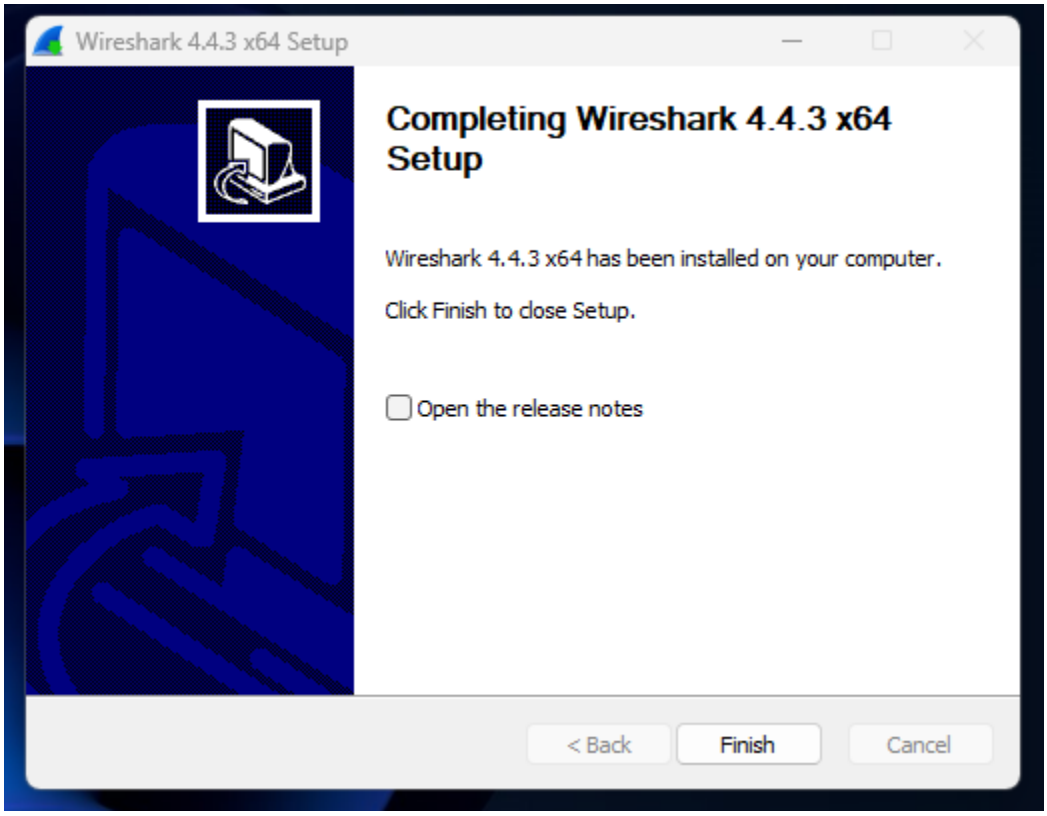
# Lab 1 - IoT Network Analysis

CS 466
2/2/2025

Patrick Hurley

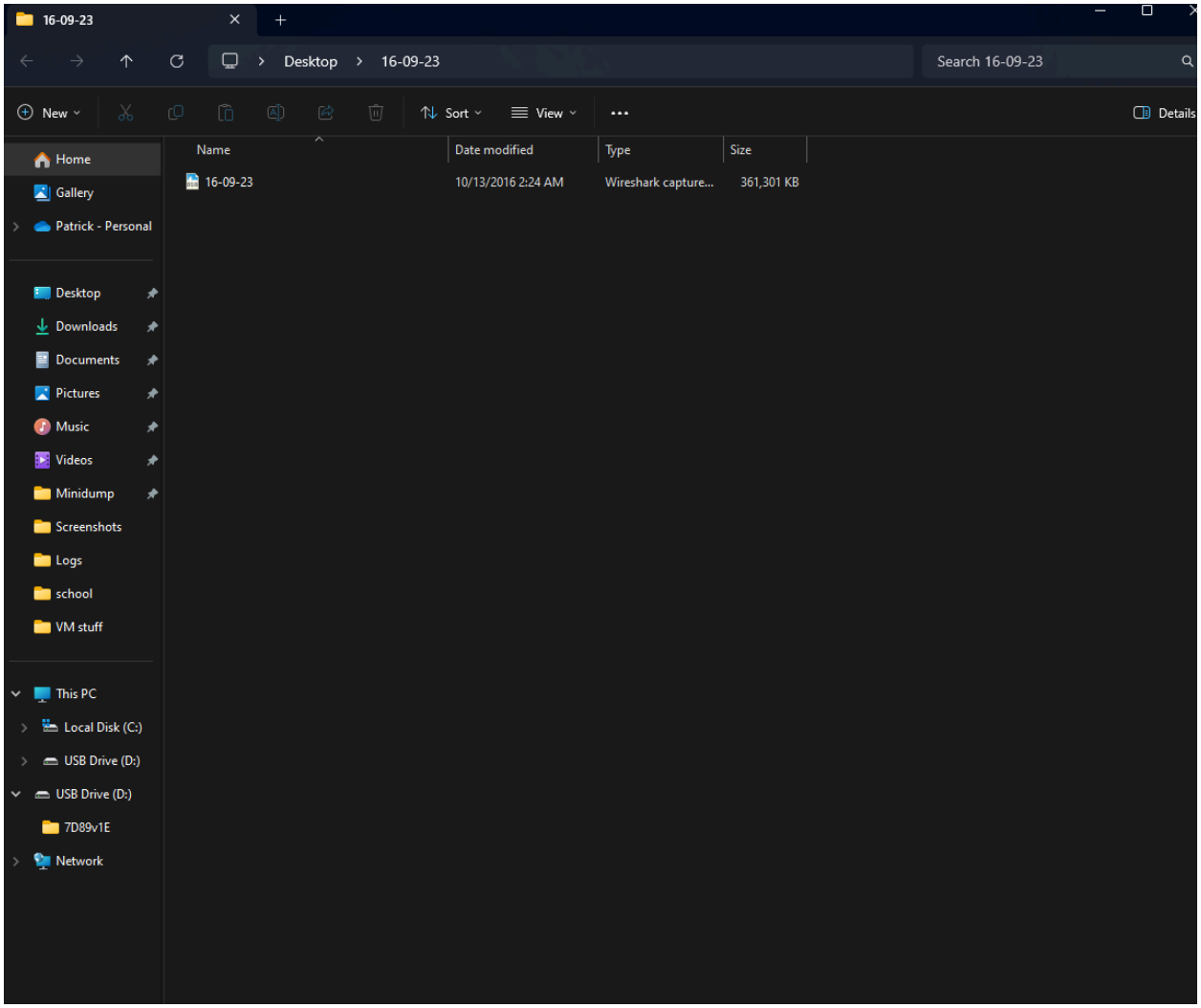
