CA169 Networks Assignment Two

Answer Sheets

STUDENT NAME:	CormacDuggan
STUDENT NUMBER:	17100348
PROJECT NUMBER:	2
MODULE CODE:	CA169
DEGREE: {CA|EC|CPSSD|ECSA]	CA
LECTURER:	Brian Stone

Declaration

In submitting this project, I declare that the project material, which I now submit, is my own work. Any assistance received by way of borrowing from the work of others has been cited and acknowledged within the work. I make this declaration in the knowledge that a breach of the rules pertaining to project submission may carry serious consequences.

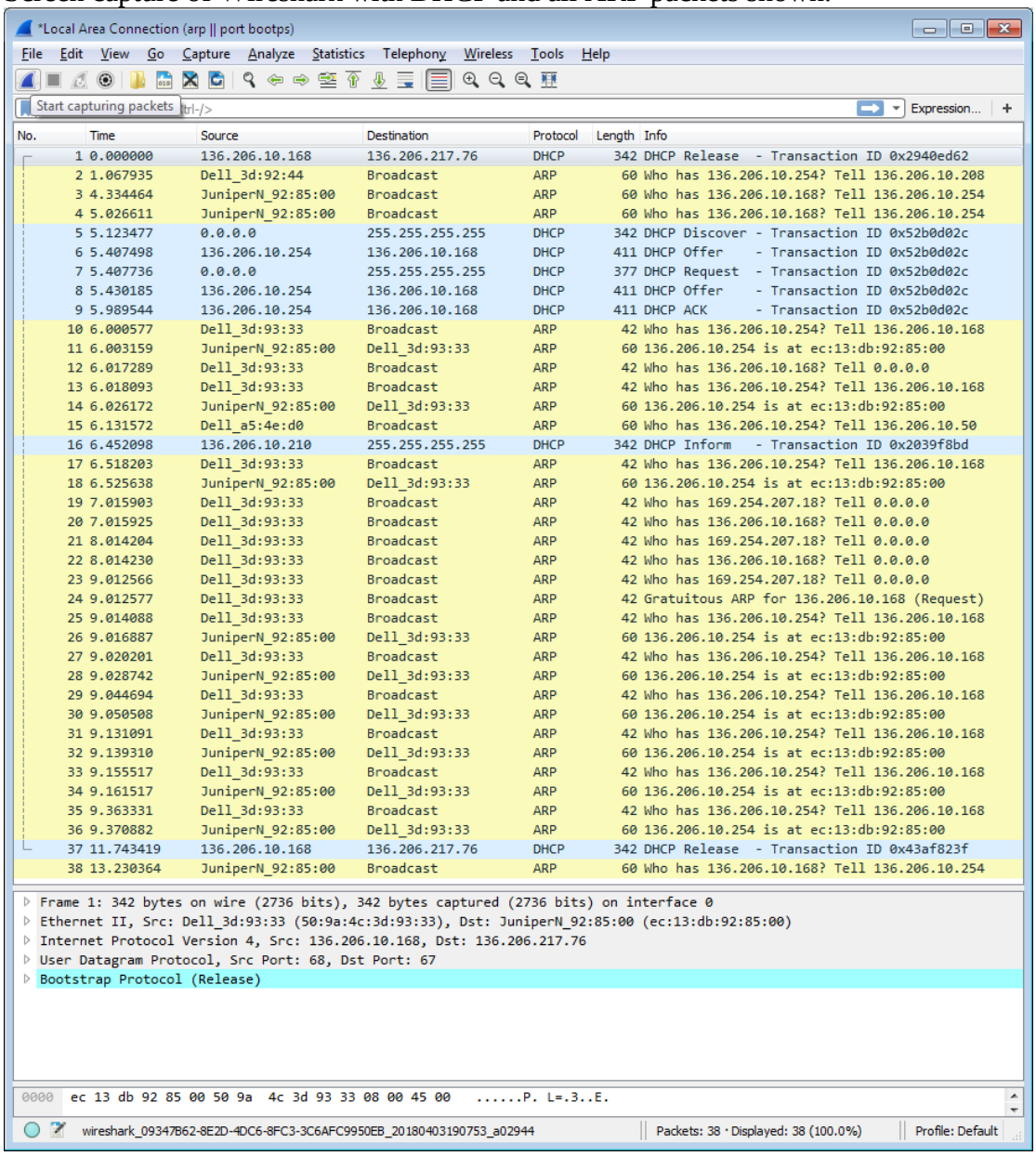
Part 1: DHCP traffic

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

136.206.10.168	50-9A-4C-3D-93-33

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 – Packet 6
c. DHCP Request – Packet 7
d. DHCP Acknowledgement – Packets 9
e. DHCP Release (if you release using `ipconfig /release`) – Packet 1, 37
f. All ARP packets used – Packets 1-4, 10-15, 17-35, 38

Function of each packet

a. DHCP DISCOVER
   Packet 5:
   This is a packet broadcast from the host machine sent across the network in search of a DHCP server to give the machine an IP

address. The packet old information on the MAC address of the host machine.

b. DHCP OFFER
   Packet 6:
   The DHCP offer packet is a response to the DHCP discover sent from the DHCP server offering the host machine an IP address.

