

## **CA169 Networks Assignment Two**

### **Answer Sheets**

STUDENT NAME:	Muhammad Umar
STUDENT NUMBER:	17313893
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)

136.206.10.200

50-9A-4C-3D-89-B7

Screen capture: ipconfig information cmd window

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

C:\Users\unerm2>ipconfig /all

Windows IP Configuration

Host Name . . . . . : L101-50
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-89-B7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::84fd:91fd:e8f7:84dd%13(Preferred)
IPv4 Address. . . . . : 136.206.10.200(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 03 April 2018 11:59:44
Lease Expires . . . . . : 04 April 2018 12:59:43
Default Gateway . . . . . : 136.206.10.254
DHCP Server . . . . . : 136.206.217.76
DHCPv6 IAID . . . . . : 273717836
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-39-D6-F3-50-9A-4C-3D-89-B7
DNS Servers . . . . . : 136.206.217.50
NetBIOS over Tcpip. . . . . : Enabled
```

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

No.	Time	Source	Destination	Protocol	Length	Info
168	7.275093	Dell_3d:87:f1	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.199
170	7.673500	Dell_3d:85:dd	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.165
176	8.447825	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0x7f87a49
179	8.724430	136.206.10.254	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x7f87a49
184	9.724981	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8237c875
185	9.959598	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0xa2be1504
187	10.432831	Dell_3d:8e:2e	Broadcast	ARP	60	Who has 136.206.10.203? Tell 0.0.0.0
197	10.632343	Dell_3d:8e:2e	Broadcast	ARP	60	Who has 136.206.10.203? Tell 0.0.0.0
199	10.832743	Dell_3d:8e:2e	Broadcast	ARP	60	Who has 136.206.10.203? Tell 0.0.0.0
205	11.548157	Dell_3d:8e:2e	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.203
226	13.678861	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.10.40? Tell 136.206.10.254
227	13.761360	136.206.10.189	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x2ad854ae
242	16.192706	136.206.10.200	136.206.217.76	DHCP	342	DHCP Release - Transaction ID 0x7ad5e593
302	16.296720	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0x12a11e62
304	16.336765	Dell_3d:85:f6	Broadcast	ARP	60	Who has 136.206.10.213? Tell 0.0.0.0
308	16.536301	Dell_3d:85:f6	Broadcast	ARP	60	Who has 136.206.10.213? Tell 0.0.0.0
313	16.736772	Dell_3d:85:f6	Broadcast	ARP	60	Who has 136.206.10.213? Tell 0.0.0.0
336	17.410947	Dell_3d:85:f6	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.213
402	23.170879	Dell_3d:89:b7	Broadcast	ARP	42	Who has 169.254.132.221? Tell 0.0.0.0
411	24.168381	Dell_3d:89:b7	Broadcast	ARP	42	Who has 169.254.132.221? Tell 0.0.0.0
427	25.167693	Dell_3d:89:b7	Broadcast	ARP	42	Who has 169.254.132.221? Tell 0.0.0.0
447	26.166031	Dell_3d:89:b7	Broadcast	ARP	42	Gratuitous ARP for 169.254.132.221 (Request)
483	27.174405	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x564847
496	27.407560	136.206.10.254	136.206.10.200	DHCP	411	DHCP Offer - Transaction ID 0x564847