**Part #1**

Here I have downloaded and installed Wireshark.



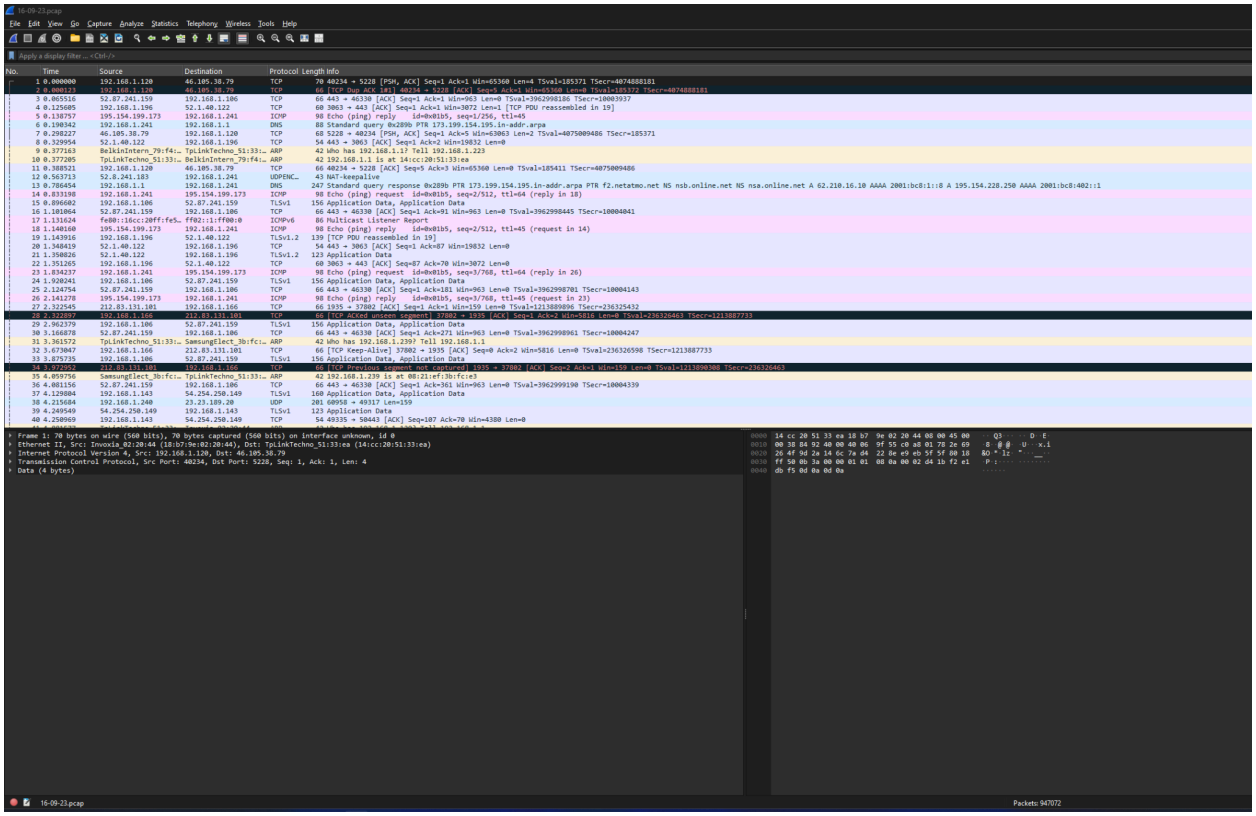

**Part #2**

Here is a screenshot of the extracted contents of the downloaded pcap file.



