

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

```
C:\Windows\system32\cmd.exe

C:\Users\duggac27>ipconfig /all

Windows IP Configuration

Host Name . . . . . : L101-18
Primary Dns Suffix . . . . . : winlabs.computing.dcu.ie
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : winlabs.computing.dcu.ie
                                  computing.dcu.ie

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : computing.dcu.ie
    Description . . . . . : Intel(R) Ethernet Connection (5) I219-U
    Physical Address. . . . . : 50-9A-4C-3D-93-33
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::a5ba:380:455f:cf12%13(Preferred)
    IPv4 Address. . . . . : 136.206.10.168(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 03 April 2018 15:05:53
    Lease Expires . . . . . : 04 April 2018 16:05:58
    Default Gateway . . . . . : 136.206.10.254
    DHCP Server . . . . . : 136.206.217.76
    DHCPv6 IAID . . . . . : 273717836
    DHCPv6 Client DUID. . . . . : 00-01-00-01-22-39-CF-C4-50-9A-4C-3D-93-33

    DNS Servers . . . . . : 136.206.217.50
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.computing.dcu.ie:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : computing.dcu.ie
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 11:

    Connection-specific DNS Suffix  . : computing.dcu.ie
    Description . . . . . : Microsoft 6to4 Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2002:88ce:aa8::88ce:aa8(Preferred)
    Default Gateway . . . . . :
    DNS Servers . . . . . : 136.206.217.50
    NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . : Microsoft Teredo Tunneling Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

C:\Users\duggac27>_
```

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	136.206.10.168	136.206.217.76	DHCP	342	DHCP Release - Transaction ID 0x2940ed62
2	1.067935	Dell_3d:92:44	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.208
3	4.334464	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.168? Tell 136.206.10.254
4	5.026611	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.168? Tell 136.206.10.254
5	5.123477	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x52b0d02c
6	5.407498	136.206.10.254	136.206.10.168	DHCP	411	DHCP Offer - Transaction ID 0x52b0d02c
7	5.407736	0.0.0.0	255.255.255.255	DHCP	377	DHCP Request - Transaction ID 0x52b0d02c
8	5.430185	136.206.10.254	136.206.10.168	DHCP	411	DHCP Offer - Transaction ID 0x52b0d02c
9	5.989544	136.206.10.254	136.206.10.168	DHCP	411	DHCP ACK - Transaction ID 0x52b0d02c
10	6.000577	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
11	6.003159	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
12	6.017289	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.168? Tell 0.0.0.0
13	6.018093	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
14	6.026172	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
15	6.131572	Dell_a5:4e:d0	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.50
16	6.452098	136.206.10.210	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x2039f8bd
17	6.518203	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
18	6.525638	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
19	7.015903	Dell_3d:93:33	Broadcast	ARP	42	Who has 169.254.207.18? Tell 0.0.0.0
20	7.015925	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.168? Tell 0.0.0.0
21	8.014204	Dell_3d:93:33	Broadcast	ARP	42	Who has 169.254.207.18? Tell 0.0.0.0
22	8.014230	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.168? Tell 0.0.0.0
23	9.012566	Dell_3d:93:33	Broadcast	ARP	42	Who has 169.254.207.18? Tell 0.0.0.0
24	9.012577	Dell_3d:93:33	Broadcast	ARP	42	Gratuitous ARP for 136.206.10.168 (Request)
25	9.014088	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
26	9.016887	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
27	9.020201	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
28	9.028742	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
29	9.044694	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
30	9.050508	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
31	9.131091	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
32	9.139310	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
33	9.155517	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
34	9.161517	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
35	9.363331	Dell_3d:93:33	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.168
36	9.370882	JuniperN_92:85:00	Dell_3d:93:33	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
37	11.743419	136.206.10.168	136.206.217.76	DHCP	342	DHCP Release - Transaction ID 0x43af823f
38	13.230364	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.168? Tell 136.206.10.254

Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
 Ethernet II, Src: Dell_3d:93:33 (50:9a:4c:3d:93:33), Dst: JuniperN_92:85:00 (ec:13:db:92:85:00)
 Internet Protocol Version 4, Src: 136.206.10.168, Dst: 136.206.217.76
 User Datagram Protocol, Src Port: 68, Dst Port: 67
 Bootstrap Protocol (Release)

0000 ec 13 db 92 85 00 50 9a 4c 3d 93 33 08 00 45 00P. L=3..E.

wireshark_09347862-8E2D-4DC6-8FC3-3C6AFC9950EB_20180403190753_a02944 | Packets: 38 · Displayed: 38 (100.0%) | Profile: Default

Packet numbers relevant to the DHCP interaction:

- DHCP DISCOVER – Packet 5
- DHCP OFFER – Packet 6
- DHCP Request – Packet 7
- DHCP Acknowledgement – Packets 9
- DHCP Release (if you release using `ipconfig /release`) – Packet 1, 37
- All ARP packets used – Packets 1-4, 10-15, 17-35, 38

Function of each packet

- 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 from 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.

