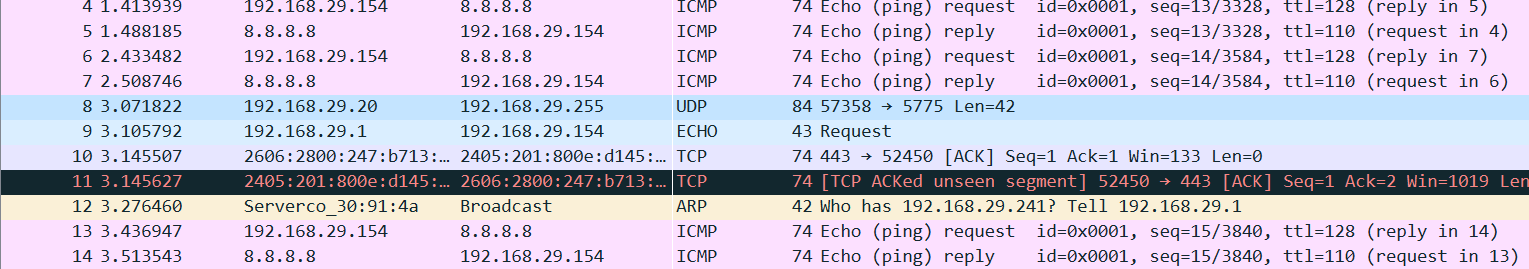
**1. Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a**

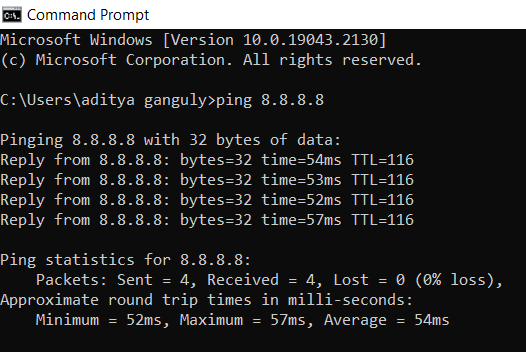
**neighbouring machine (or router). Note the results in Wireshark. The initial ARP request**