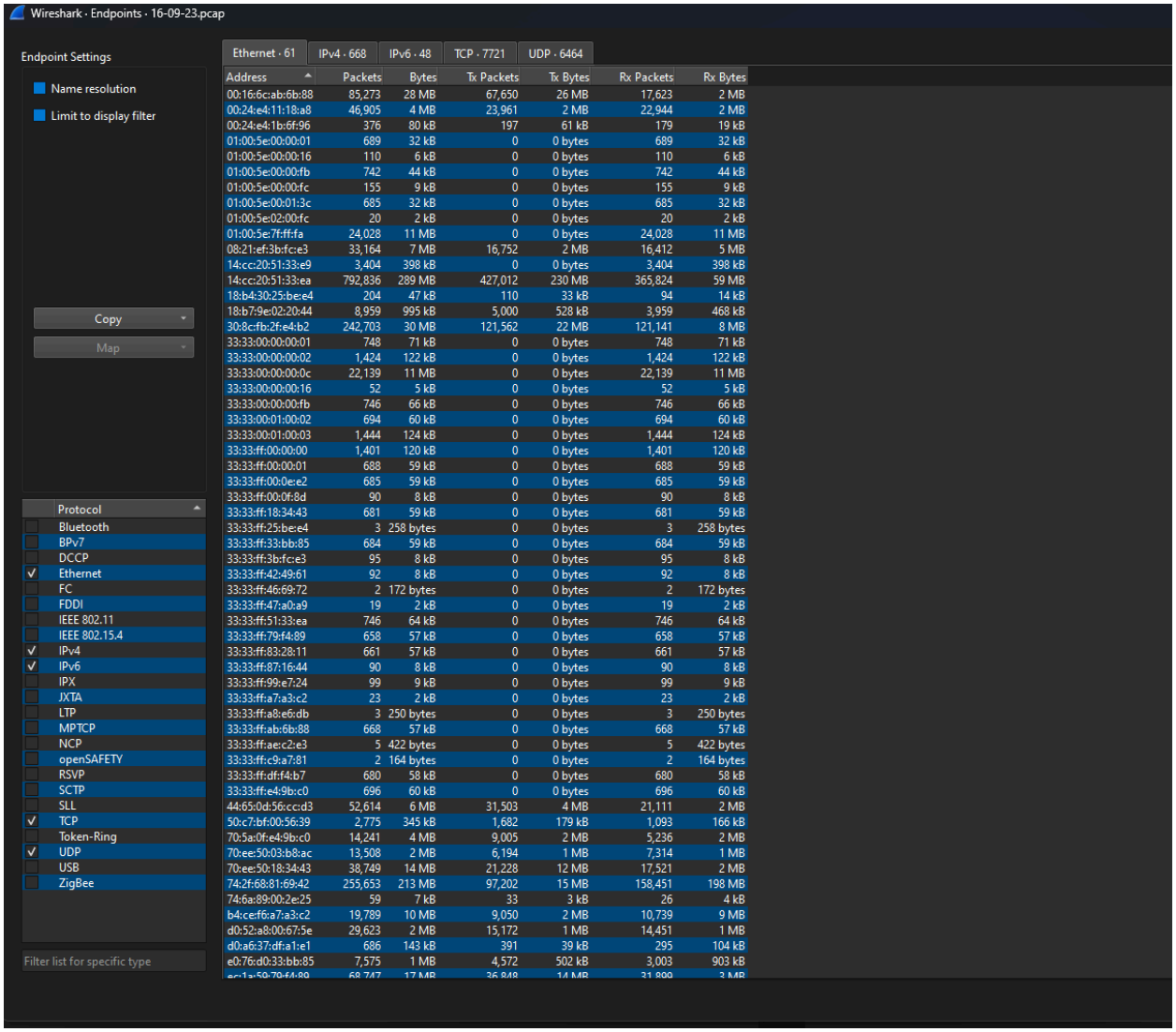

**Part #3**

This screenshot shows the pcap file had ben opened in Wireshark.



**Part #4**

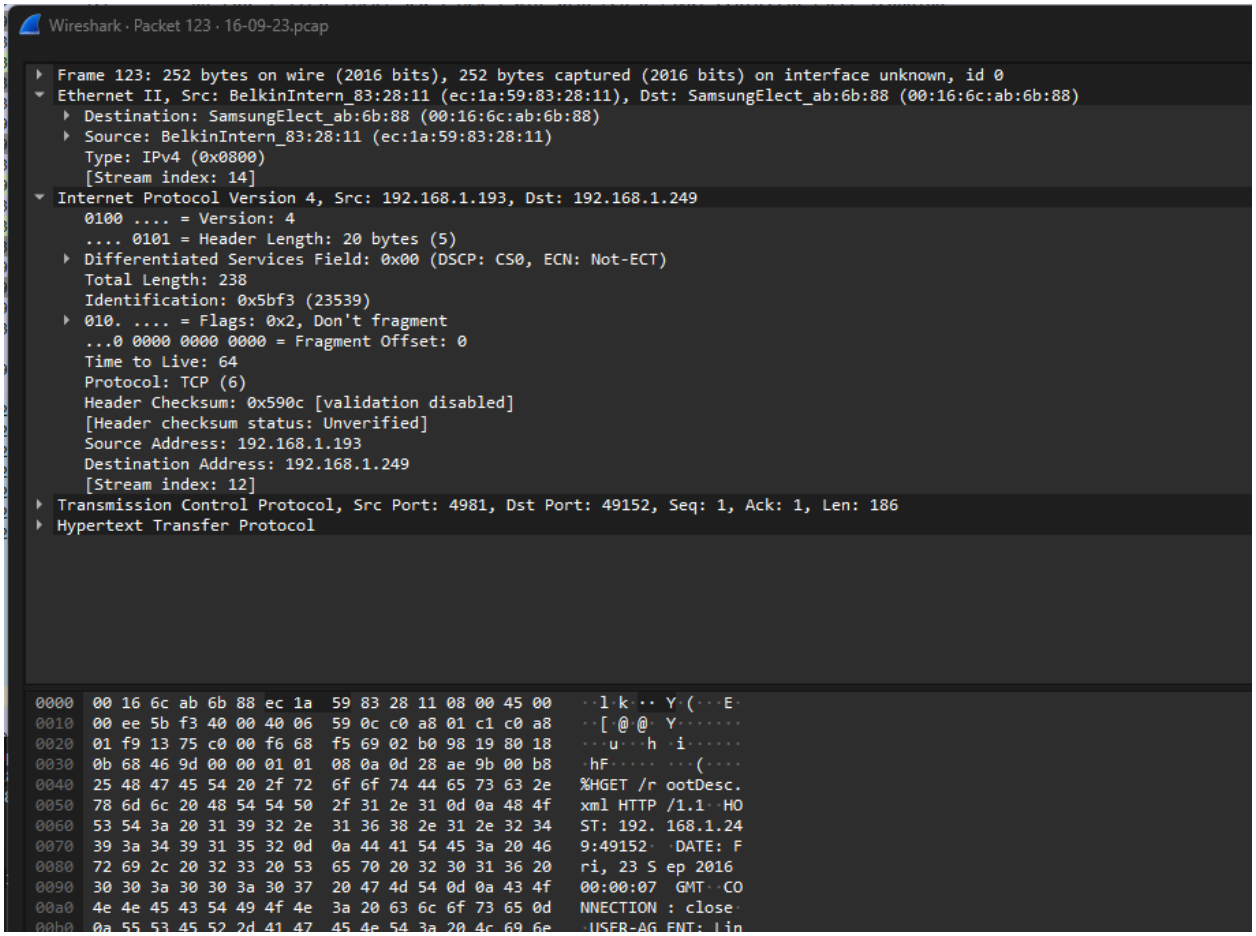
Below is a screenshot of the list of mac addresses in the endpoints tab.
The first two MAC addresses listed below belong to the Samsung Smart Cam (00:16:6c:ab:6b:88) and the Withings Smart Baby Monitor (00:24:e4:11:18:a8).