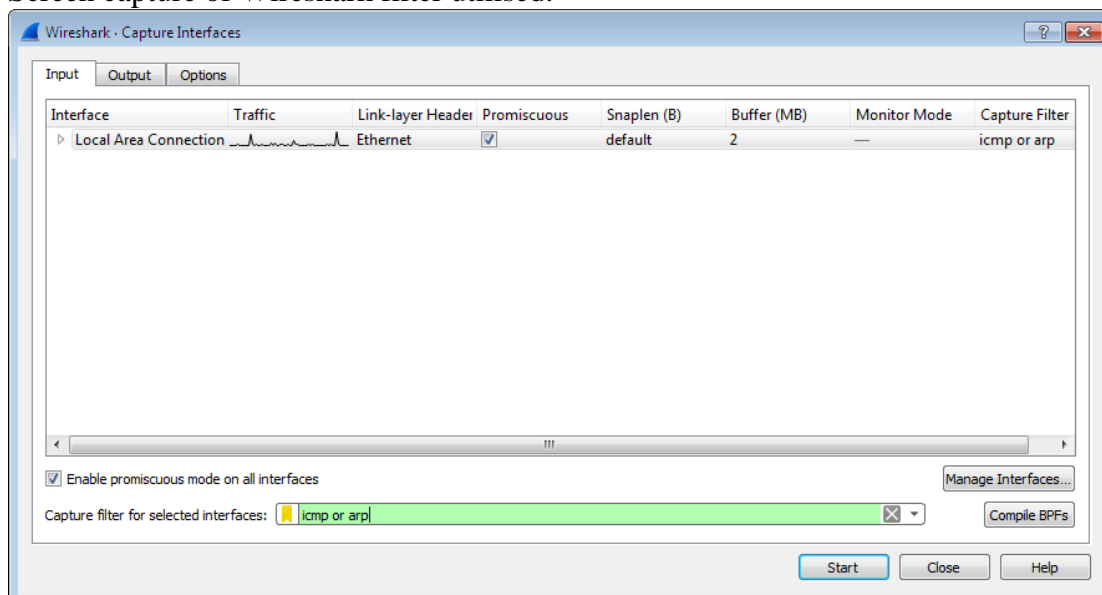
Part 2: *ping traffic*

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

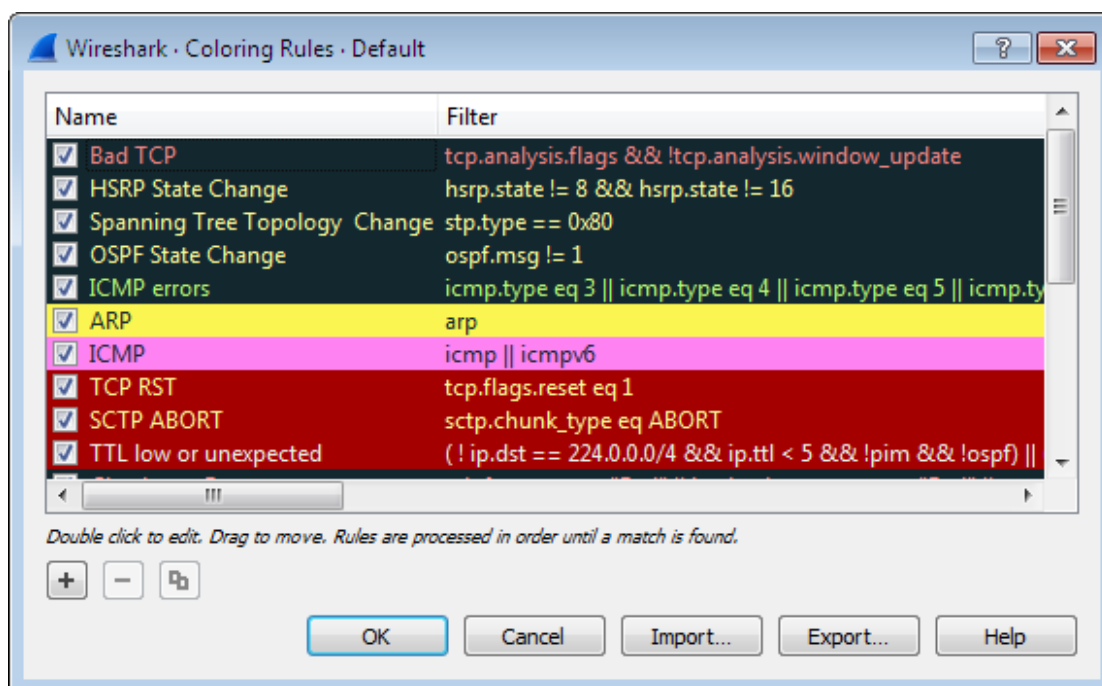
136.206.10.168

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.192? Tell 136.206.10.254
2	0.899852	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.192? Tell 136.206.10.254
3	1.699795	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.192? Tell 136.206.10.254
4	2.599745	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.192? Tell 136.206.10.254
5	3.507629	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.192? Tell 136.206.10.254
6	5.831963	136.206.10.168	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 7)
7	5.834476	52.31.60.123	136.206.10.168	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=46 (request in 6)
8	6.835532	136.206.10.168	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 9)
9	6.837537	52.31.60.123	136.206.10.168	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=46 (request in 8)
10	7.833831	136.206.10.168	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 11)
11	7.835787	52.31.60.123	136.206.10.168	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=46 (request in 10)
12	8.833154	136.206.10.168	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 13)
13	8.835074	52.31.60.123	136.206.10.168	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=46 (request in 12)
14	13.924943	Dell_3d:8f:6e	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.154
15	13.965455	Dell_a5:4c:a8	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.34
16	17.375253	Dell_3d:8e:73	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.153
17	26.025917	Dell_3d:8e:10	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.171
18	26.808429	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.29? Tell 136.206.10.254

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: JuniperN_92:85:00 (ec:13:db:92:85:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

0000 ff ff ff ff ff ff ec 13 db 92 85 00 00 06 00 01

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)