**broadcast from your PC determines the physical MAC address of the network IP Address, and**

**the ARP reply from the neighbouring system. After the ARP request, the pings (ICMP echo**

**request and replies) can be seen.**

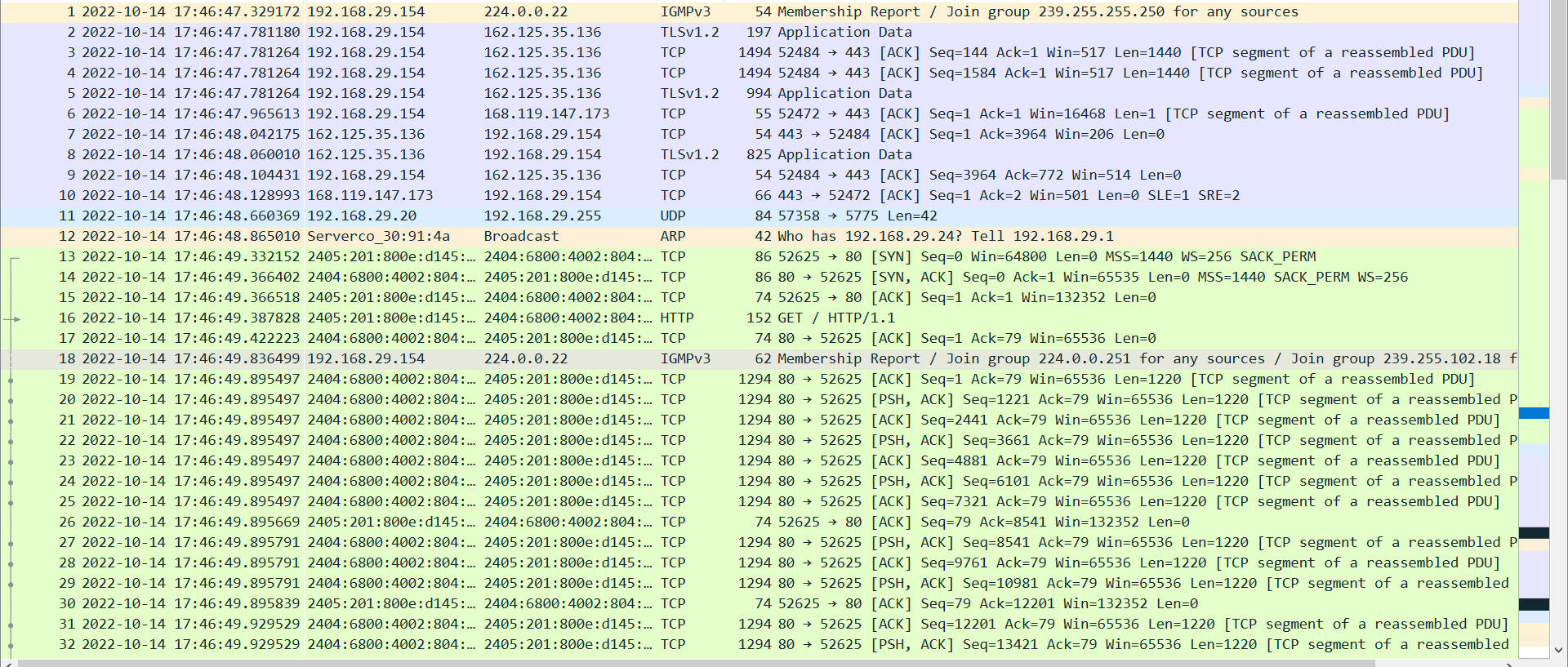
****



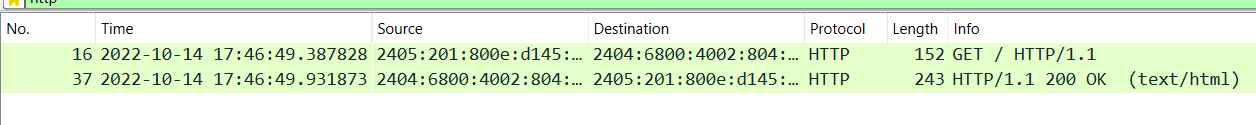
**2. Generate some web traffic and**

**a. find the list the different protocols that appear in the protocol column in the**

**unfiltered packet-listing window of Wireshark.**

****

**Some Protocols are HTTP, TCP, UDP, ARP, IGMPv3, TLSv1.2**



**Time = 49.93 – 49.38 = 0.55 s**

**c. What is the Internet address of the website? What is the Internet address of your**

**computer?**

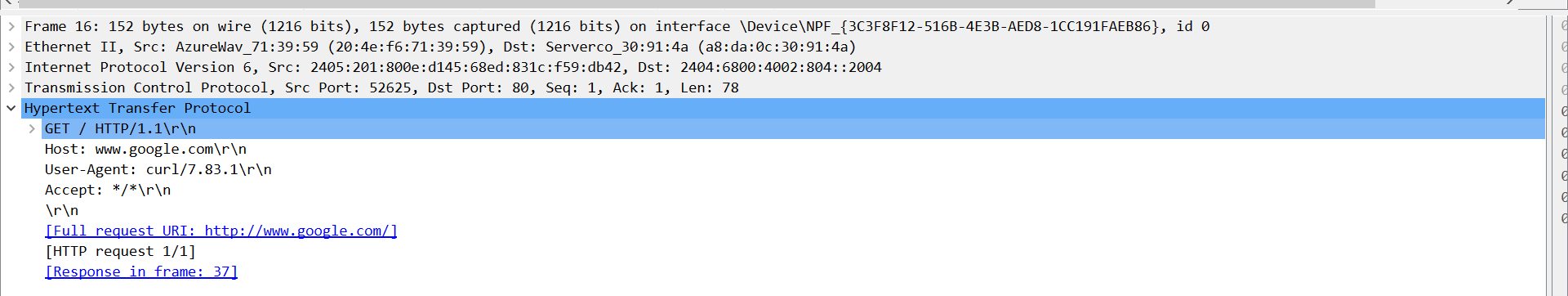
**Ipv6 address of my computer is 2405:201:800e:d145:6180:3c74:cc11:1668**

