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

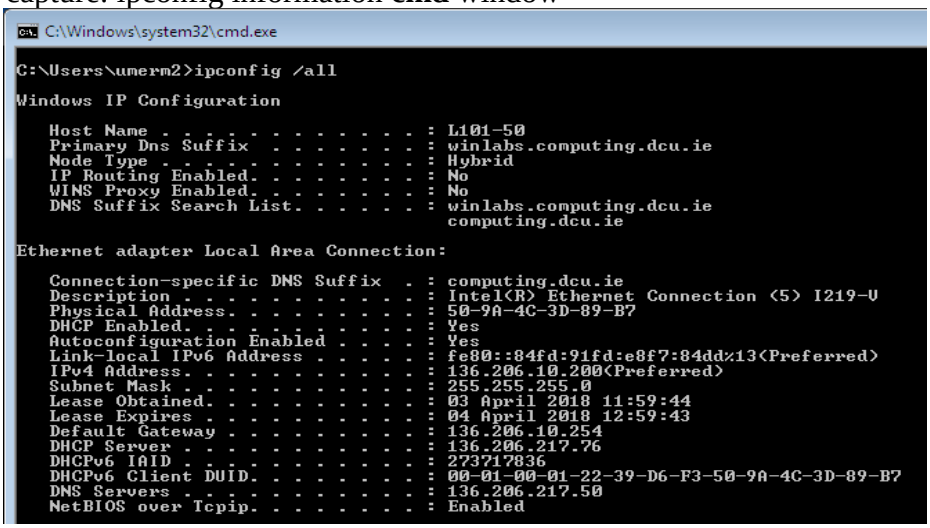
In submitting this project, I declare that the project material, which I now submit, is my own work. Any assistance received by way of borrowing from the work of others has been cited and acknowledged within the work. I make this declaration in the knowledge that a breach of the rules pertaining to project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

Part 1: DHCP traffic

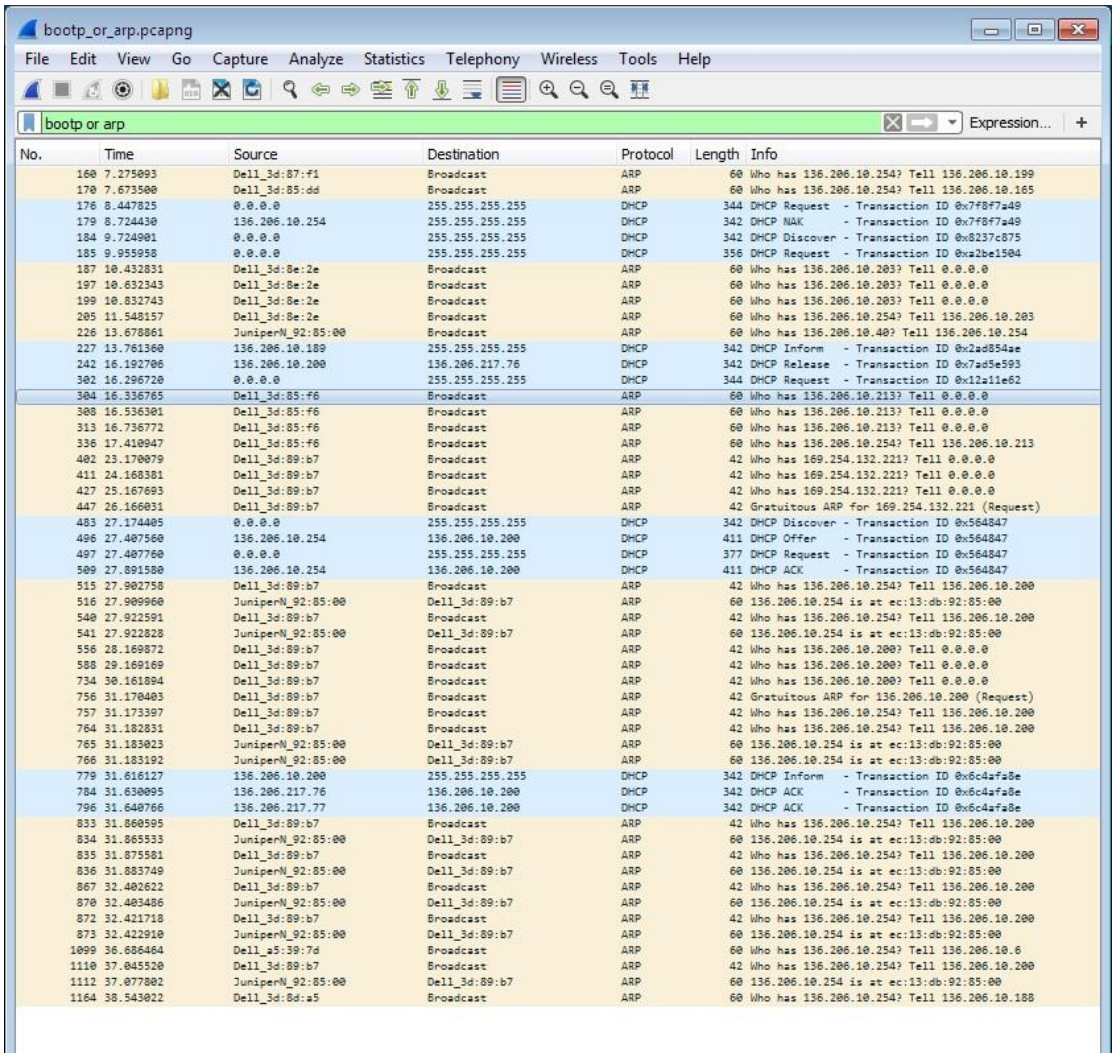
Your IP & MAC address for this experiment (use ipconfig)

