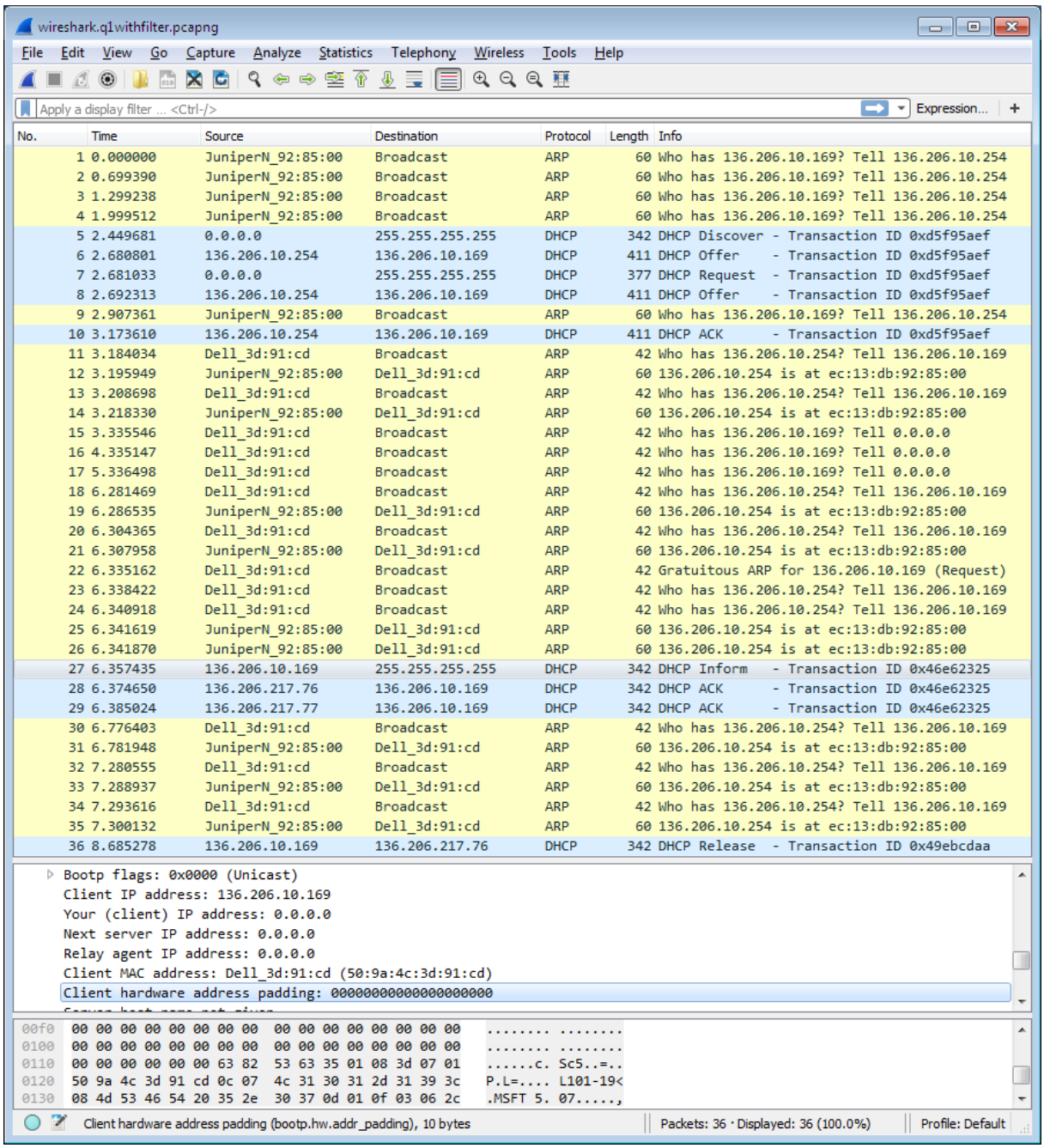
Part 1: DHCP traffic

Your IP & MAC address for this experiment (use ipconfig)

136.206.10.169	50-9A-4C-3D-91-CD

Screen capture: ipconfig information **cmd** window

Screen capture of Wireshark with DHCP and all ARP packets shown.