c. DHCP Request
   Packet 7:
   The DHCP request packet is a response to the DHCP offer from the host machine telling the server that it is happy and would like to take the IP address it has been offered.

d. DHCP Acknowledgement
   Packet 9:
   The acknowledgement packet is the DHCP server responding to the previous request packet saying "Ok you want that IP, got it, it's yours."

e. DHCP Release (if you release using `ipconfig /release`)
   Packets 1 and 37:
   This packet is sent form the host machine to the DHCP server telling it to release the IP linked to the host's MAC address and start to let it be assigned to other clients.

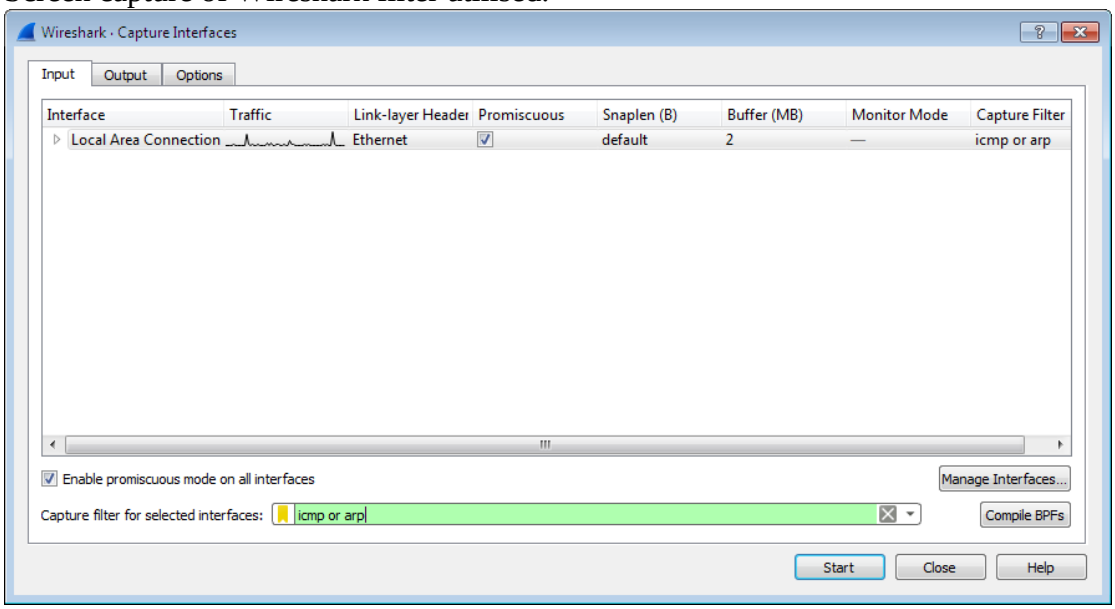
f. ARP
   Packets 1-4, 10-15, 17-35, 38:
   The ARP packets sent out in this experiment are requests from the host machine asking if another machine with a given MAC address has a certain IP. Some of the ARP packets are replies from the machines that contain the MAC and IP sent in a request packet. If the machine responds with both the MAC and IP from the request it will send back an ARP reply packet containing only its MAC address.
   Packet 24 is a Gratuitous ARP packet which is sent from the host machine across the network telling the other machines of its new IP address mapping.