497	27.407760	0.0.0.0	255.255.255.255	DHCP	377	DHCP Request - Transaction ID 0x564847
509	27.091580	136.206.10.254	136.206.10.200	DHCP	411	DHCP ACK - Transaction ID 0x564847
515	27.902758	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
516	27.909960	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
540	27.922591	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
541	27.922828	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
556	28.169872	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.200? Tell 0.0.0.0
588	29.169169	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.200? Tell 0.0.0.0
734	30.161894	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.200? Tell 0.0.0.0
756	31.170403	Dell_3d:89:b7	Broadcast	ARP	42	Gratuitous ARP for 136.206.10.200 (Request)
757	31.173397	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
764	31.182831	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
765	31.183023	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
766	31.183192	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
779	31.616127	136.206.10.200	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6c4afa8e
784	31.630095	136.206.217.76	136.206.10.200	DHCP	342	DHCP ACK - Transaction ID 0x6c4afa8e
796	31.640766	136.206.217.76	136.206.10.200	DHCP	342	DHCP ACK - Transaction ID 0x6c4afa8e
833	31.060595	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
834	31.065533	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
835	31.075581	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
836	31.083749	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
867	32.402622	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
870	32.403486	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
872	32.421718	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
873	32.422910	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
1099	36.060464	Dell_3d:89:b7	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.6
1110	37.045520	Dell_3d:89:b7	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.200
1112	37.077802	JuniperN_92:85:00	Dell_3d:89:b7	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
1164	38.543022	Dell_3d:8d:a5	Broadcast	ARP	60	Who has 136.206.10.254? Tell 136.206.10.188

Packet numbers relevant to the DHCP interaction:

- a. DHCP DISCOVER (184, 483)
- b. DHCP OFFER (496)
- c. DHCP Request (176, 185, 302, 497)
- d. DHCP Acknowledgement (509, 784, 796)
- e. DHCP Release (if you release using `ipconfig /release`) (242)
- f. All ARP packets used (160, 170, 187, 197, 199, 205, 226, 304, 308, 313, 336, 402, 411, 427, 447, 515, 516, 540, 541, 556, 588, 734, 756, 757, 764, 765, 766, 833, 834, 835, 836, 867, 870, 872, 873, 1099, 1110, 1112, 1164)

Function of each packet:

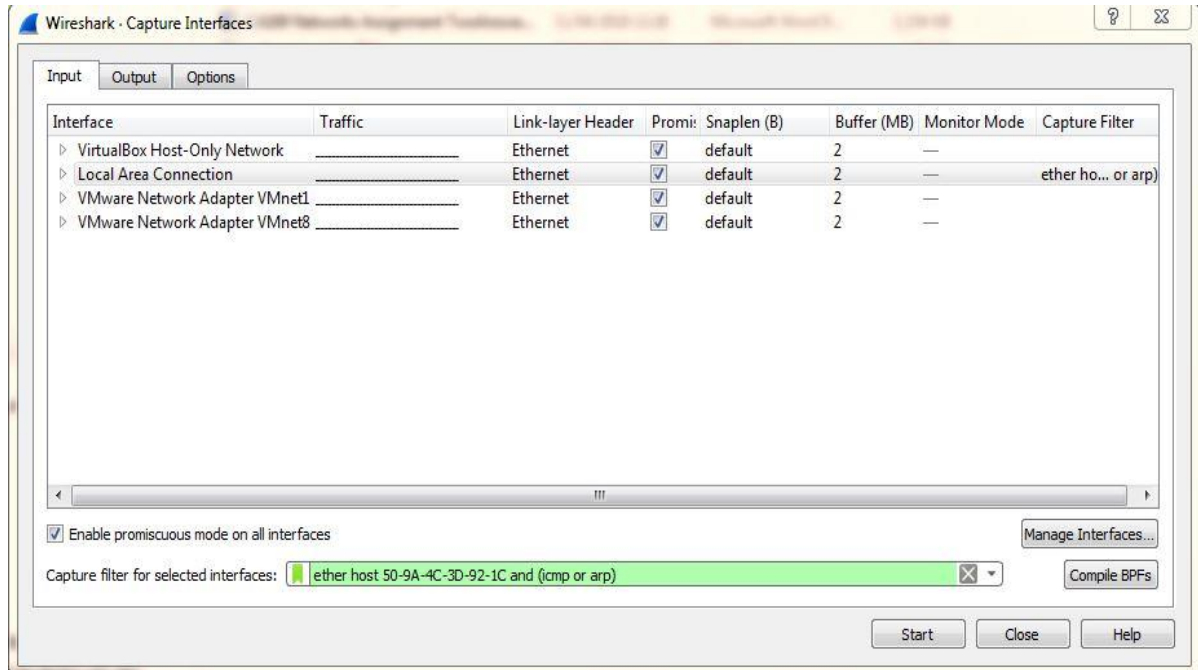
- a. DHCP DISCOVER: This packet is broadcasted to request IP address info from a DHCP server, when a DHCP client computer tries to log on to some network for the first time.
- b. DHCP OFFER: When a DHCP server receives a client's DHCP Discover packet, it responds it with a DHCP Offer Packet which contains an IP address and all the additional info related to TCP/IP config info, e.g. subnet mask, etc. A DHCP Offer packet can be generated by many DHCP servers but client accepts the DHCP Offer packet that arrives first.