Packet numbers relevant to the DHCP interaction:

a. DHCP DISCOVER - Packet 5
b. DHCP OFFER - Packets 6, 8
c. DHCP Request - Packet 7
d. DHCP Acknowledgement - Packets 10, 28, 29
e. DHCP Release (if you release using `ipconfig /release`) - Packet 36
f. All ARP packets used - 1, 2, 3, 4, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 30, 31, 32, 33, 34, 35

Function of each packet

a. DHCP DISCOVER

Packet 5:
This packet is used by my computer to broadcast a request on the network for a new IP address from a DHCP server.

b. DHCP OFFER

Packets 6, 8:
This are response messages to my computer's DCHP Discover broadcast. The server is offering my computer an IP address. The packets contain other information such as my computer's MAC address and the IP address being offered.

c. DHCP Request

Packet 7:
This is a reply message broadcasted from my computer in reply to the DHCP Offer packet. This packet accepts the IP address that the DHCP server offered.

d. DHCP Acknowledgement

Packets 10, 28, 29:
These are packets sent from the DHCP server acknowledging the request for the IP address. They also contain configuration information and the duration of the lease for the DHCP IP address.

e. DHCP Release (if you release using `ipconfig /release`)

Packet 36:
This is a packet my computer sends to the DHCP server to release the current IP address it is using. The DHCP server may now lease this address to other clients.

f. ARP

Packets 1, 2, 3, 4, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 30, 31, 32, 33, 34, 35:

ARP packets are used by IP RFC826 to map IP addresses. There are both ARP Requests and Replies here. The ARP request message is broadcasted and received by all systems on the network. If there is a machine with the IP address that was in the ARP request message, it sends an ARP Reply packet which contains its MAC address so that the machines may communicate.

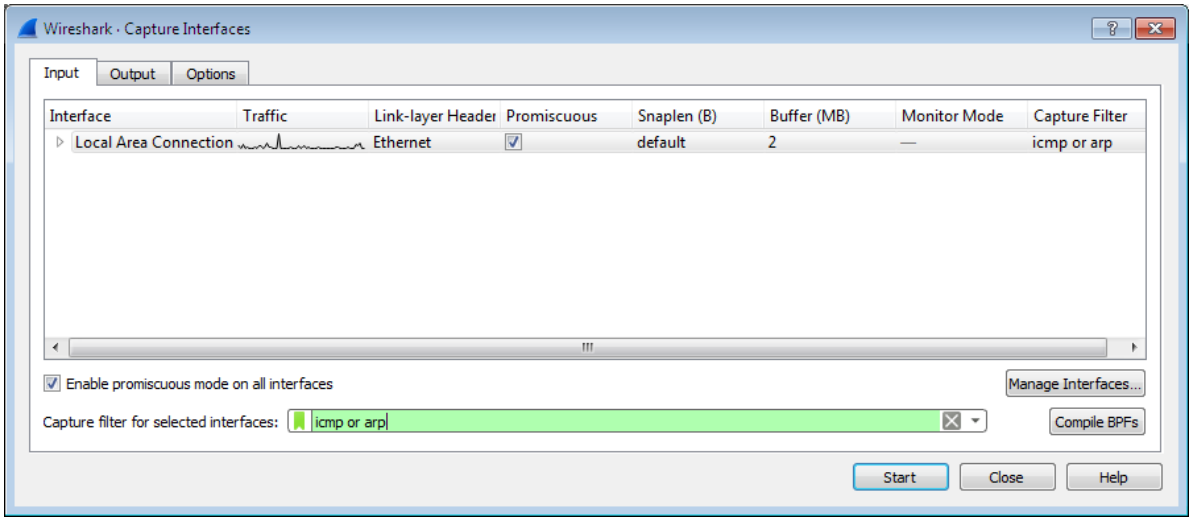
Packet 22 is a Gratuitous ARP packet. It updates the ARP cache.