**Ipv6 address of website is 2404:6800:4002:804::2004**

**d. Search back through your capture, and find an HTTP packet containing a GET**

**command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in**

**the Packet Details Panel, from the packet.**

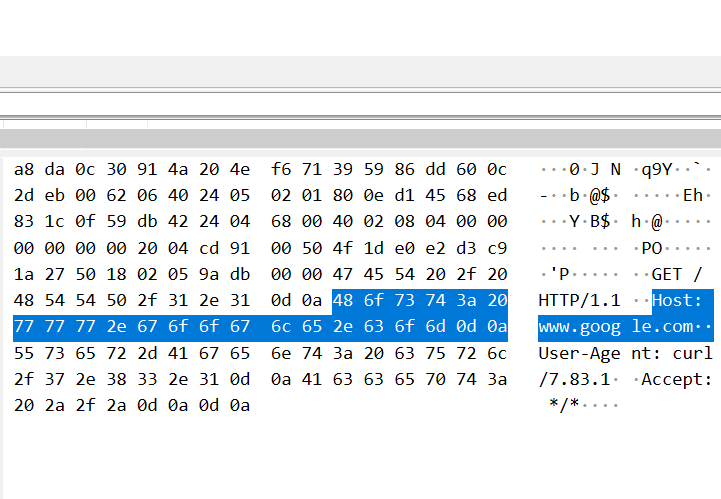


**e. Find out the value of the Host from the Packet Details Panel, within the GET**

**command.**

**Host:** [**www.google.com**](http://www.google.com)

**3. Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.**

****

**4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.**

**First four bytes are 48 6f 73 74**

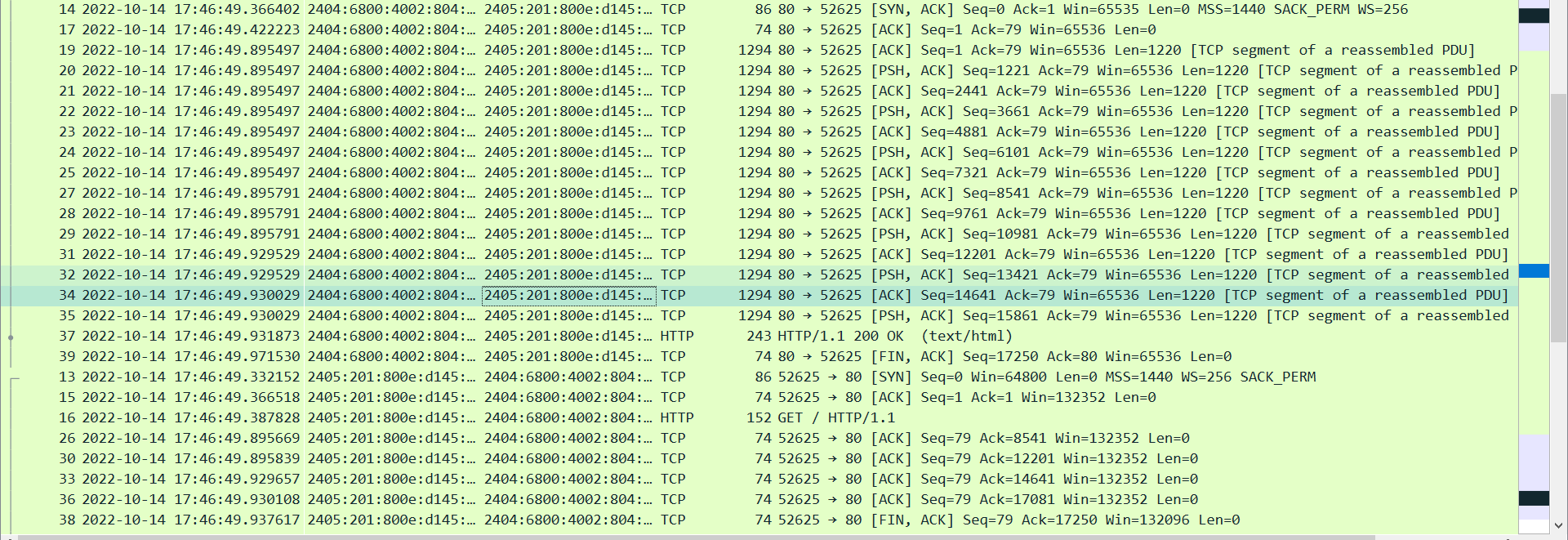
**5. Filter packets with http, TCP, DNS and other protocols.**