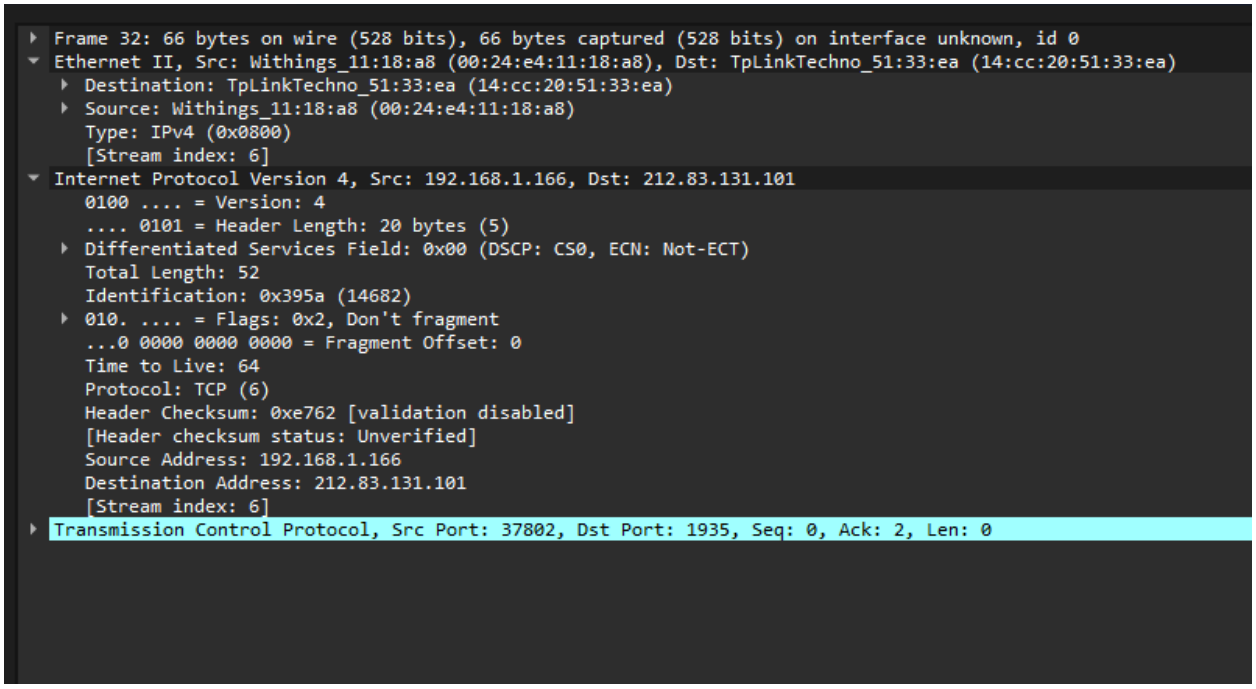

**Part #5**

I will continue using the two MAC addresses from the previous question, the Samsung Smart Cam (00:16:6c:ab:6b:88) and the Withings Smart Baby Monitor (00:24:e4:11:18:a8).

The first screenshot below shows that the Samsum Smart Cam is the destination. Through this, we can figure out the destination IP address, which is **192.168.1.249.**