Part 2: `ping` traffic

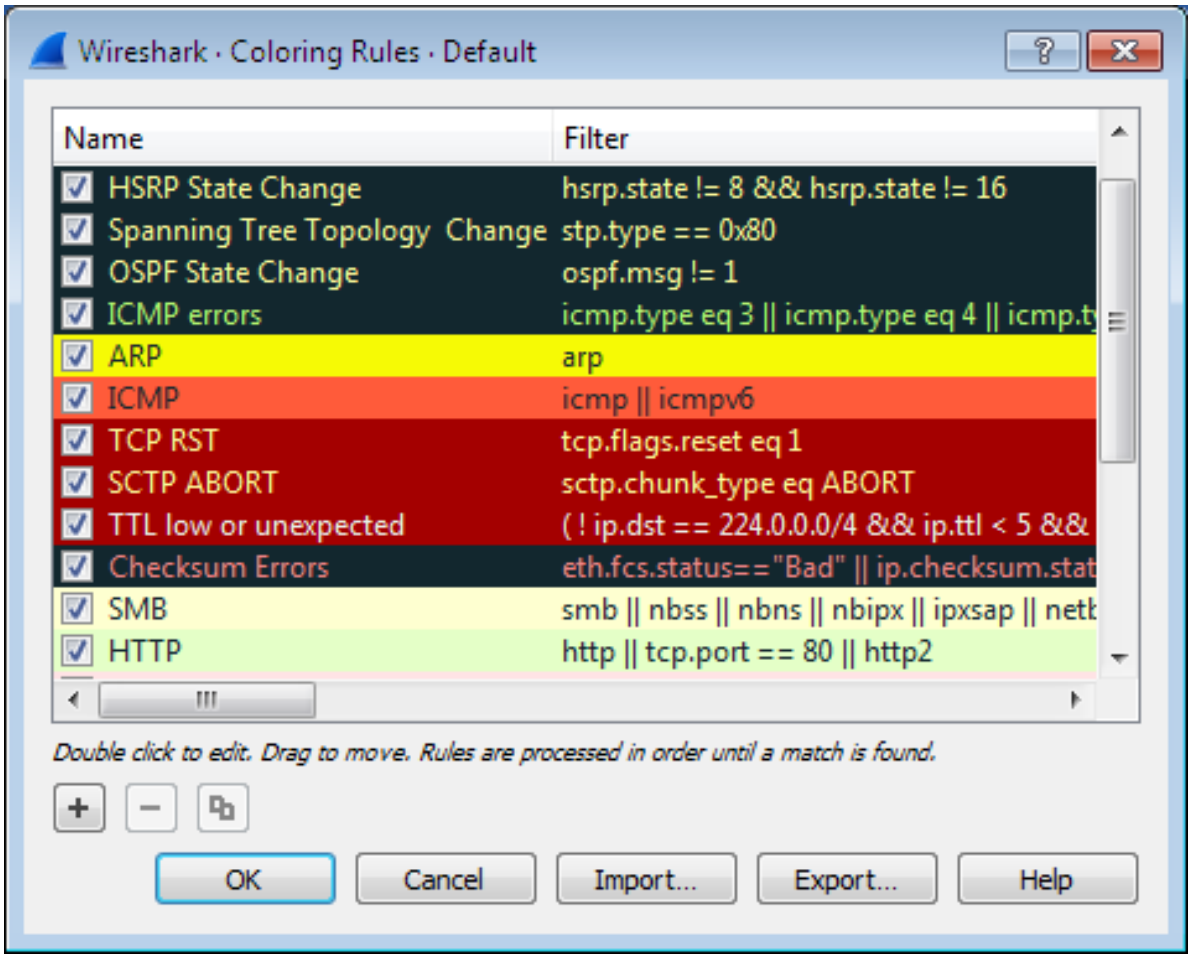
Your IP & MAC address for this experiment (use ipconfig)