Part 2: `ping` traffic

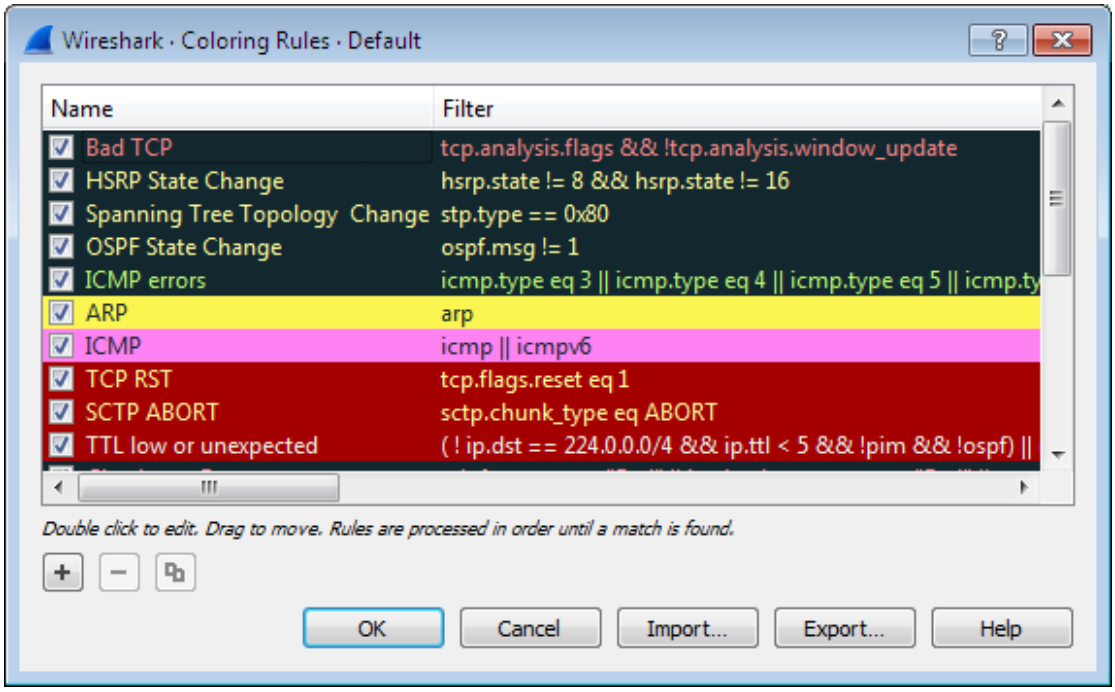
Your IP & MAC address for this experiment (use ipconfig)