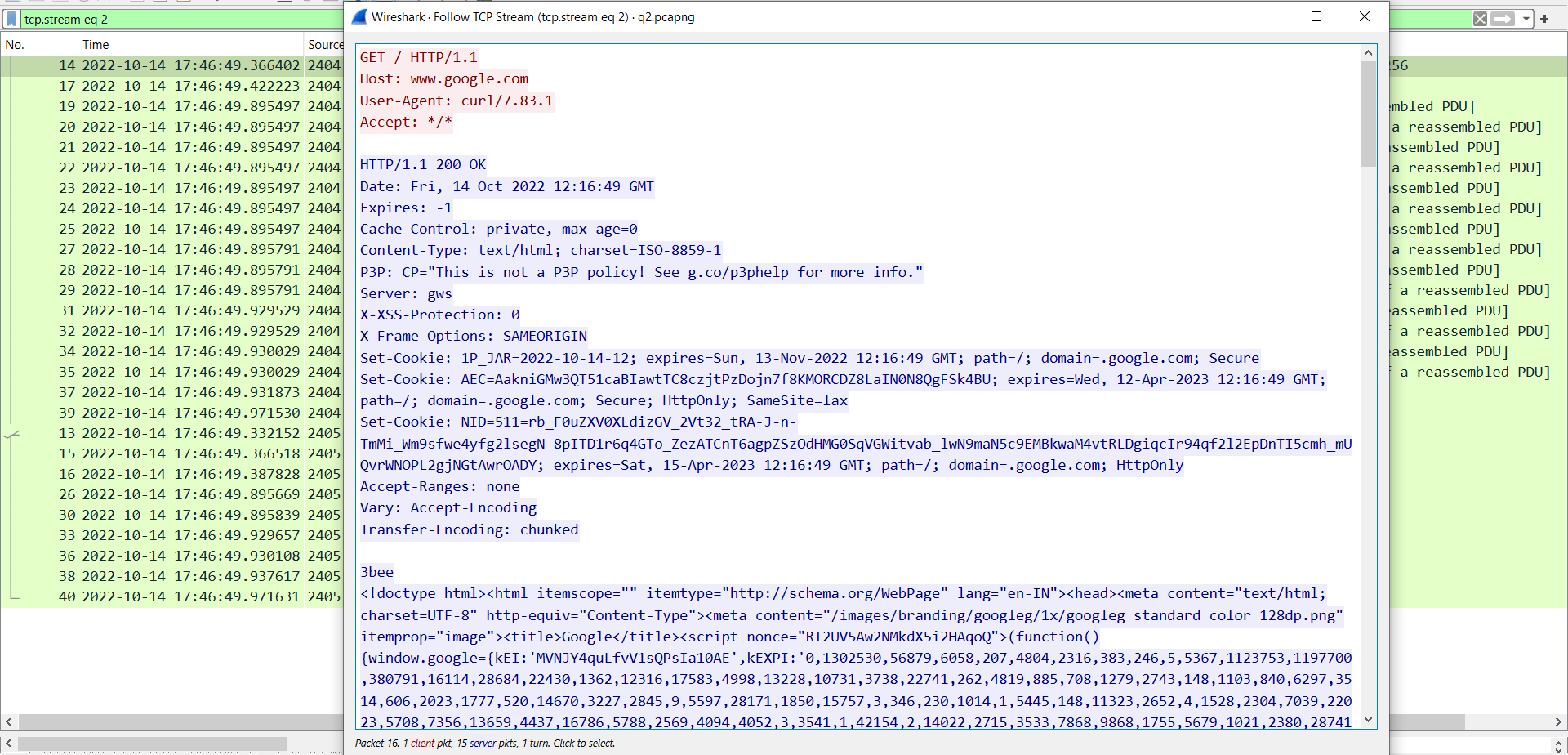
**a. Find out what are those packets contain by following one of the conversations (also**