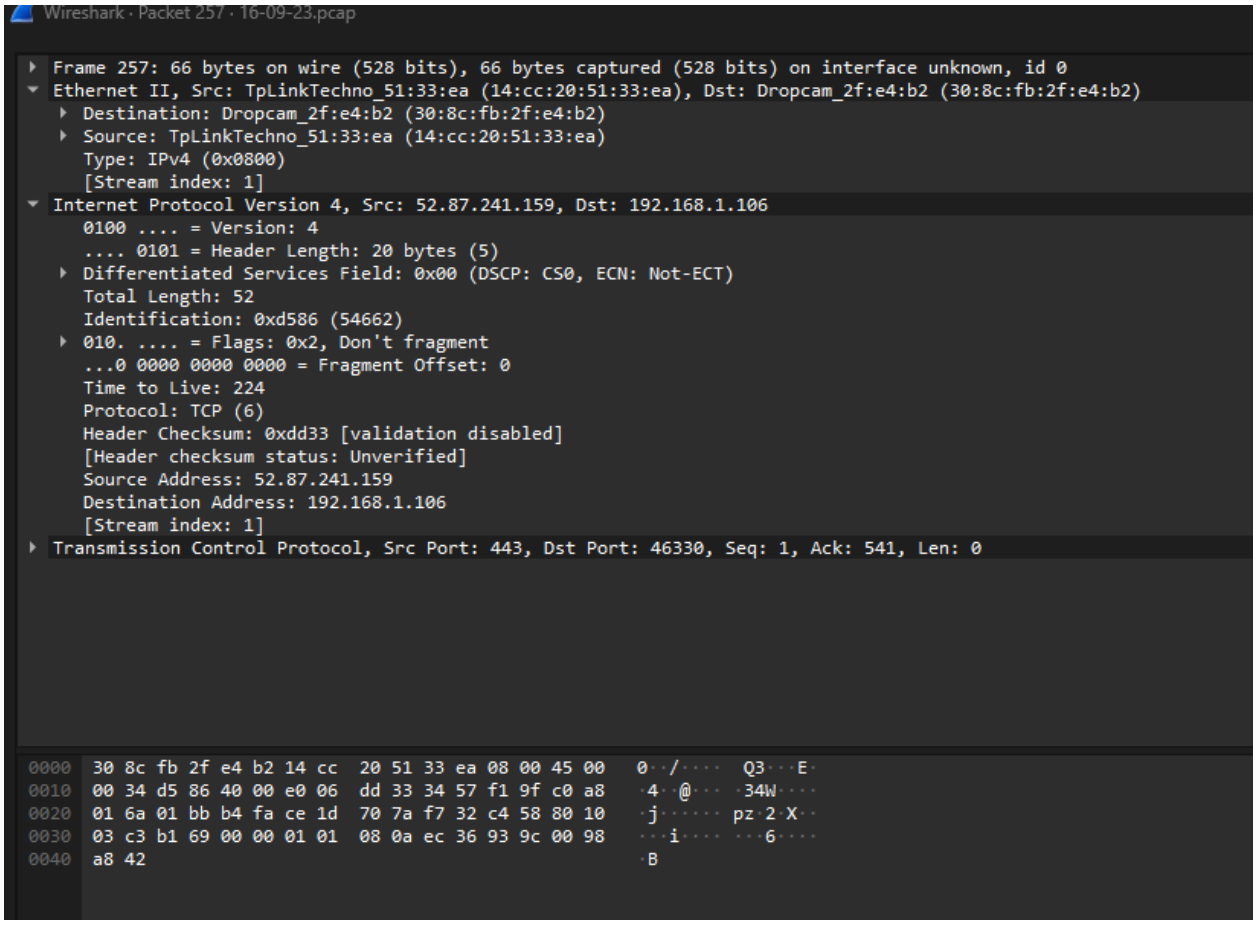



The second screenshot below shows that the Withings Smart Baby Monitor is the source this time. The source Ip address for the baby monitor is **192.168.1.166.**