136.206.10.168	50-9A-4C-3D-93-33

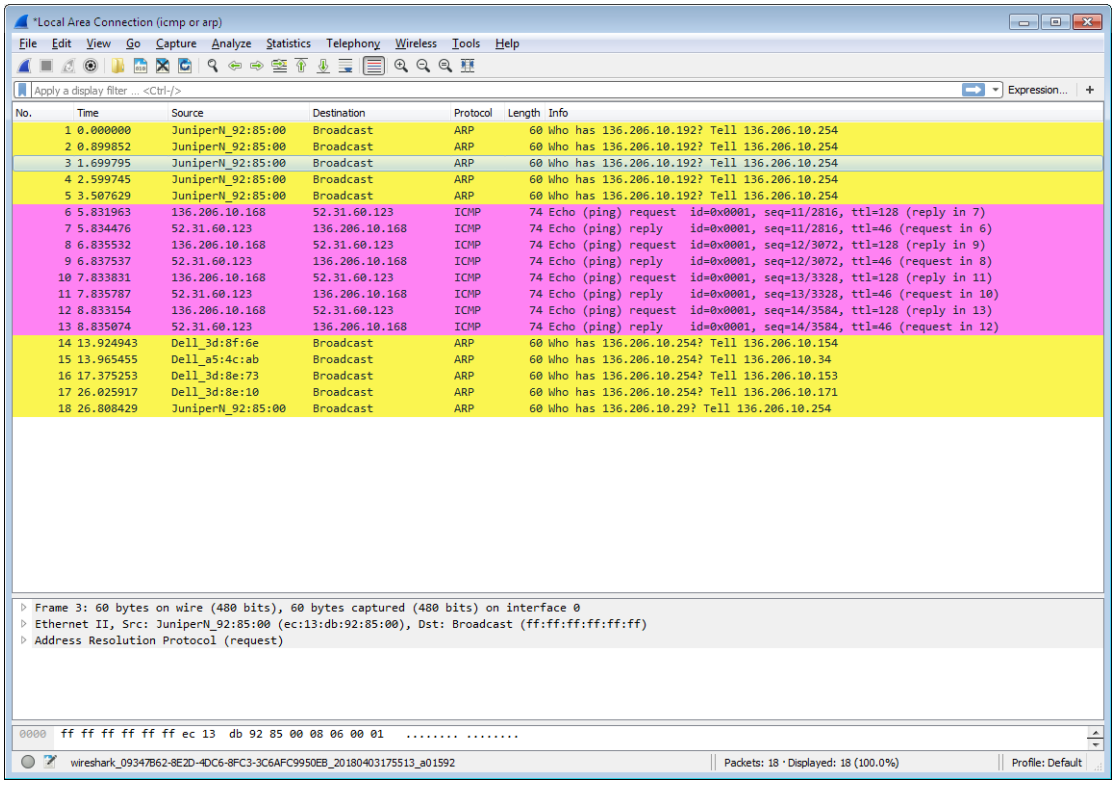
Screen capture of Wireshark filter utilised.



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:
For this experiment packets 6-13 are relevant.
Explanation for each packet

For this experiment I pinged www.dcu.ie.

Packet 6:

The first ICMP echo packet was sent when dcu.ie is pinged. The packet is 74 bytes long and the data in the echo request is 32 bytes. The ICMP packets are a way for the host machine to find out if it is able to connect to another machine. The packet holds the IP address of the final destination (dcu.ie) and the time to live of the echo requests which is 128 ms. The packet also shows the time taken to receive a reply which in this case is 7 ms.

Packet 7:

Packet 7 is the ICMP echo reply which is received from 52.31.60.123 or dcu.ie. This reply is a response sent to the host machine telling it that dcu.ie received the echo request packet. The ICMP reply lets the host machine know that it and the requested IP are able to communicate over the network.

Packets 8, 10, and 12:

These packets are the Echo request process being repeated.

Packets 9, 11, and 13:

These packets are the Echo reply process being repeated.

The Echo request and reply process is repeated multiple times to ensure that the host machine can get accurate data on the connection between another IP and their own including the time for a round trip and how accurate the received data from the requested IP will be (aka packet loss).

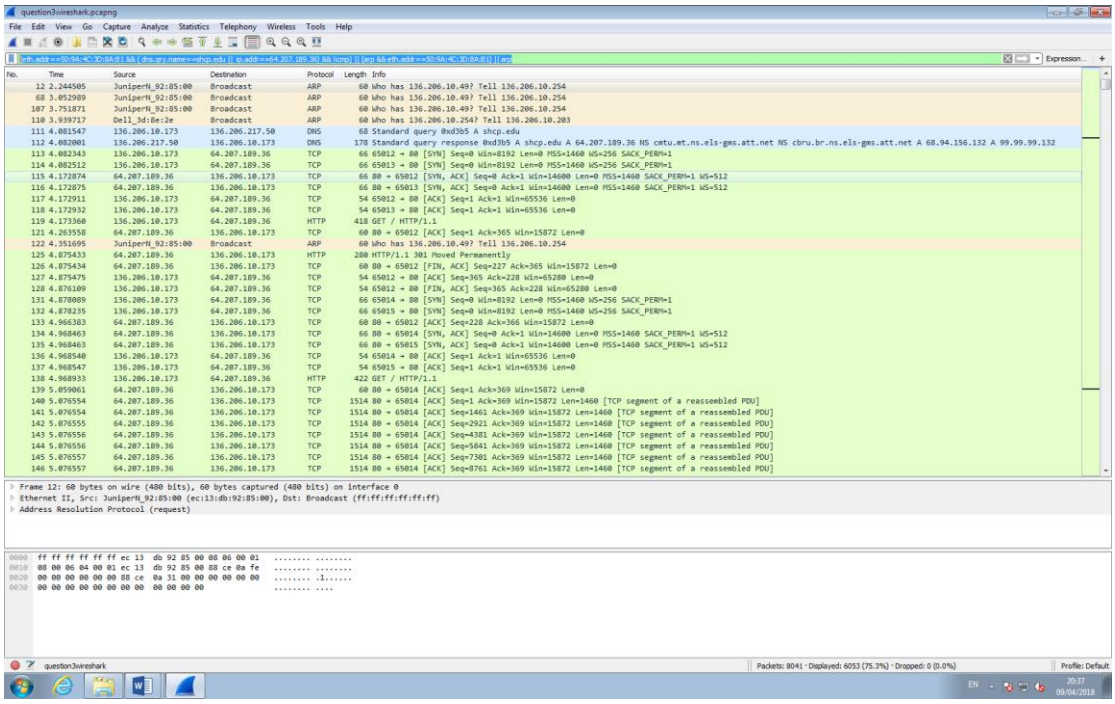
Part 3:

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

136.206.10.173	50-9A-4C-3D-8A-B1

I used www.shcp.edu for this exercise.
Filter to show only traffic concerning the test machine

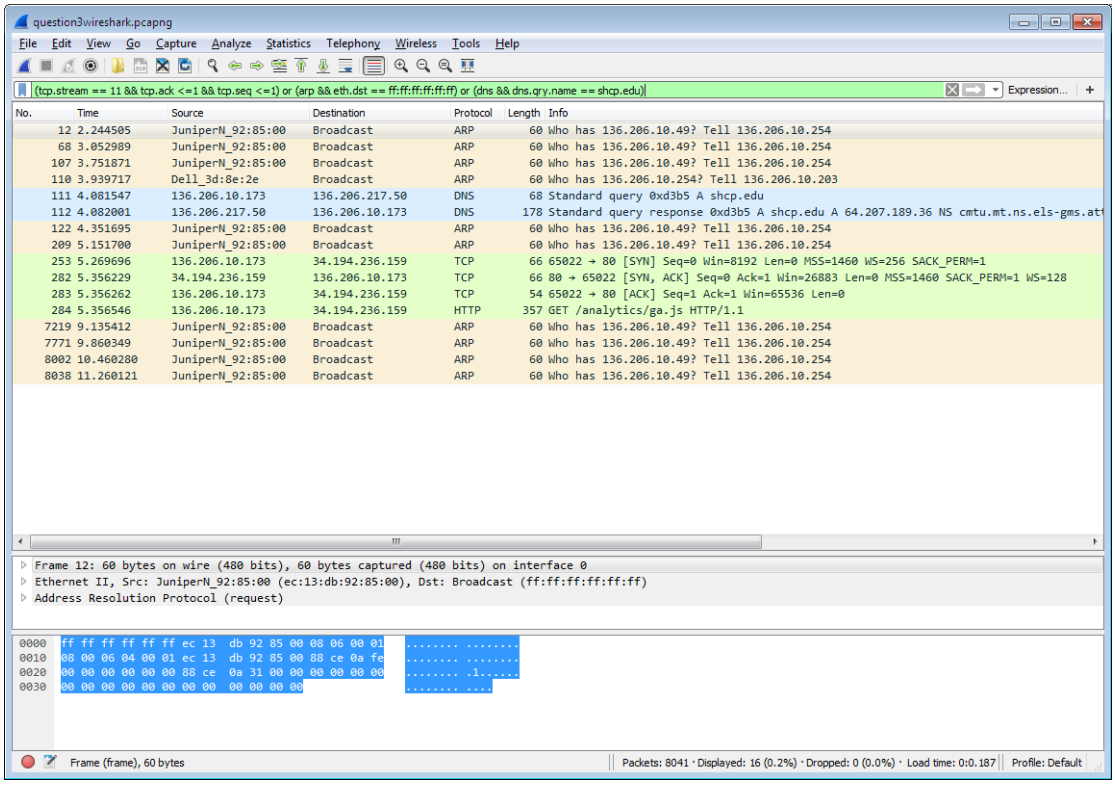
Filter	(eth.addr==50:9A:4C:3D:8A:B1 && (dns.qry.name==shcp.edu || ip.addr==64.207.189.36) && !icmp) || (arp && eth.addr==50:9A:4C:3D:8A:B1) || arp