**called network flows), select one of the packets and press the right mouse**

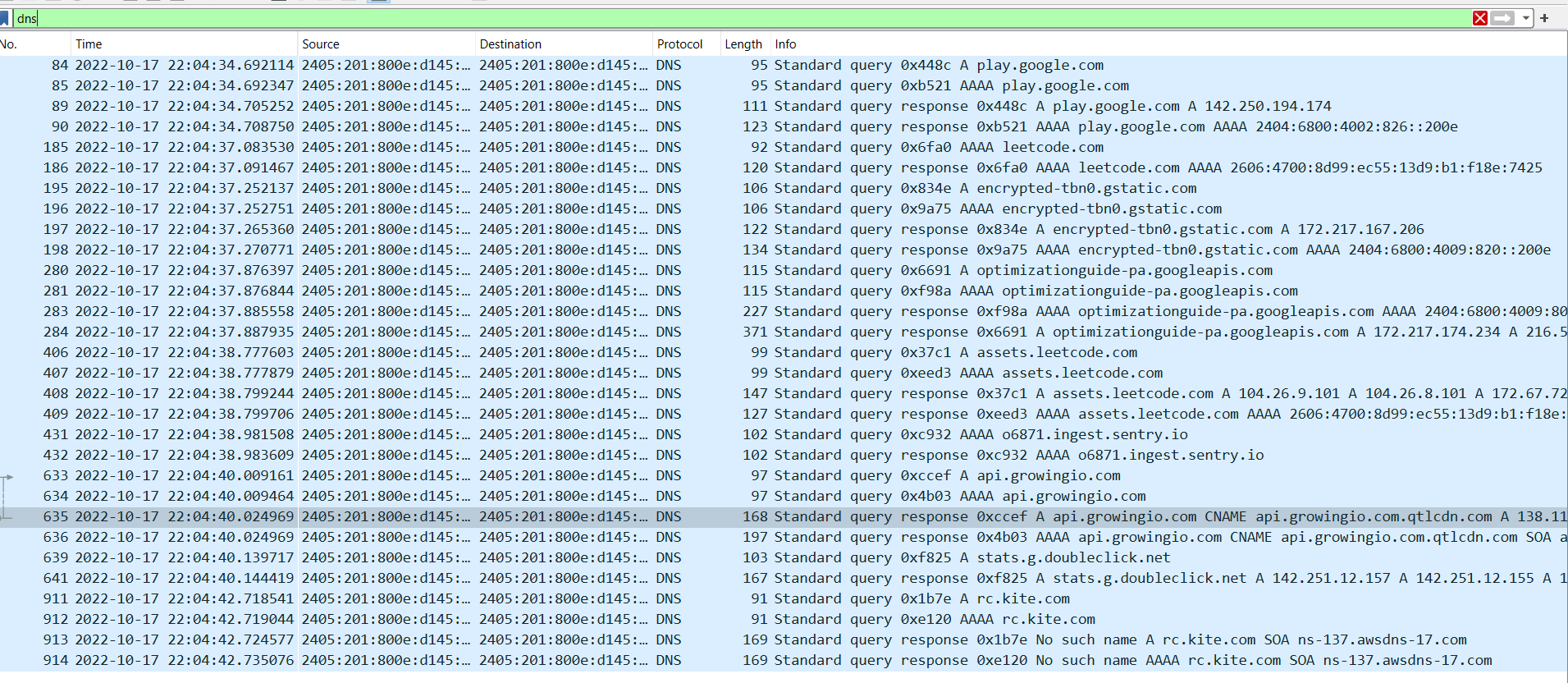
**button..click on follow.**

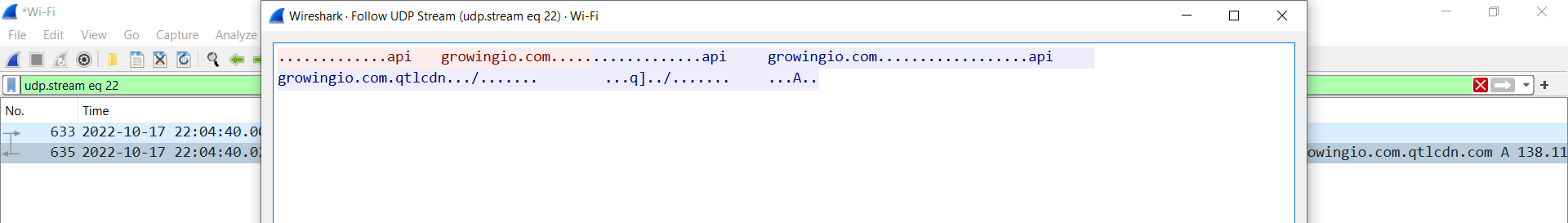
**TCP**

****



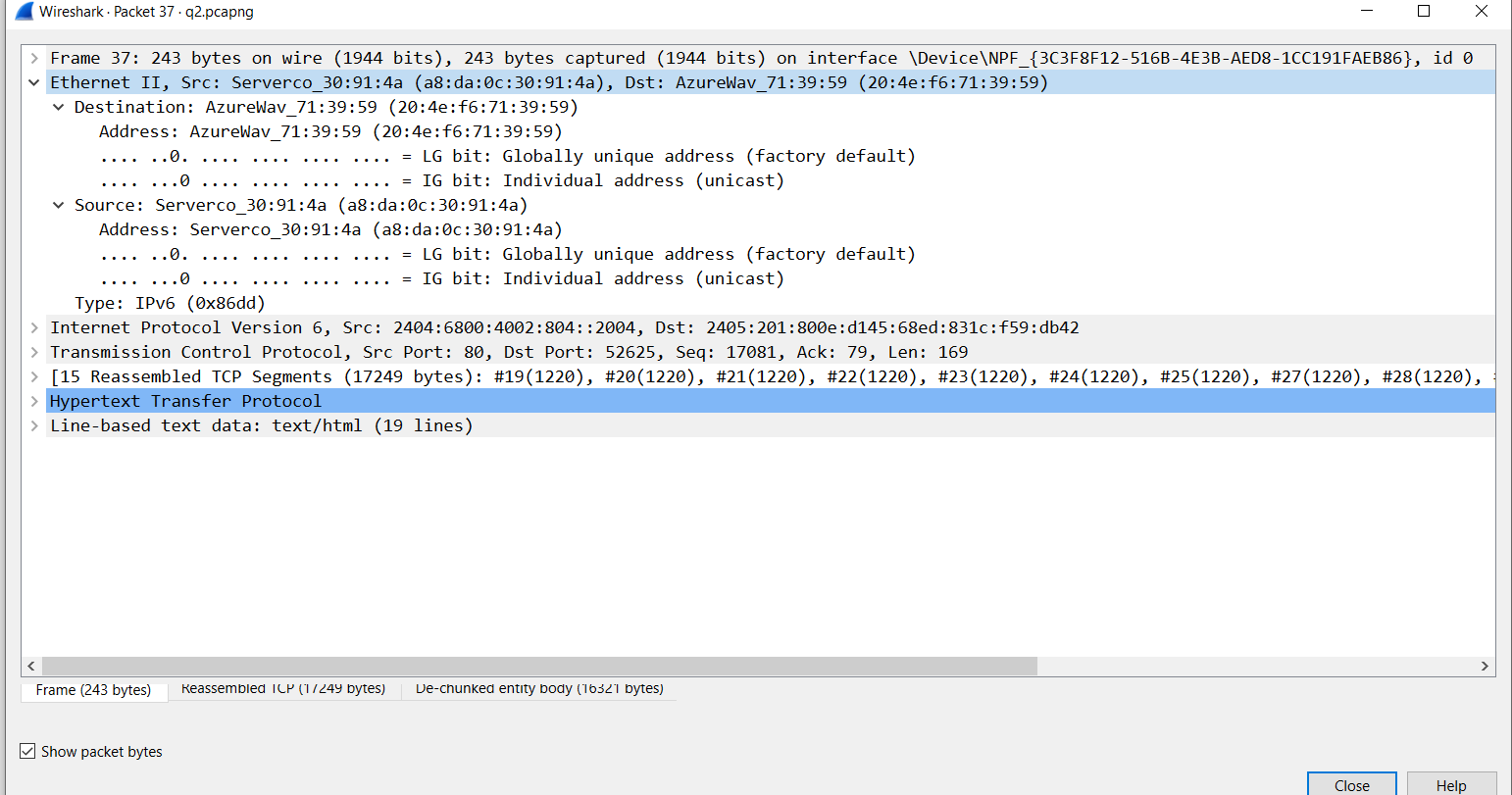
**DNS**

****

****

**6. Search through your capture, and find an HTTP packet coming back from the server (TCP**

**Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.