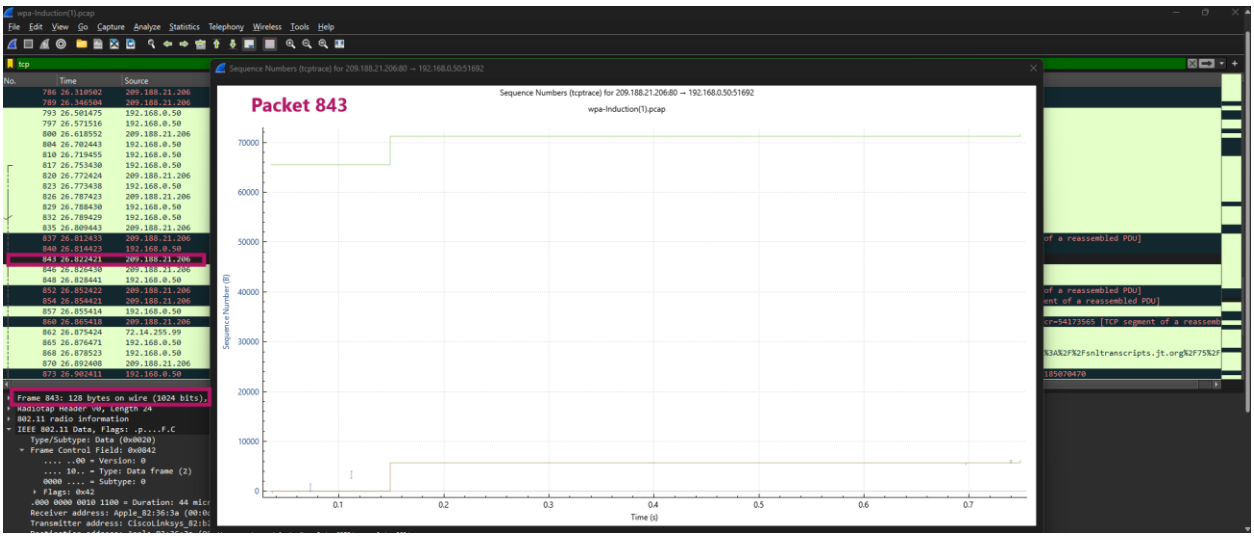




Time Sequence Graphs (tcptrace)

- I again selected two packets to compare, packet # 432 and packet # 843, images below. Results were sort of like results of throughput graph (previous images) where in the graph for packet 432 seems to be climbing up, but this time at a much smaller magnitude, and packet 843 ends up reaching a point where it just flattens out.





Summary:

I have seen how to work with endpoints to analyze traffic and to visually represent the endpoints, depending on the data I am working with. Additionally, I have seen the different types of graphs that can be used to analyze traffic and their application areas. Furthermore, I also learned about how to apply Hex code and String filtering to find certain packets.