- c. DHCP Request: This packet is broadcasted in response to the DHCP Offer packet which the client has received. This packet carries the info of the IP address that client received in the DHCP Offer packet and displays its acceptance.
- d. DHCP Acknowledgement: This packet tells the client that the DHCP request it sent for the IP address and it has been acknowledged by the DHCP server.
- e. DHCP Release (if you release using `ipconfig /release`): This packet is sent to the DHCP server by the DHCP client to release the IP address.
- f. ARP: The ARP (address resolution protocol) maps the IP network addresses it gets to the hardware addresses with the help of data link protocol.

## Part 2: ping traffic

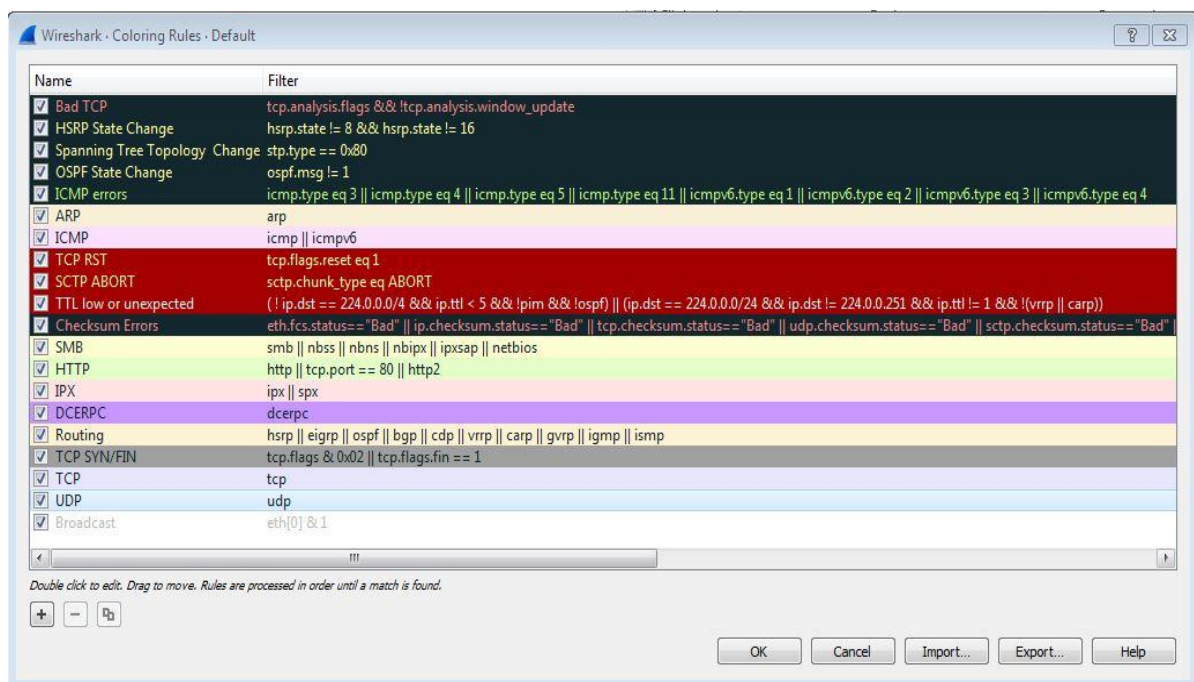
Your IP & MAC address for this experiment (use ipconfig)

136.206.10.216	50-9A-4C-3D-92-1C
----------------	-------------------

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.

- I pinged [www.dcu.ie](http://www.dcu.ie) to generate traffic which included ARP and ICMP traffic.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_3d:92:1c	Broadcast	ARP	42	Who has 136.206.10.254? Tell 136.206.10.216
2	0.003324	JuniperW_92:85:00	Dell_3d:92:1c	ARP	60	136.206.10.254 is at ec:13:db:92:85:00
3	3.911619	136.206.10.216	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 4)
4	3.913430	52.31.60.123	136.206.10.216	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=46 (request in 3)
5	4.927166	136.206.10.216	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 6)
6	4.929078	52.31.60.123	136.206.10.216	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=46 (request in 5)
7	5.941149	136.206.10.216	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 8)
8	5.942983	52.31.60.123	136.206.10.216	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=46 (request in 7)
9	6.955055	136.206.10.216	52.31.60.123	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (no response found!)
10	6.956875	52.31.60.123	136.206.10.216	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=46 (request in 9)

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 Ethernet II, Src: Dell\_3d:92:1c (50:9a:4c:3d:92:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Address Resolution Protocol (request)

0000 ff ff ff ff ff 50 9a 4c 3d 92 1c 08 06 00 01 .....P. Lw.....

Local Area Connection: <live capture in progress> | Packets: 10 · Displayed: 10 (100.0%) | Profile: Default

Packet numbers relevant to the experiment:

- Packets 1-10 are relevant to this experiment.

Explanation for each packet

- **Packet 1** is an ARP packet (length 42 bytes), which broadcasts itself through the network from the host machine, trying to figure out which machine has IP address 136.206.17.254 (this is the router). MAC address of the router (136.206.17.254) is needed to build/start communication between the host machine and the router.