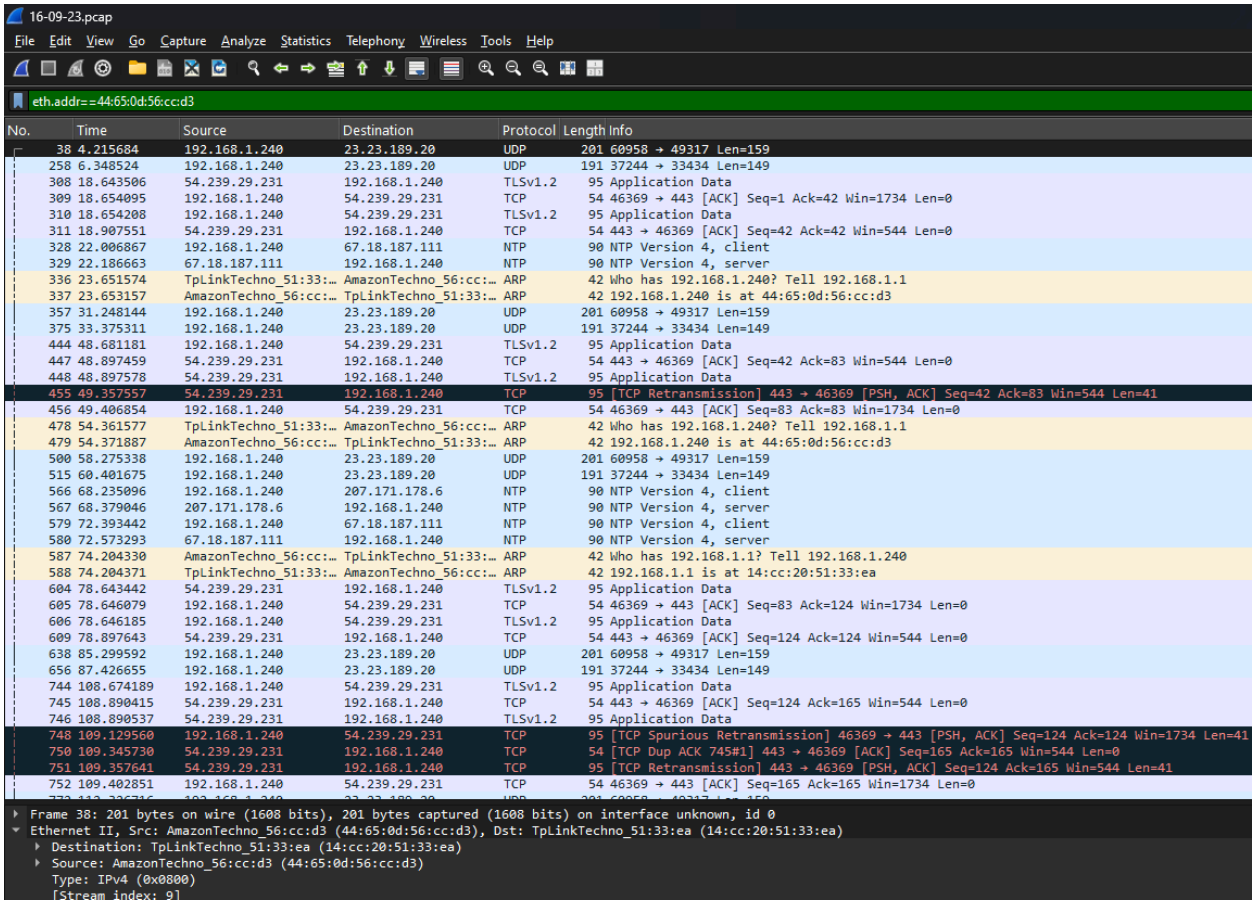

**Part #6**

In the screenshot below, I used the given MAC address for the router to search for it on Wireshark. From this screenshot I can see that the router is the source, because of this I can then use that to see that the IP address of the router is **52.87.241.159**

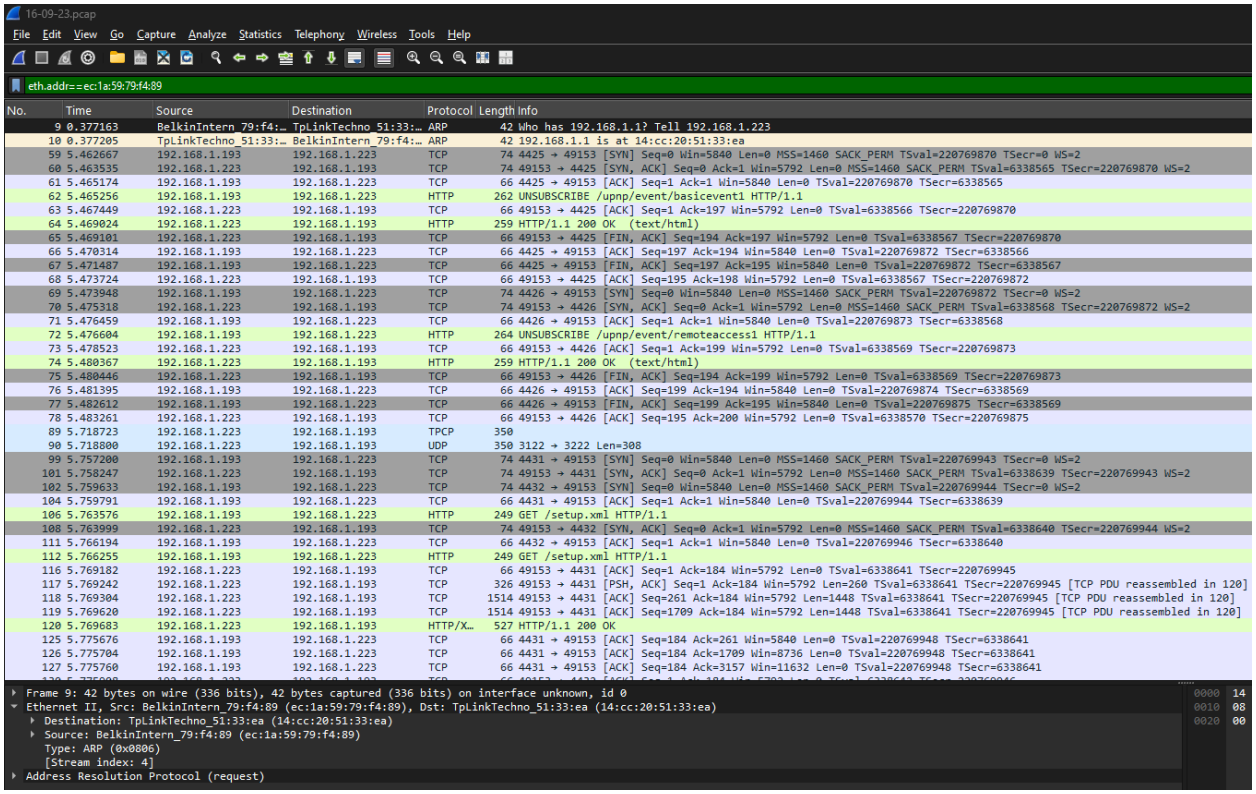



**Part #7**

The first IOS device I searched for was the Amazon Echo by using its MAC address, and I was able to see many different protocols it used. Below is a screen showing protocols like **UDP, TCP, and NTP.**




The second IOT device I chose was the Belkin Wemo switch. The screenshot below shows multiple protocols including **ARP, TCP, HTTP, and UDP**.