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

To find start of interaction: (dns contains "shcp" or tcp) and (eth.addr eq 50:9A:4C:3D:8A:B1)
This filter was put in as a display filter in order to single out the correct packets for the start of the three-way handshake interaction. The dns part of the filter separates the packets so that only the dns packets that contain the proper website in them are shown. As well as this I used the eth.addr to separate only the packets that related to my host machine. The two combined with an and statement makes the display show only packets that contain an interaction with shcp.edu and my device.

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 253:
This is the SYN packet which is sent by the host machine to the server of the website asking to open up a connection between the two of them. The packet also contains a sequence number which is 0.

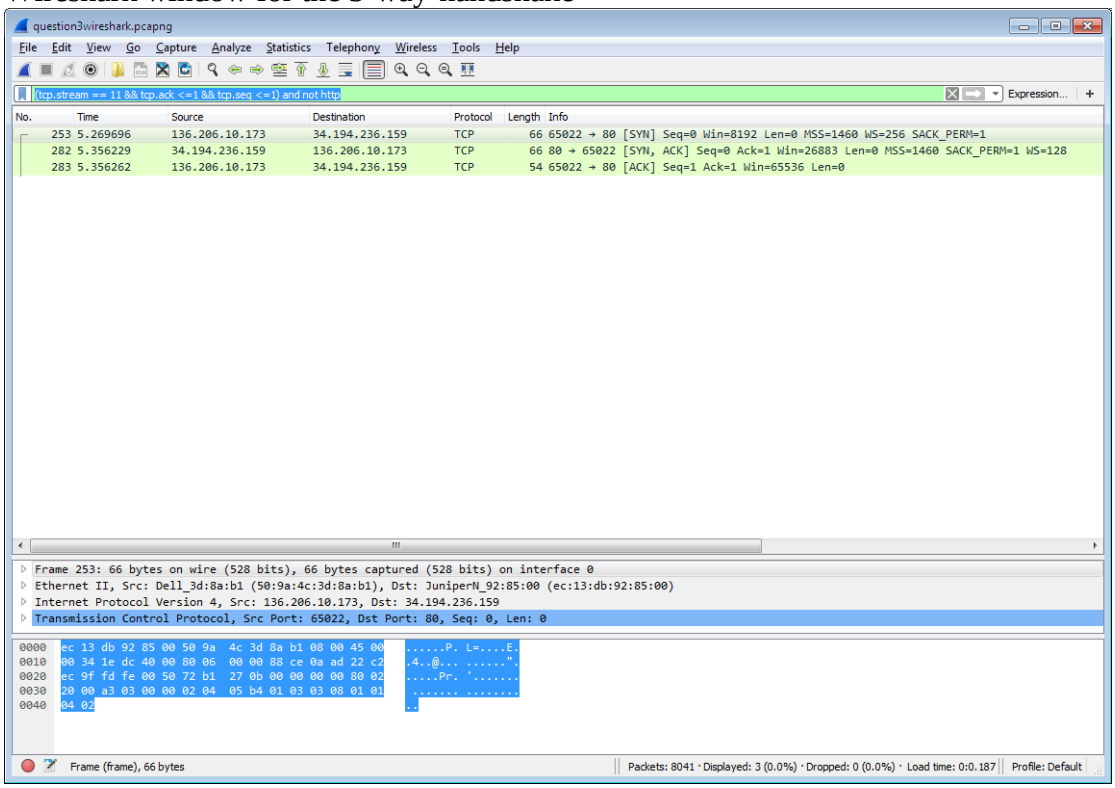
Packet 282:
This is the SYN/ACK packet which is a response packet from the server when they have received the first SYN packet. The SYN/ACK packet tells the host machine that they are able to connect to each other and contains a sequence number which is still 0 and the ACK which is the sequence number plus 1.

Packet 283:
This is the ACK packet which the host machine send back to the server once it has received the SYN/ACK packet saying it has heard that it is allowed to connect and is now going to do so. The packet contains the previous sequence number which is still 0 and the ACK number which corresponds to the previous SYN/ACK number.