136.206.10.169	50-9A-4C-3D-91-CD

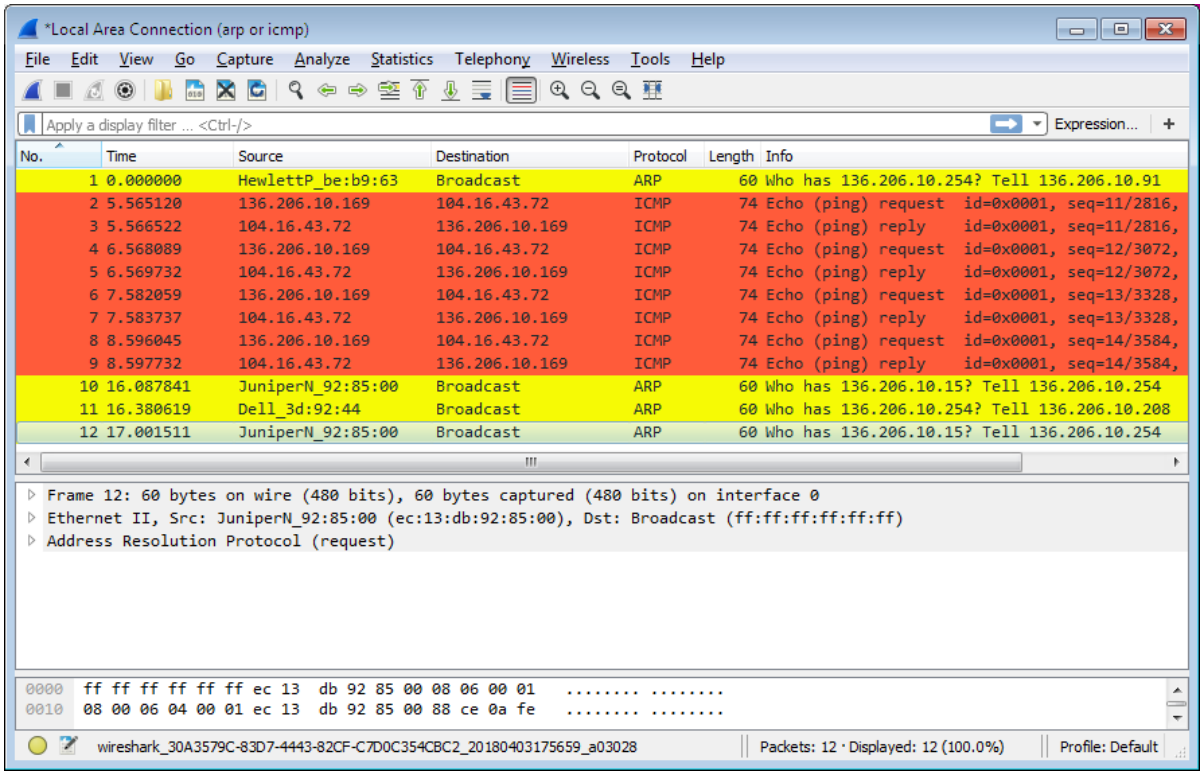
Screen capture of Wireshark filter utilised:



Screen capture of Wireshark colouring rules applied:



Screen capture of Wireshark packet trace showing all relevant ping generated traffic, including ARP and ICMP traffic.



Packet numbers relevant to the experiment:

Packets 1 – 9 are relevant.

Packet 1: ARP Packet that acquires the MAC address from the machine being pinged.

Packets 2 – 9: Echo replies from the machine being pinged.

Explanation for each packet

- Function

Packet 1:

This is an ARP Packet that acquires the MAC address from the machine being pinged. It is broadcasted across the network by my machine. It asks who has the IP address contained in the packet, in this case that IP address is 136.206.10.254. Now my computer can communicate with that machine. The length of this packet is 60 bytes.