**

****

**7. What are the manufacturers of your PC’s Network Interface Card (NIC), and the servers NIC?**

**Manufactures of my NIC - AzureWav\_71:39:59 (20:4e:f6:71:39:59)**

**Manufactures of Servers NIC - Serverco\_30:91:4a (a8:da:0c:30:91:4a)**

**8. What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?**

**My OUI – 20 4e f6**

**Servers OUI – a8 da 0c**

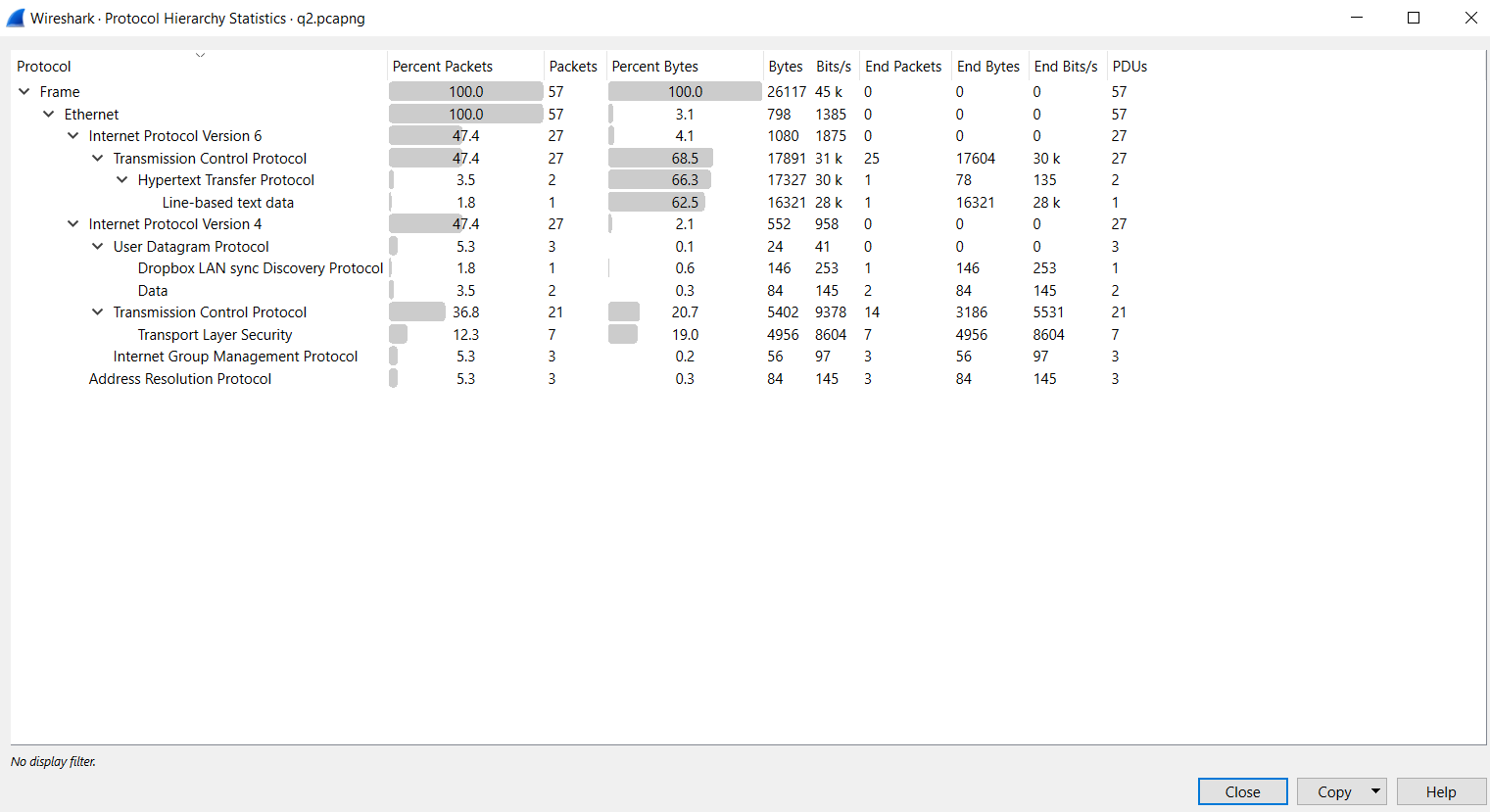