136.206.10.200	50-9A-4C-3D-89-B7

Screen capture: ipconfig information **cmd** window



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



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:

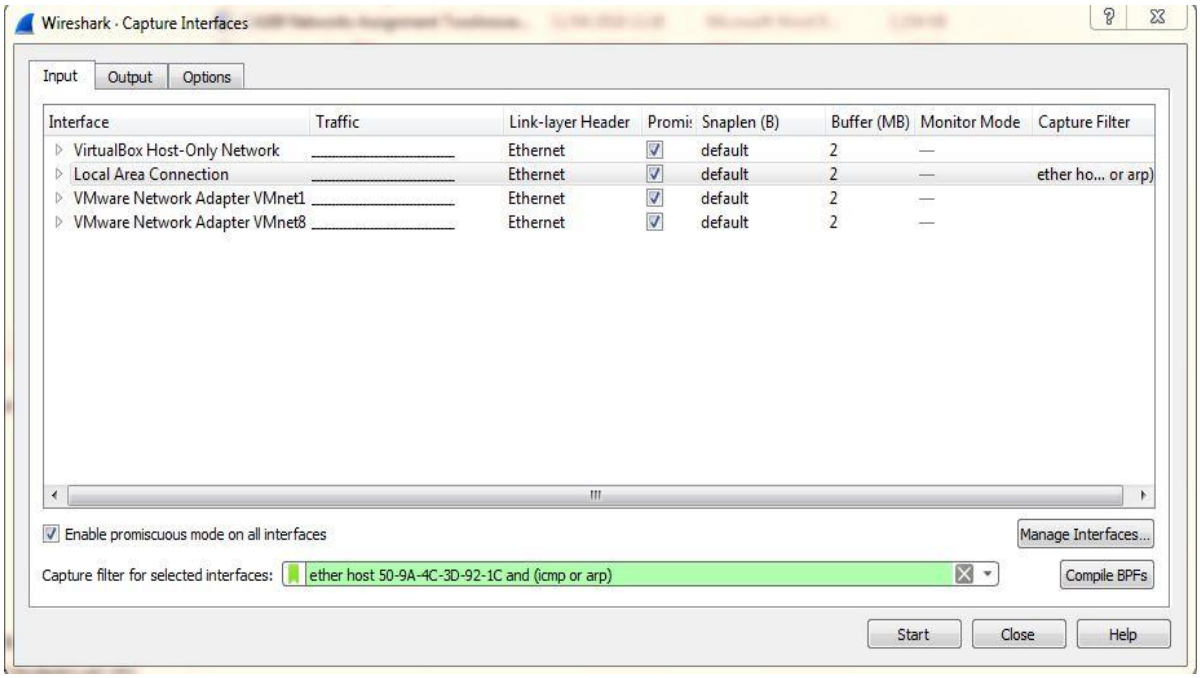
a. DHCP DISCOVER: This packet is broadcasted to request IP address info from a DCHP server, when a DCHP client computer tries to log on to some network for the first time.
b. DHCP OFFER: When a DCHP server receives a client's DCHP Discover packet, it responds it with a DCHP Offer Packet which contains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