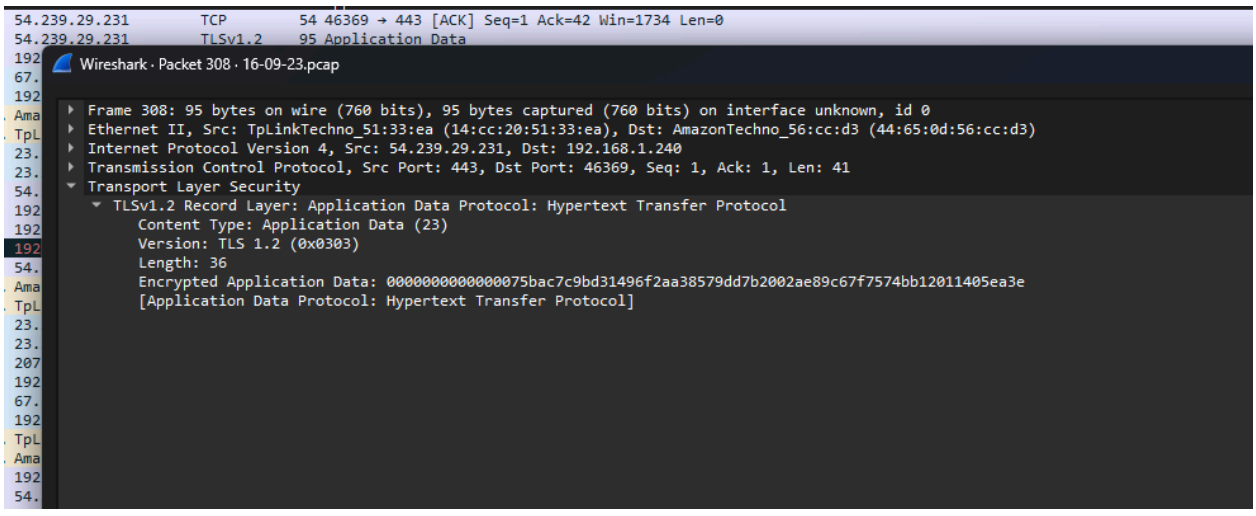



**Part #8**

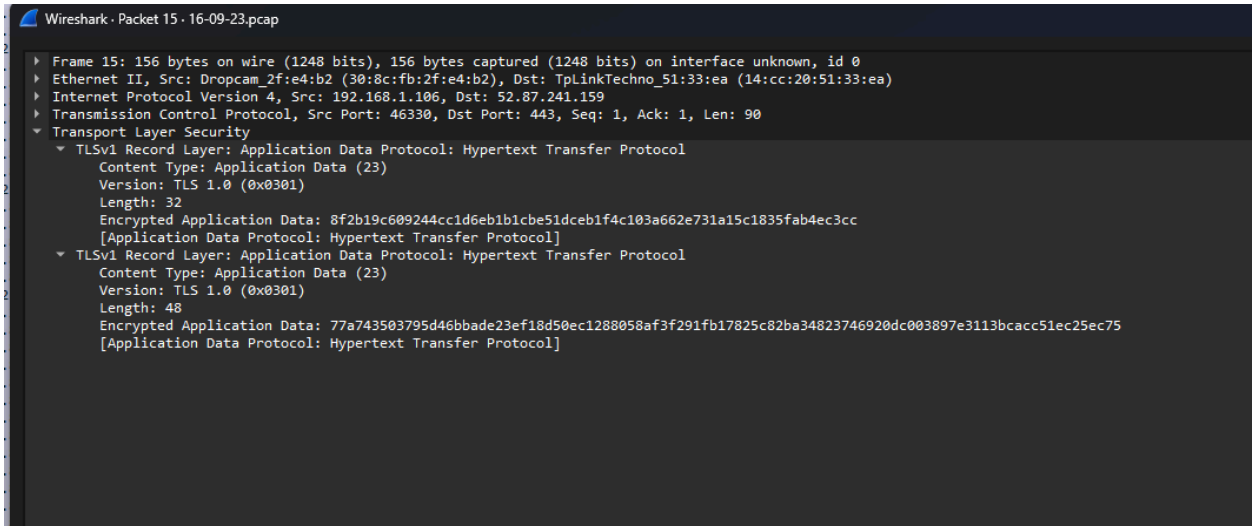
Elephant flow is talking about the flow of very large amounts of packets. Mice flow is talking about smaller amounts of packets being sent

**Part #9**

The first IoT device I chose was the Amazon Echo. The screenshot below shows that the Amazon Echo has **Transport Layer Security version 1.2.**

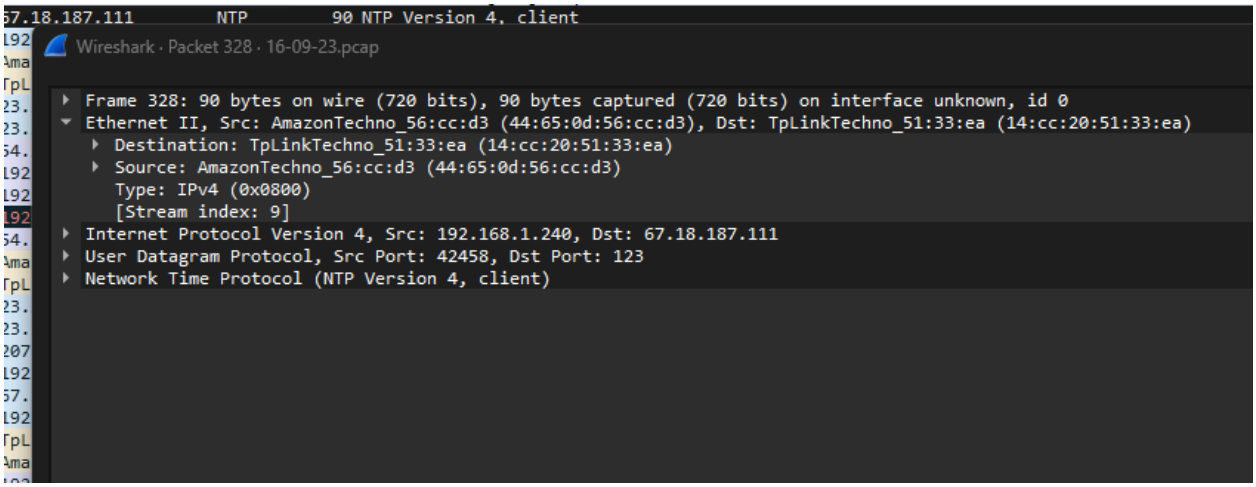



The second IOT device i chose was the DropCam. The screenshot below shows that the DropCam has **TLS version 1.**