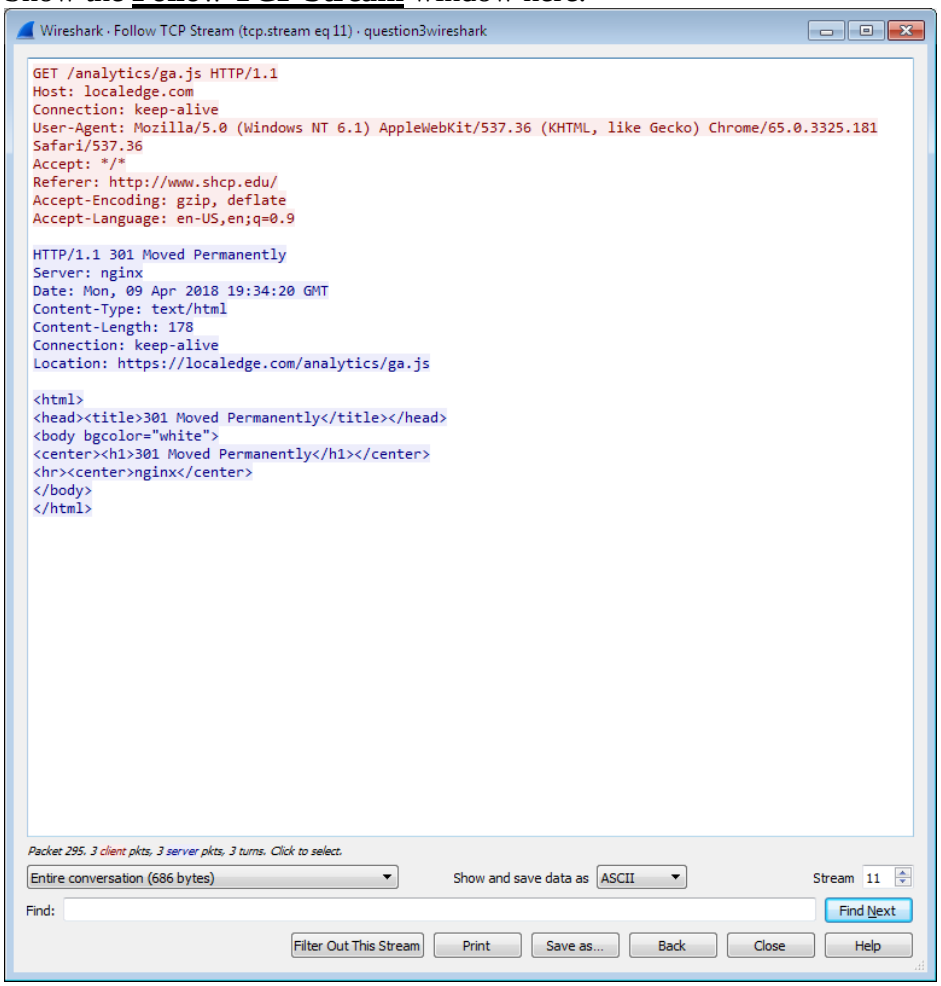
Write down a filter to show only these three-way-handshake packets

Filter	(tcp.stream == 11 && tcp.ack <=1 && tcp.seq <=1) and not http

Wireshark window for the 3-way-handshake



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



Your notes on…

a. The GET requests made
   Inside the TCP steam follow there is a get request asking for /analytics/ga.js which is asking for a JavaScript file in the analytics folder of the server. Considering there are quite a few advanced effects on the website this file probably controls them. So when requesting the website the server has to send back not only the link to the html file but also the JavaScript file that makes the html appear properly.

b. The responses from the server
   From the get request the server sends back the location of the JavaScript file which can be located at https://localledge.com/analytics/ga.js. This means the host machine must now send a request to the server asking for that file from localledge.com.

c. The HTTP response codes used in the interaction and what they mean (look them up yourself on the Web)
   In my Follow TCP Stream the response code from the http is "Http 1.1 301 Moved Permanently". This means that the requested data has been moved to a new link permanently. The new link can be found in the location header which states that the new link is https://localledge.com/analytics/ga.js.