Packet 2:

This is the first ping Echo Request packet. It is used by the ICMP protocol. This packet was sent when I pinged www.rte.ie. Its length is 42 bytes. ICMP is a protocol that checks if one machine may communicate with a different machine. This is important as it contains a lot of information in the Ethernet header which is inside the packet. Within the Ethernet header, there is information on the IP address for rte.ie, the ICMP header and ICMP packet type. The packet also has a TTL. We will be able to see if the machine has issues communicating with the other by the Echo Requests.

Packet 3:
This is the first ping Echo Reply. As I pinged rte.ie, this is where the reply came from. We can see that as the IP address source is 104.16.43.72. This reply is to let the sender of the request packet know that the machine is online. We will be able to see any issues with the network by the statistics show. For example, we will know there is an error if the TTL expires.

Packets 4, 6, 8:
This is the ping Echo Request process being repeated.

Packets 5, 7, 9:
This is the ping Echo Reply process being repeated.

- Explain why it is generated:

  ARP messages are generated and broadcasted to all systems on the network. We will find out if there is a machine with the IP address that was in the ARP packet. That machine sends an ARP Reply packet which contains its MAC address so that the two machines may communicate. These ARP messages were generated as we cleared the ARP cache and the information needed to be re-acquired.

  The process of generating Echo Request and Reply packets is repeated so that statistics can be provided on the connection between the two machines.

- Explain the data contained in the packet:

  ARP packets contain the source IP address and the target IP address, the source MAC address and the target MAC address, the size of the packet and the ICMP data.

  Echo Request and Reply packets contain information such as the average Round Trip time, amount of packets lost, and the TTL.

Rte.ie was pinged

Part 3:

Your IP & MAC address for this experiment (use ipconfig)

136.206.10.174	50-9A-4C-3D-92-59

Filter to show only traffic concerning the test machine

Filter	(eth.addr == 50:9a:4c:3d:92:59 && (dns.qry.name==dspca.ie || ip.addr==78.153.214.103) && !icmp) || (arp && eth.addr == 50:9a:4c:3d:92:59) || arp

Explain how you found the start of the interaction between your PC and the website.

I used the following filter to find the start of the interaction:

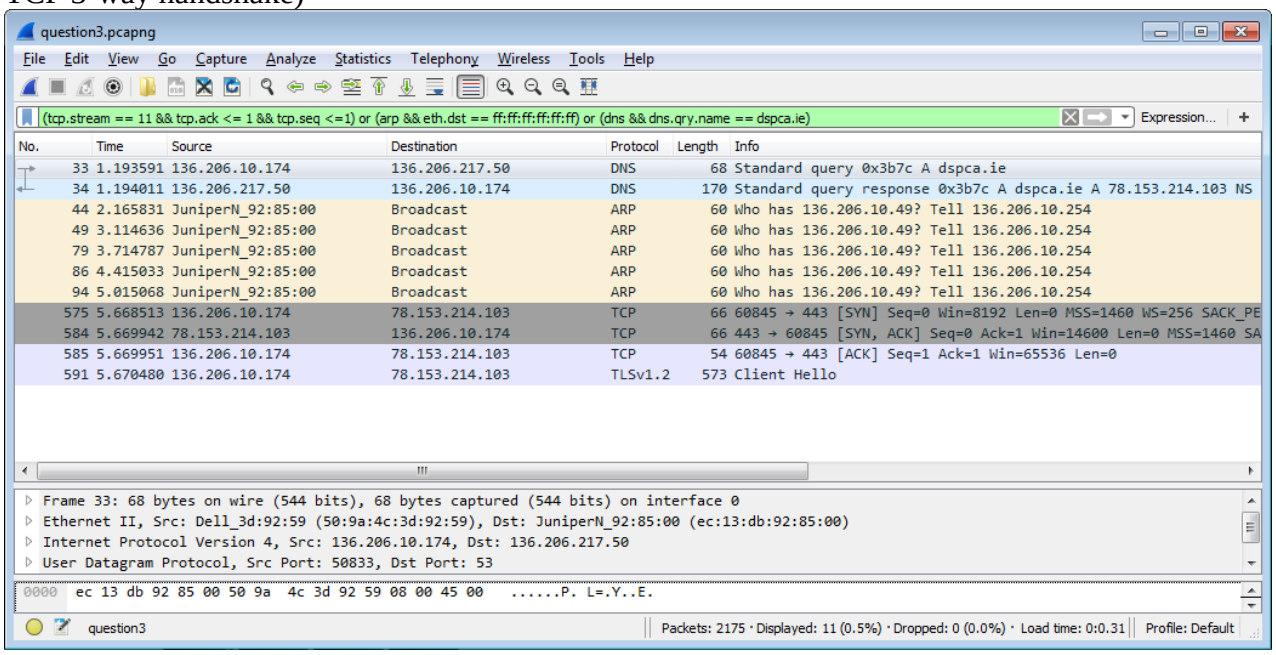
(tcp.stream ==11 && tcp.ack <= 1 && tcp.seq <=1) or (arp && eth.dst == ff:ff:ff:ff:ff:ff) or (dns && dns.qry.name == dspca.ie)