**9. Find the following statistics:**

**a. What percentage of packets in your capture are TCP, and give an example of the**

**higher level protocol which uses TCP?**

**b. What percentage of packets in your capture are UDP, and give an example of the**

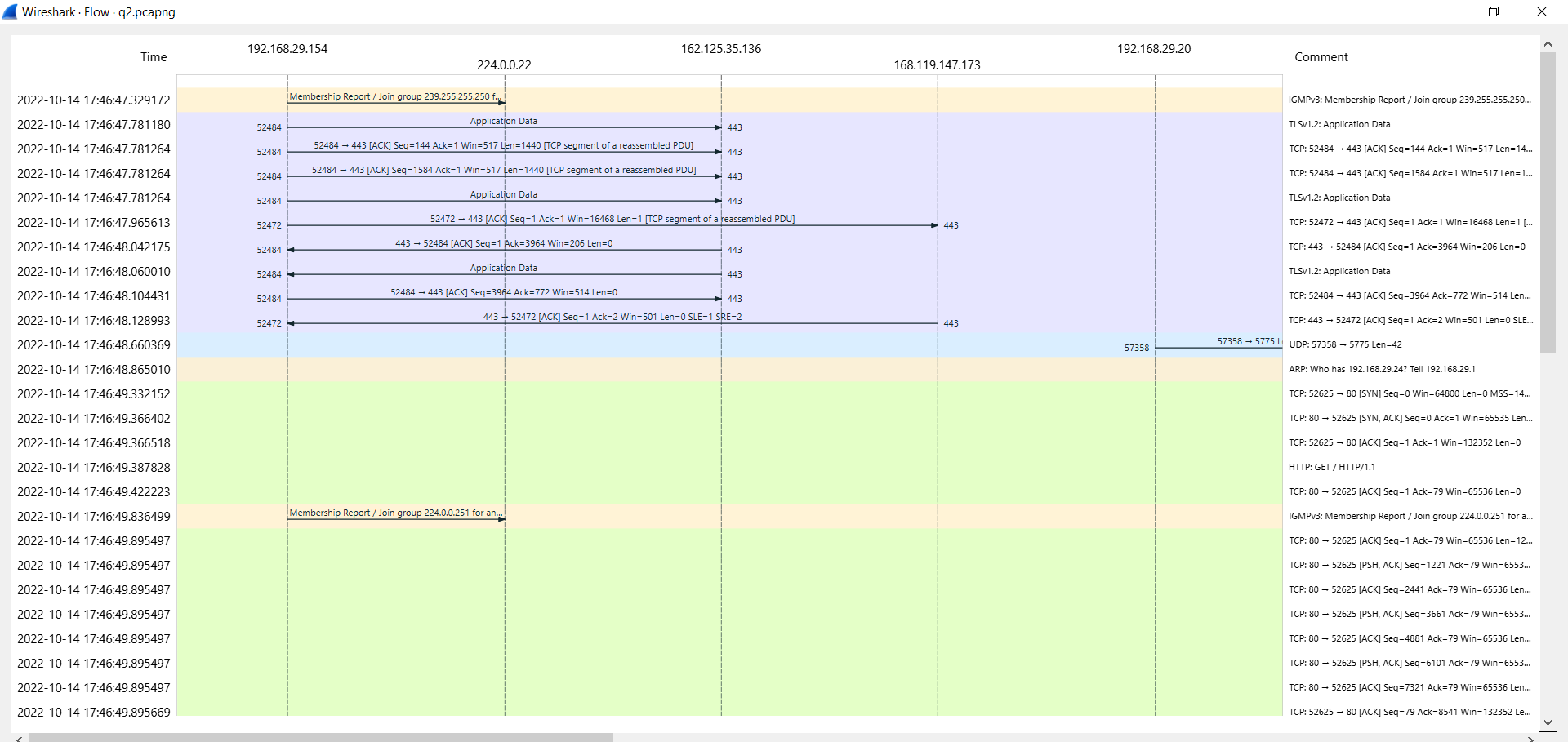
**higher level protocol which uses UDP?**

