

CA169 Networks Assignment Two

Answer Sheets

STUDENT NAME:	Tomas Baltrunas
STUDENT NUMBER:	17350793
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)

136.206.17.177

50-9A-4C-3D-8F-C9

Screen capture: ipconfig information cmd window

```
C:\Windows\system32\cmd.exe
C:\Users\baltrut2>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : LG27-28
    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-8F-C9
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::78f1:7ef8:af41:80c2%13(Preferred)
    IPv4 Address. . . . . : 136.206.17.177(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 29 March 2018 18:14:35
    Lease Expires . . . . . : 30 March 2018 18:14:35
    Default Gateway . . . . . : 136.206.17.254
    DHCP Server . . . . . : 136.206.217.76
    DHCPv6 IAID . . . . . : 273717836
    DHCPv6 Client DUID. . . . . : 00-01-00-01-22-1C-DB-94-50-9A-4C-3D-8F-C9

    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
11	3.989941	136.206.17.177	136.206.217.76	DHCP	365	DHCP Request - Transaction ID 0xc58ad450
12	4.007648	136.206.217.76	136.206.17.177	DHCP	411	DHCP ACK - Transaction ID 0xc58ad450
15	4.019240	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
24	4.024294	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
92	7.359989	136.206.17.177	136.206.217.76	DHCP	342	DHCP Release - Transaction ID 0x13fe78a5
97	8.333348	JuniperN_92:85:00	Broadcast	ARP	60	Who has 136.206.17.177? Tell 136.206.17.254
98	8.333361	Dell_3d:8f:c9	JuniperN_92:85:00	ARP	42	136.206.17.177 is at 50:9a:4c:3d:8f:c9
165	14.163652	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2e9cff5d
167	14.396203	136.206.17.254	255.255.255.255	DHCP	411	DHCP Offer - Transaction ID 0x2e9cff5d
168	14.396203	136.206.17.254	255.255.255.255	DHCP	411	DHCP Offer - Transaction ID 0x2e9cff5d
169	14.396395	0.0.0.0	255.255.255.255	DHCP	377	DHCP Request - Transaction ID 0x2e9cff5d
176	14.990202	136.206.17.254	255.255.255.255	DHCP	411	DHCP ACK - Transaction ID 0x2e9cff5d
180	15.002440	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
188	15.011650	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
201	15.016777	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
202	15.022735	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
240	15.387542	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.177? Tell 0.0.0.0
244	15.391690	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
245	15.395370	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
271	15.882699	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 169.254.128.194? Tell 0.0.0.0
324	16.379284	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.177? Tell 0.0.0.0
330	16.881401	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 169.254.128.194? Tell 0.0.0.0
359	17.098908	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
360	17.108137	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
379	17.390247	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.177? Tell 0.0.0.0