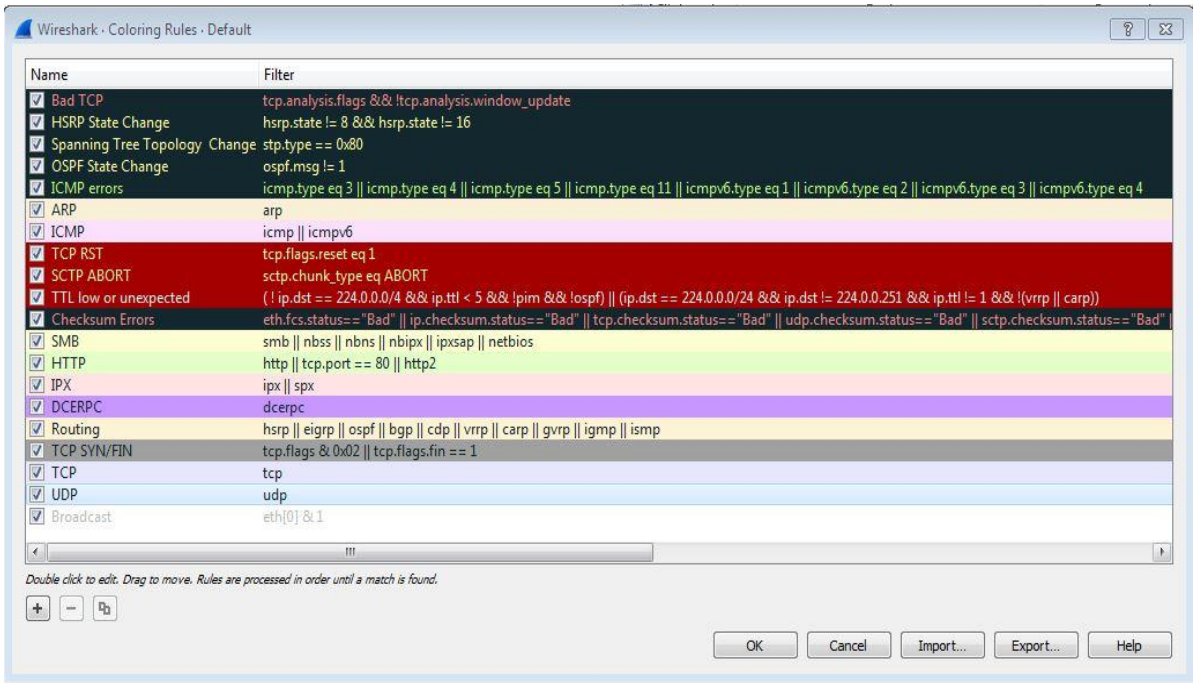
Your IP & MAC address for this experiment (use ipconfig)

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

Screen capture of Wireshark filter utilised.

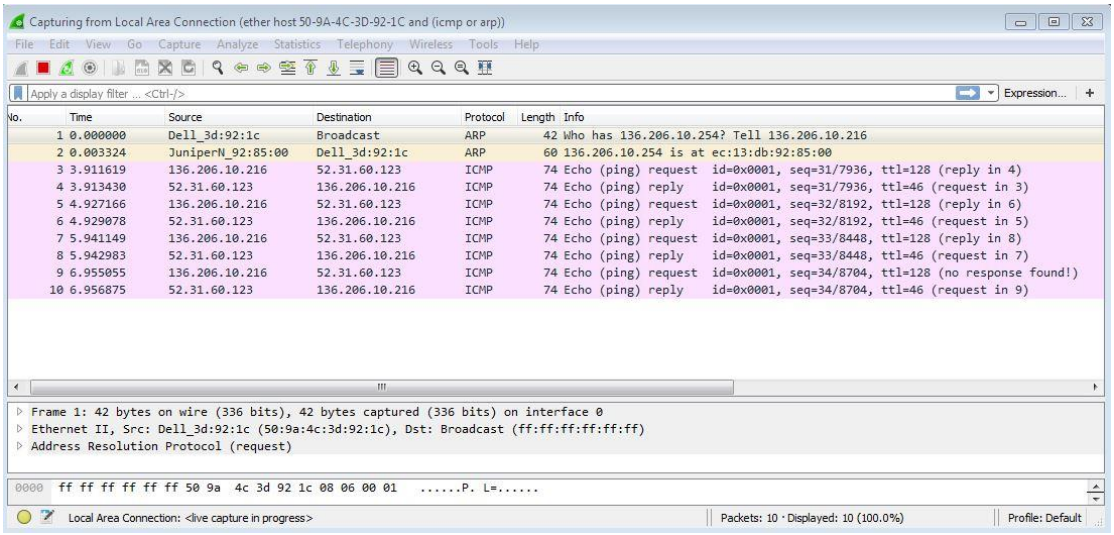


Screen capture of Wireshark colouring rules applied



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

- I pinged www.dcu.ie to generate traffic which included ARP and ICMP traffic.



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 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 (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

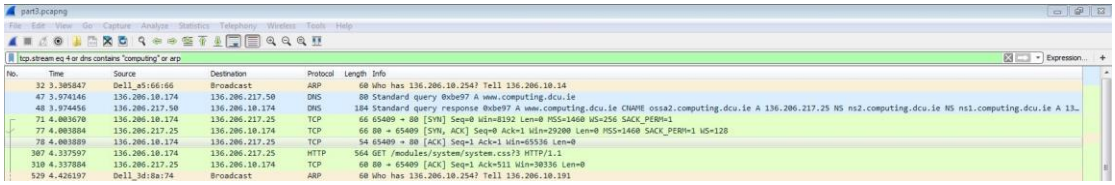
Filter to show only traffic concerning the test machine

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 (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)



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.