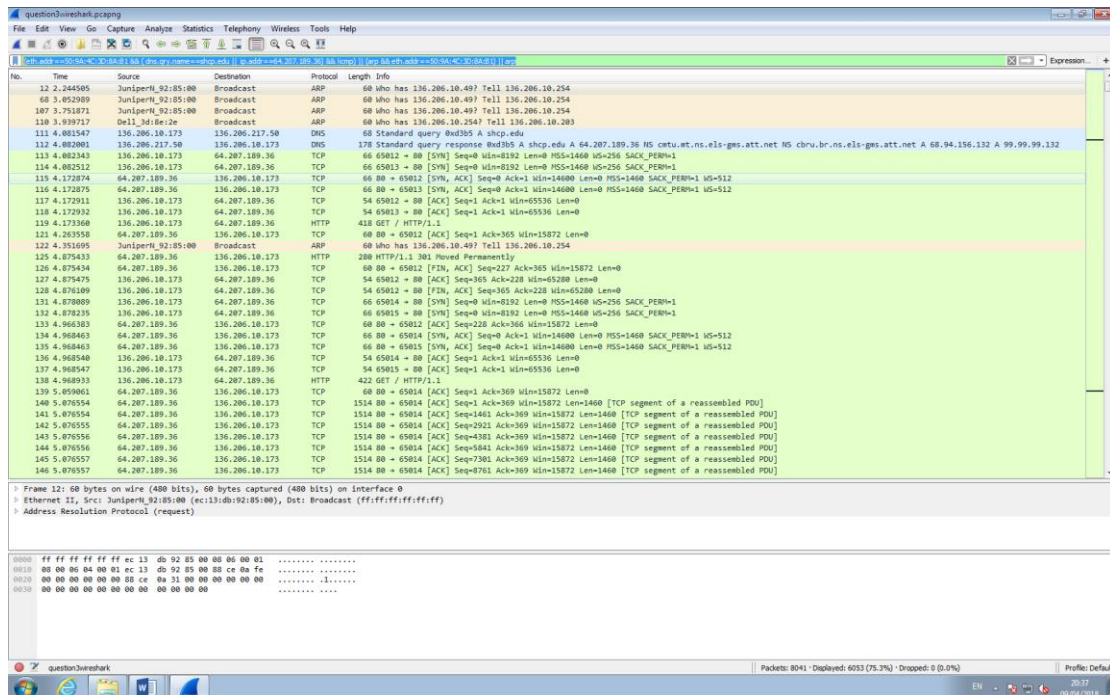
136.206.10.173

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

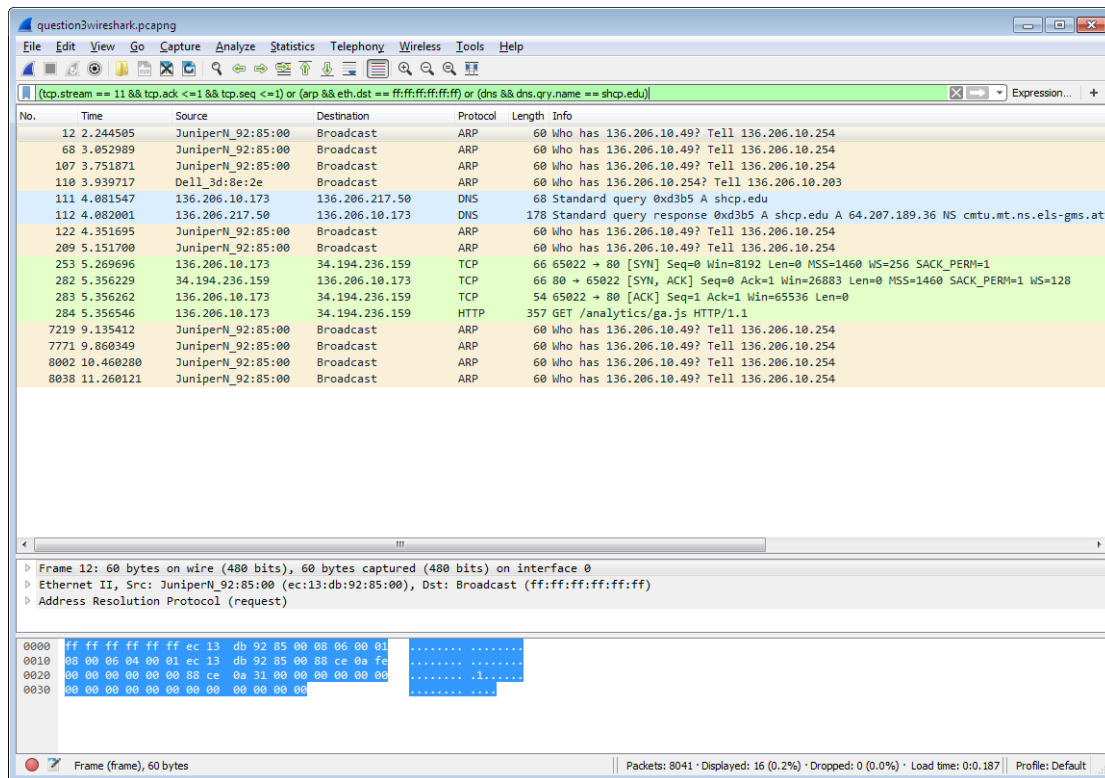