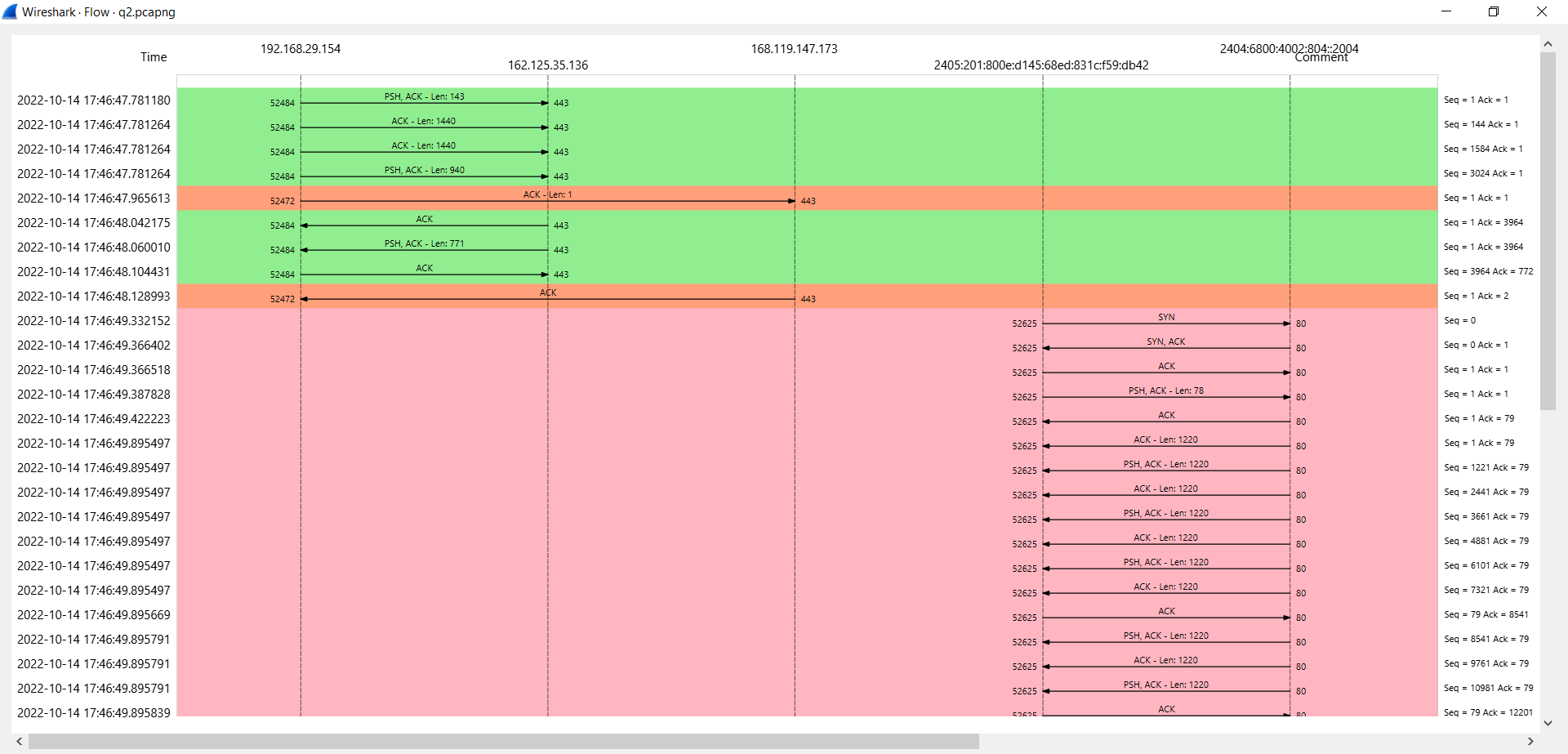
****

1. **47.4 % packets are TCP ipv6, higher level protocols using TCP – HTTP, FTP**
2. **5.3% packets are UDP ipv4, higher level protocol using UDP – DNS, SNMP**

**10. Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and**

**Network Source options, and click the OK button.**

****

****