- **Packet 2** is an ARP packet (length 60 bytes), which is reply sent by the router (136.206.17.254) in response the ARP request (**Packet 1**). This reply contains the router's MAC address which will allow the host machine and the machine to which the ARP request was sent to, in this case router, communicate with each other.
- **Packet 3** is an ICMP Echo Request packet (length 74 bytes) is generated when [www.dcu.ie](http://www.dcu.ie) is pinged just to check the if both machine are communicating with each other. This is the initial ICMP Echo Request contains the destination address where this packet is meant to go next, router in this case and also the IP address of the DCU website that I pinged is contained in this packet. This packet also has a TTL which translates to Time To Live attached to it and it makes sure that the packet is not stuck in any kind of loop. As this packet moves along different router the TTL value gets smaller and if it reaches zero, the packet is rejected which usually means that the packet couldn't reach its destination. It carries the mac address of the source which is contained in the Ether layer and it also carries the source IP address which is contained in the IP layer. Data relevant to this ICMP packet is also contained within.

- **Packet 4** is an ICMP Echo Reply packet (length 74 bytes) is sent back from the [www.dcu.ie](http://www.dcu.ie) (52.31.60.123) in response to the packet 3 we sent earlier. This ICMP Echo Reply packet tells the host that target (DCU) is ready to communicate with host. This packet is usually containing ASCII characters. This packet may carry the timestamp showing time of the transmission which lets ping calculate the round-trip-time in a stateless way and there is no need to calculate the transmission time for each packet.
- The process done for the ICMP Echo Request in **Packet 3** is repeated in **Packet 5, 7 and 9**.
- The process done for the ICMP Echo Request in **Packet 3** is repeated in **Packet 5, 7 and 9**.
- The repetition of these **Packet 3 and 5** is required in order to get some information on how the Round-Trip time of the connection, the max and min time the packets took and the average of those times, the amounts of packets lost during this process.



### 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	tcp.stream eq 4 or dns contains "computing" or arp
--------	--

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

- I found the start of the interaction by loading up Wireshark and start capturing then load the page in chrome whose data I want to capture then I stop the capture. I used the filter *dns contains "computing"* in order to see DNS queries for [www.computing.dcu.ie](http://www.computing.dcu.ie) (the website I went to while capturing). I found the 3-way-handshake packets by using the filter. I pressed right click on one of the three handshake packets and in the option follow I chose TCP stream which gave us information on all the traffic regarding to the website and the test-machine.

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