Explain how you found the start of the interaction between your PC and the website.

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.

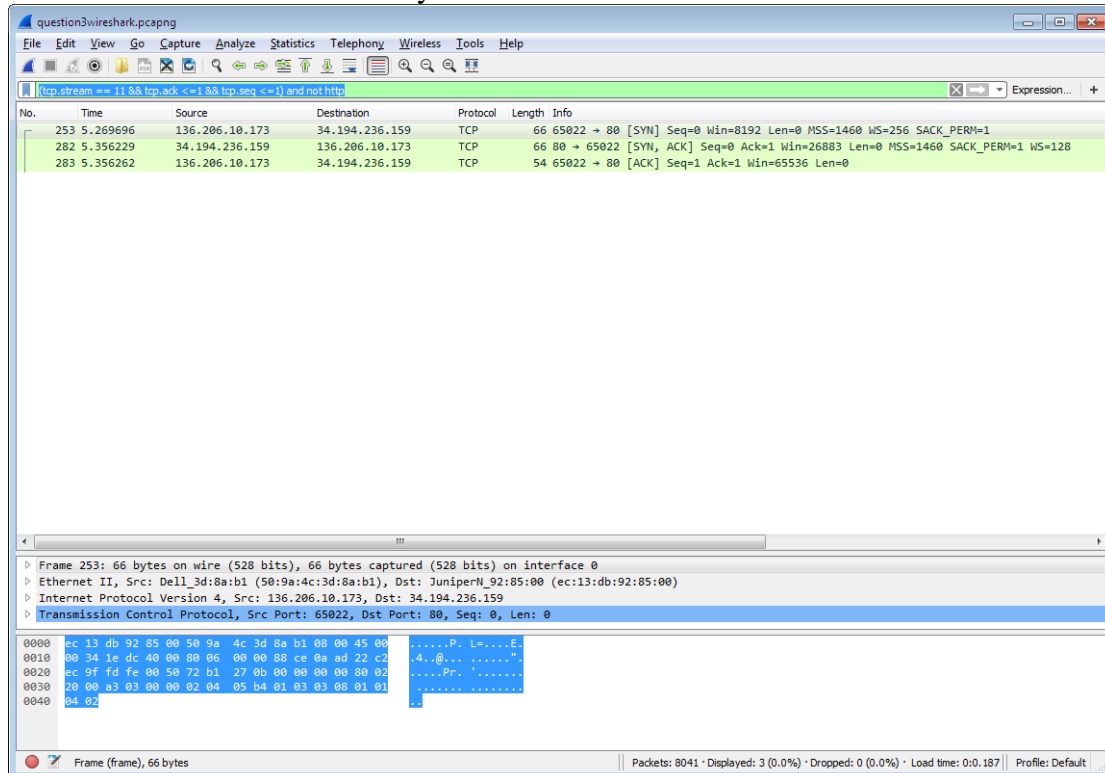
Packet 283:

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.

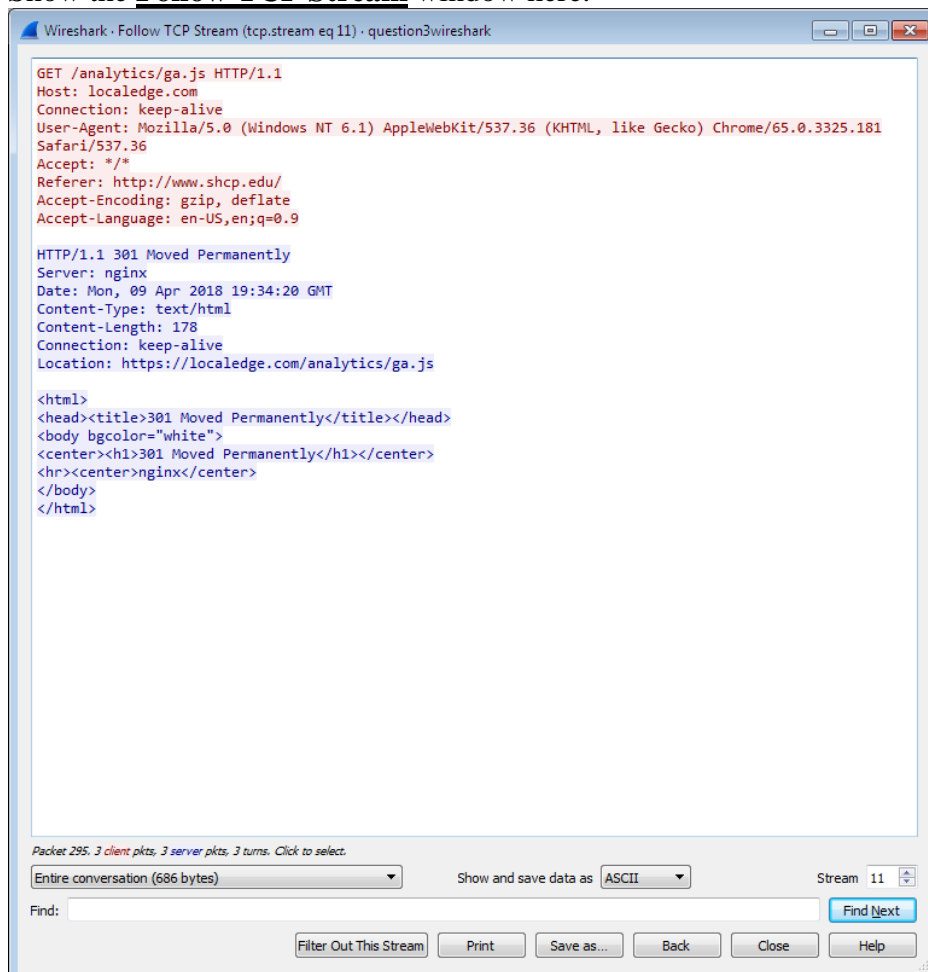
Write down a filter to show only these three-way-handshake packets

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 stream 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>.