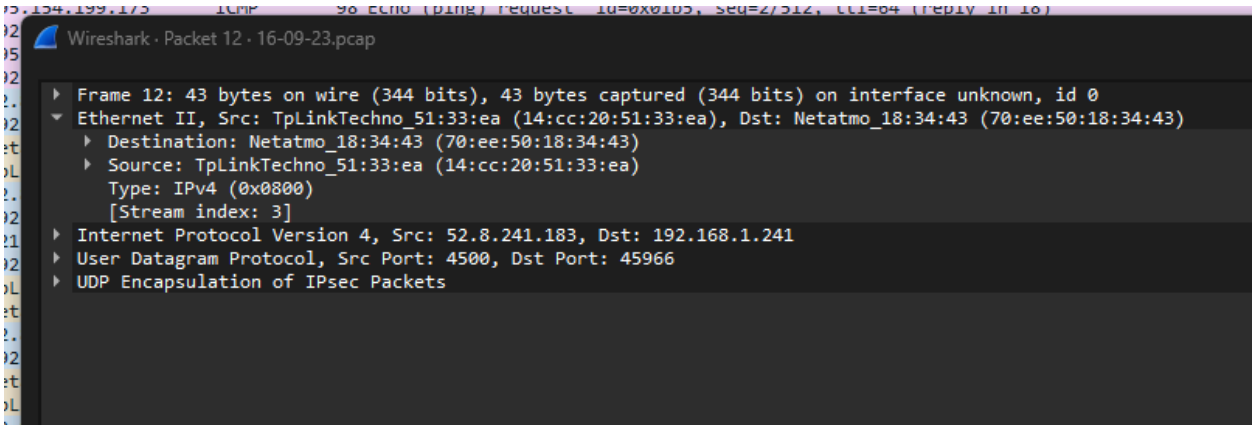



**Part #10**

Below is a screenshot that shows the Amazon Echo device is communicating with an external IP address of **67.18.187.111**, because if it was communicating with internal addresses it would start with 192.168.xxx.xxx

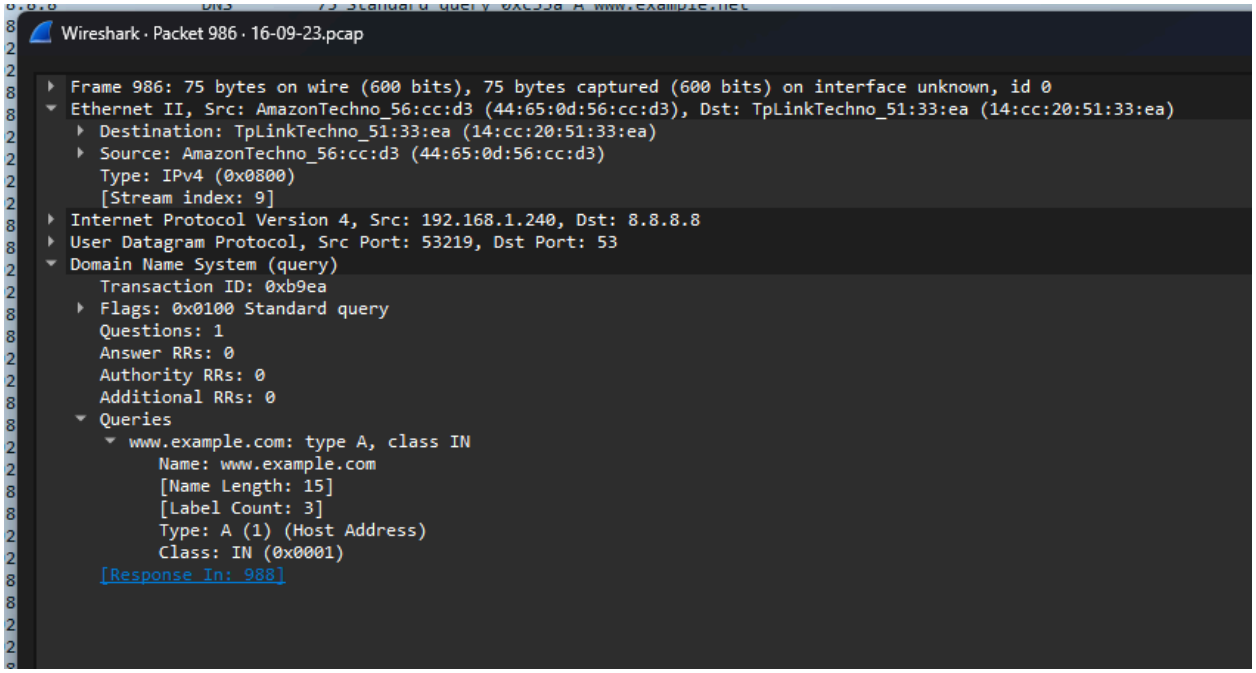



The Below screenshot is of the Netatmo Welcome. The Netatmo is receiving information from an external IP address **52.8.241.183.**



**Part #11**

In the below screenshot, I am showing that the Amazon Echo is capable of sending out DNS packets. In this specific packet, the Amazon Echo is searching for the domain name **www.example.com**




In the below screenshot, the Netatmo Weather Station is trying to search for the domain name **netcom.netatmo.com.**