This checks the following requirements:

the TCP packets are the first sent or
the ARP and eth.dst is my MAC address or
the DNS packets contain “dspca.ie” as that is the website I contacted

This filtered out what I did not need and showed me the DNS queries for dspca.ie, revealing the beginning of the interaction.

Wireshark window showing the start of the interaction (should show ARP, DNS and TCP 3-way handshake)



Write down the numbers of the packets with the 3-way handshake.
Explain what is happening with these 3 packets.

Packet 738: This is a SYN packet. It is sent by my machine to the server. It checks if the sever is open or new connections.

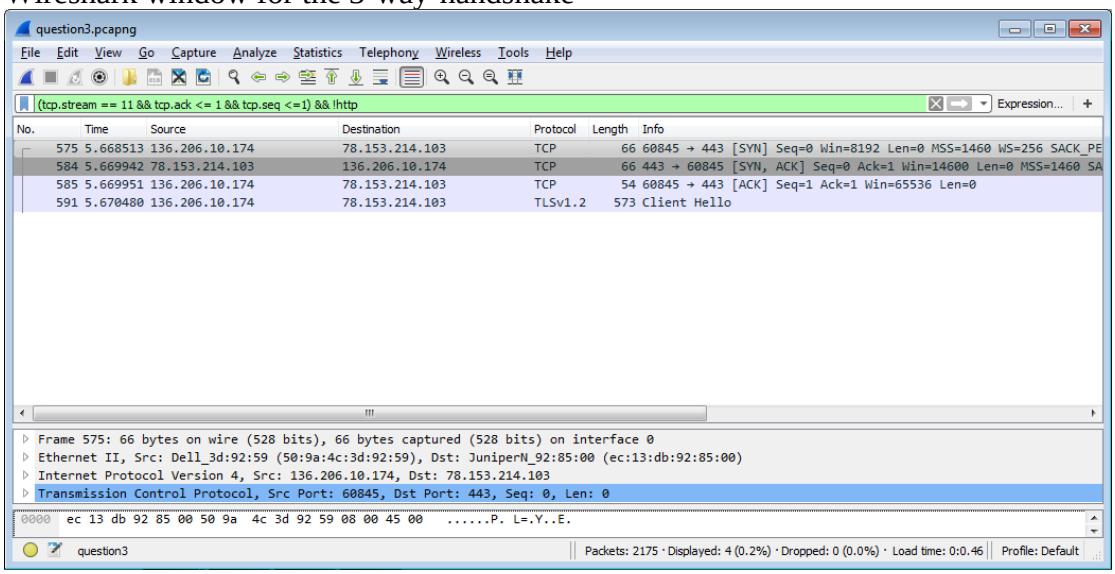
Packet 739: This is a SYN/ACK packet. This was sent by the server in response to the SYN packet. Now my computer knows that the it can connect to the server.

