shark on wire 2

Problem

> We found this packet capture. Recover the flag that was pilfered from the network. You can also find the file in /problems/shark-on-wire-2_0_3e92bfbdb2f6d0e25b8d019453fdbf07.

- Packet Capture

Solution

1. Open the ".pcap" file in wireshark.
2. Since the previous challenge involved following the UDP stream, that is the first step we should take to solve this. Go to `Analyze -> Follow -> UDP Stream` and click through the streams.
3. One stream has a message labeled start and the following streams are all strings of various lengths that contain the character "a".
4. Looking in the info column, we can see that the requests all come from different ports from the same IP.
5. Filter the IP: `ip.src == 10.0.0.66`
6. We can see that the second message originates from source port 5112. 112 is a number which should alert us, since its ASCII representation is `p`, which matches the flag template.
7. Run the script.py to grab all the port numbers and convert them to ASCII, which is the flag.

Flag

`picoCTF{p1LLf3r3d_data_v1a_st3g0}`