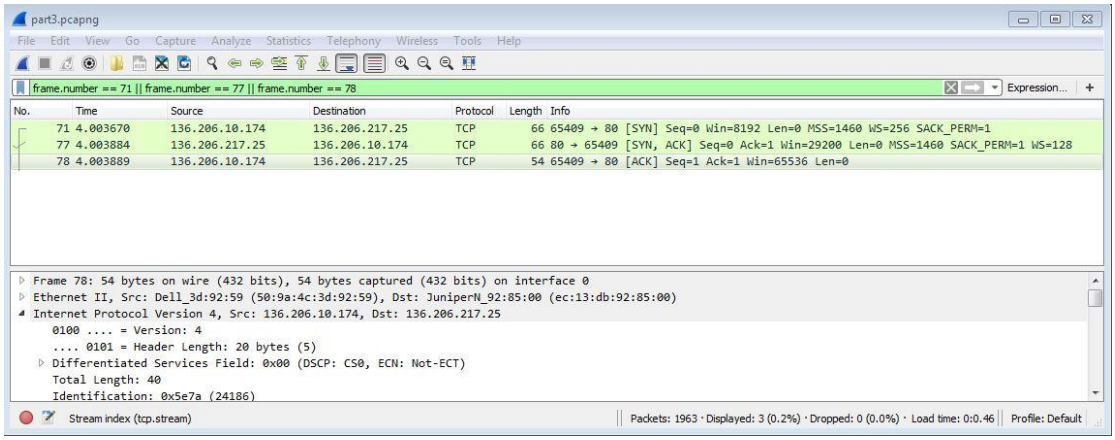
- **Packet 77** is called a **SYN/ACK** packet which is replied by the server to the host machine to let it know that it has acknowledged the **SYN** packet it sent and the server now is ready to make connections with the host machine.

- **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.

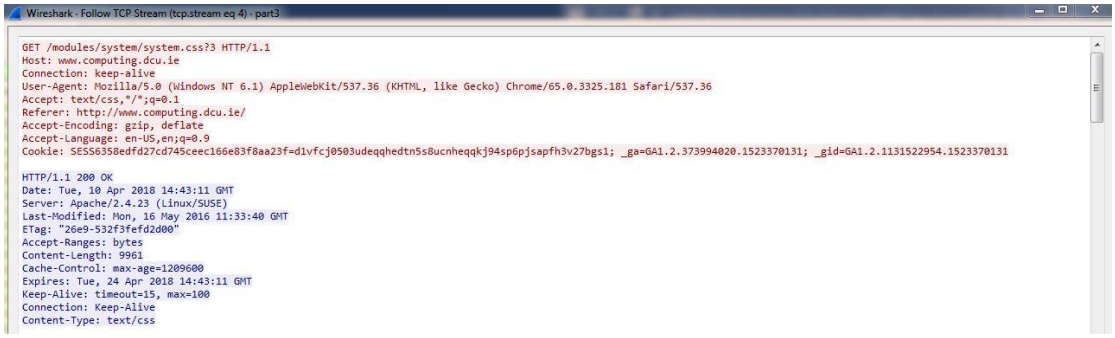
Write down a filter to show only these three-way-handshake packets

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

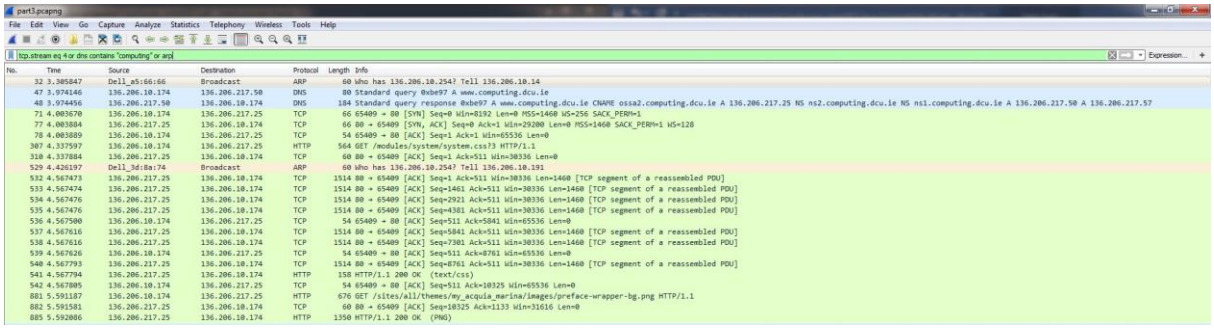
Wireshark window for the 3-way-handshake



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.