Packet 740: This is a ACK packet. This was sent by my computer to acknowledge the SYN/ACK packet. The server and my computer are now connected.

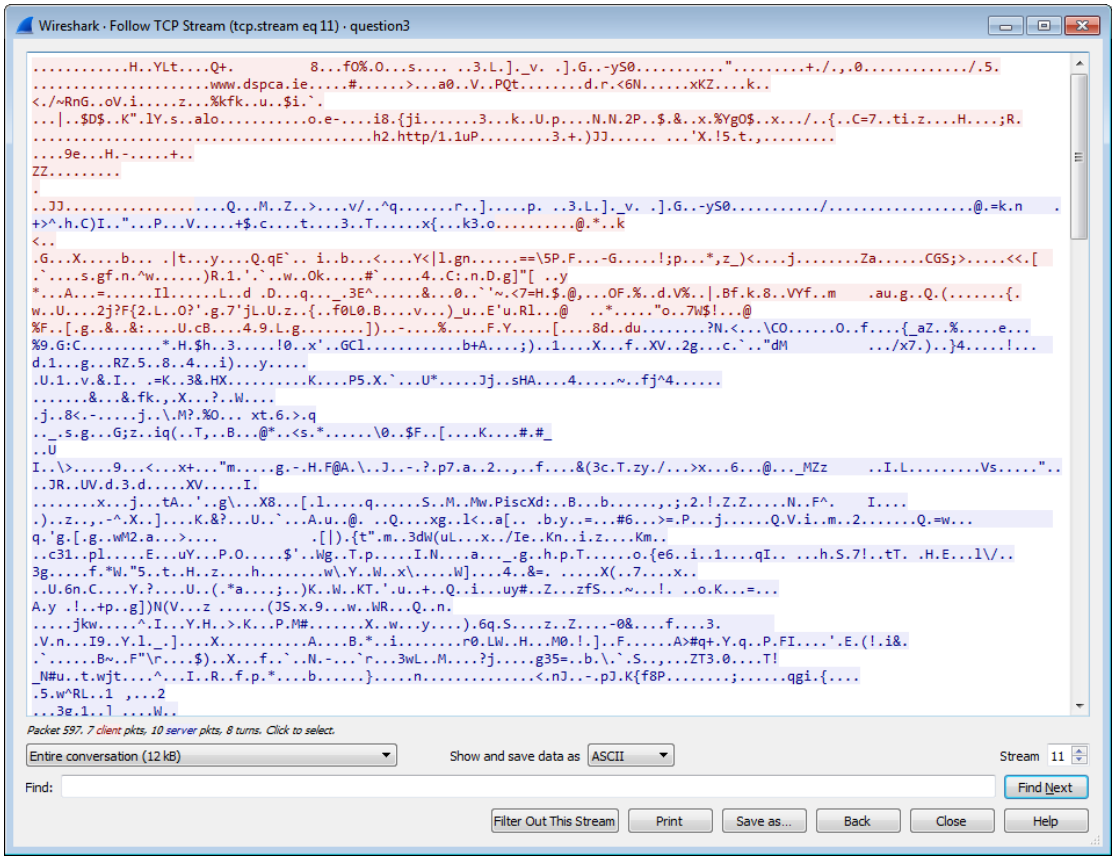
Write down a filter to show only these three-way-handshake packets

Filter	(tcp.stream == 11 && tcp.ack <= 1 && tcp.seq <=1) && !http

Wireshark window for the 3-way-handshake



Show the **Follow TCP Stream** window here.



Your notes on…

a. The GET requests made

b. The responses from the server

c. The HTTP response codes used in the interaction and what they mean (look them up yourself on the Web)