The image shows a Wireshark packet capture window with the filter 'tcp.stream eq 4 or dns contains "computing" or arp'. The packet list shows several packets, with packets 71, 77, and 78 highlighted. Packet 71 is a SYN packet from the host to the server. Packet 77 is a SYN/ACK packet from the server to the host. Packet 78 is an ACK packet from the host to the server. The packet details pane shows the structure of these packets, including the Ethernet II, Internet Protocol, and TCP/UDP headers.

No.	Time	Source	Destination	Protocol	Length	Info
32	3.385847	0e11:95:66:66	Broadcast	ARP	68	Who has 136.206.10.254? Tell 136.206.10.14
47	3.974146	136.206.10.174	136.206.217.50	DNS	80	Standard query 0x0e97 A www.computing.dcu.ie
48	3.974456	136.206.217.50	136.206.10.174	DNS	184	Standard query response 0x0e97 A www.computing.dcu.ie CNAME ossa2.computing.dcu.ie A 136.206.217.25 NS ns2.computing.dcu.ie NS ns1.computing.dcu.ie A 136.206.217.25
71	4.003670	136.206.10.174	136.206.217.25	TCP	66	65409 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=0 SACK_PERM=1
77	4.003884	136.206.217.25	136.206.10.174	TCP	66	80 → 65409 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
78	4.003889	136.206.10.174	136.206.217.25	TCP	54	65409 → 80 [ACK] Seq=1 Ack=1 Win=0 Len=0
307	4.337597	136.206.10.174	136.206.217.25	HTTP	564	GET /modules/system/system.css?3 HTTP/1.1
330	4.337884	136.206.217.25	136.206.10.174	TCP	60	80 → 65409 [ACK] Seq=1 Ack=511 Win=30536 Len=0
529	4.426197	0e11:95:66:66	Broadcast	ARP	68	Who has 136.206.10.254? Tell 136.206.10.14

Write down the numbers of the packets with the 3-way handshake.

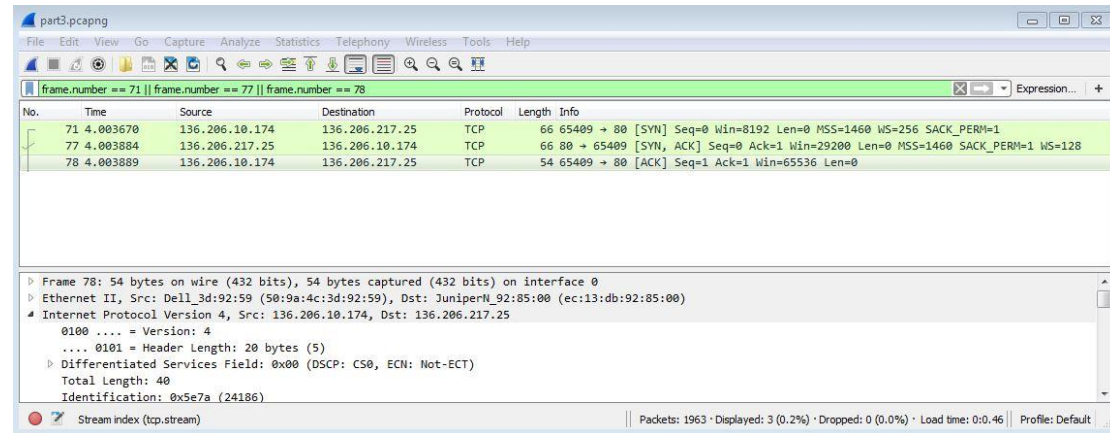
Explain what is happening with these 3 packets.

- Packet 71** is called a **SYN** packet which the server receives from the host machine to make sure that the server is ready and open for any new connections the host machine wants to make.
- Packet 77** is called a **SYN/ACK** packet which is replied by the server to the host machine to let it know that it has acknowledged the **SYN** packet it sent and the server now is ready to make connections with the host machine.
- Packet 78** is called a **ACK** packet which is replied by the host machine to the server to let it know that it has seen the **SYN/ACK** packet it sent previously and has established a connection between the two machines.

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

Filter	frame.number == 71    frame.number == 77    frame.number == 78
--------	--

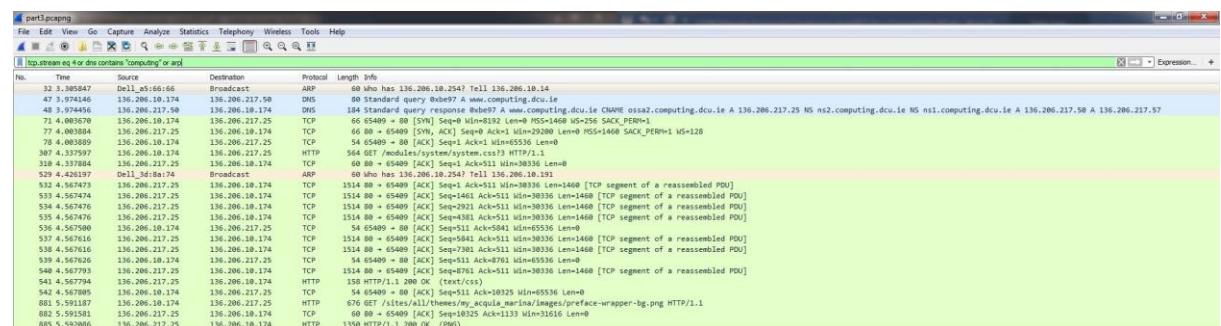
Wireshark window for the 3-way-handshake



Show the Follow TCP Stream window here.



Your notes on...



a. The GET requests made:

The GET requests (packet 307 and 881) made by my machine which can be seen in the picture above. These requests are sent to the server in order to grab the files from the server that the host machine sent the GET request for.



- b. The responses from the server

The responses I got were called HTTP/1.1 200 OK (packet 541 and 885) which can be seen in the picture above. These packets were sent in response to the GET requests made by the host machine.

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

I received two **HTTP/1.1 200 OK** one for (text/css) and the other one for (PNG) which are telling the host machine that those files are sent successfully and connections is successful.