Challenge 2: Homework Network Analysis

After looking at bad traffic at work all day, you start to wonder what's going on on your home network.

- Run a capture on your homework network on any device. Leave the capture running in the background for 2+ hours. Be sure to use the device some while it is running!

- Stop the capture.

- Identify at least 2 instances of suspicious, interesting, and/or unfamiliar protocols/communication.

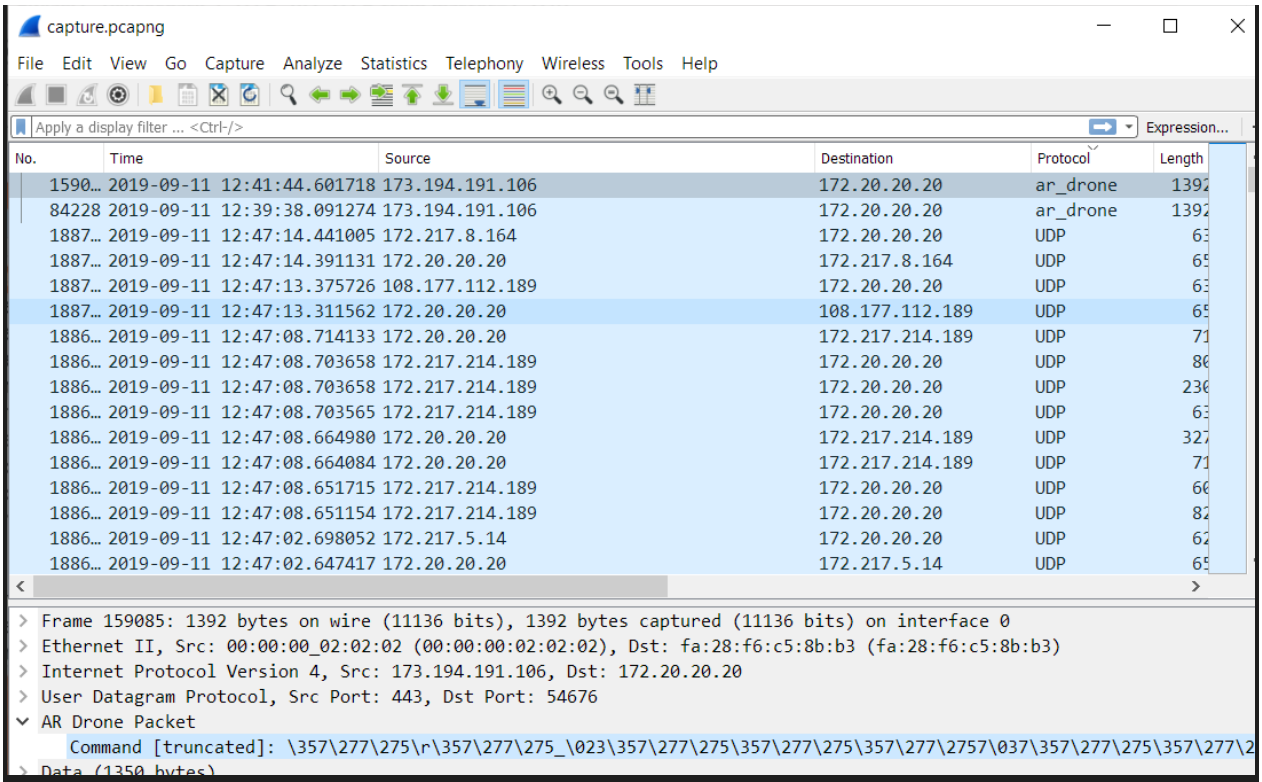
- To complete this challenge, you'll submit a document named `Home-Analysis` in your **Challenge-2** folder. It should include:

  - A 2-3 paragraph write-up for each of the communication examples (4-6 paragraphs total).

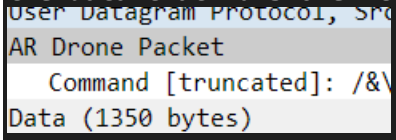
  - Images and screenshots to communicate how you found the communication, and how you investigated it.

  - An explanation of any unfamiliar protocols and how they work, if relevant.

  - A description of the purpose and outcome of that communication.



This ar_drone protocol is unfamiliar to me. After doing some research, this protocol is the AR Drone Packet. It's a UDP packet from port 5556. It captures the data that runs over the network between the network and client.



Noticing these commands were truncated, I looked up the bug and it is named "Bugzilla-daemon". Basically, in contrast to other descriptor types, configuration descriptors have varying lengths and may be quite long. This makes them much more prone to truncation by a host that is cautious about reading large descriptors.