478	17.892451	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 169.254.128.194? Tell 0.0.0.0
586	18.135411	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
594	18.140432	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
610	18.147603	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
611	18.151050	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
635	18.392406	Dell_3d:8f:c9	Broadcast	ARP	42	Gratuitous ARP for 136.206.17.177 (Request)
638	18.397586	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
639	18.399170	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
643	18.408558	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
644	18.411006	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
645	18.428977	136.206.17.177	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x66643a11
700	18.716851	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
701	18.721105	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
702	18.724498	Dell_3d:8f:c9	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.177
703	18.732253	JuniperN_92:85:00	Dell_3d:8f:c9	ARP	60	136.206.17.254 is at ec:13:db:92:85:00

Header checksum (p.checksum), 2 bytes

Packets: 778 · Displayed: 40 (5.1%) · Load time: 0:0.13 · Profile: Default

Packet numbers relevant to the DHCP interaction:

- DHCP DISCOVER: **165**
- DHCP OFFER: **167, 168**
- DHCP Request: **169**
- DHCP Acknowledgement: **176**
- DHCP Release (if you release using `ipconfig /release`): **92**
- All ARP packets used: **15, 24, 97, 98, 180, 188, 201, 202 ... 702, 703**

Function of each packet

- DHCP DISCOVER: For the client to find a nearby DHCP server and request an IP address lease, by broadcasting to the entire network, with its IP address set to all 0's (no IP)**
- DHCP OFFER: To reserve and offer an IP lease and send additional configuration information to a client that sent a DISCOVER.**
- DHCP Request: For the client to accept and request the offered IP (also sent when renewing a lease)**
- DHCP Acknowledgement: For the server to confirm the client's new IP lease and to send additional configuration details (also a confirmation of lease requests)**

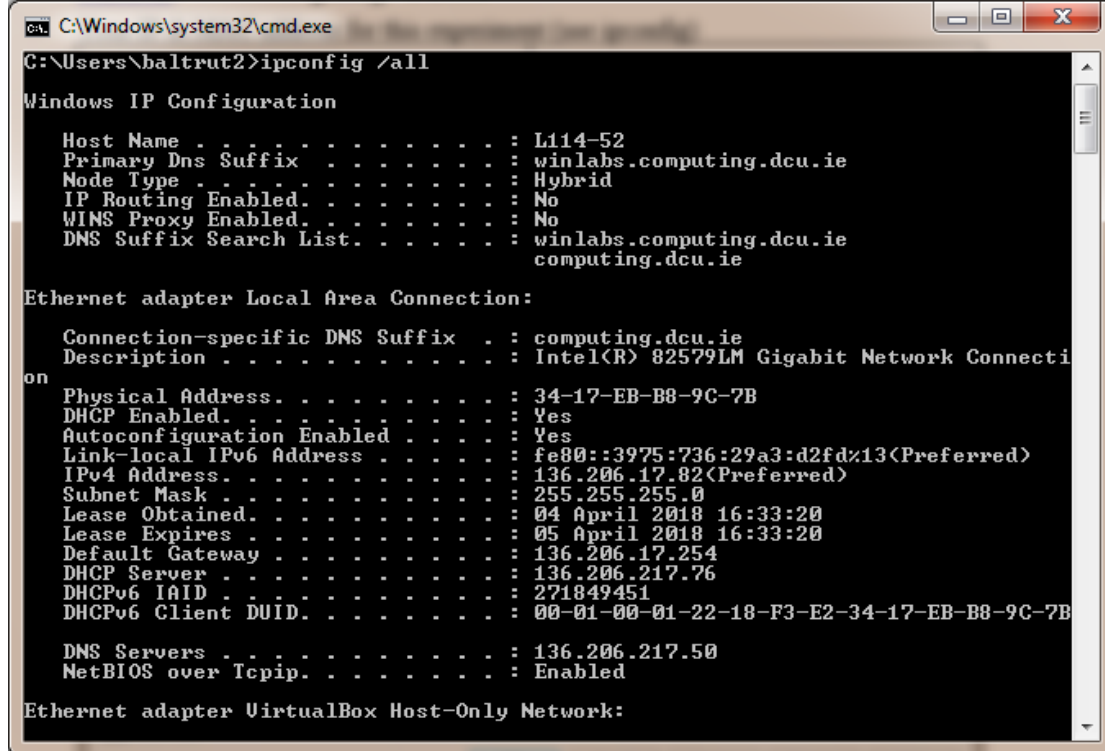
- e. DHCP Release (if you release using `ipconfig /release`): **For the client to announce to the DHCP server that it gives up (releases) its IP lease**
- f. ARP: **Lets computers find each other's MAC addresses from knowing their IP addresses. With this, the client can connect to the DHCP server. The server can check that an IP is not in use. And the client can test that it got the IP assigned correctly.**

Part 2: ping traffic

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

136.206.17.82

34-17-EB-B8-9C-7B



```
C:\Windows\system32\cmd.exe
C:\Users\baltrut2>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : L114-52
    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

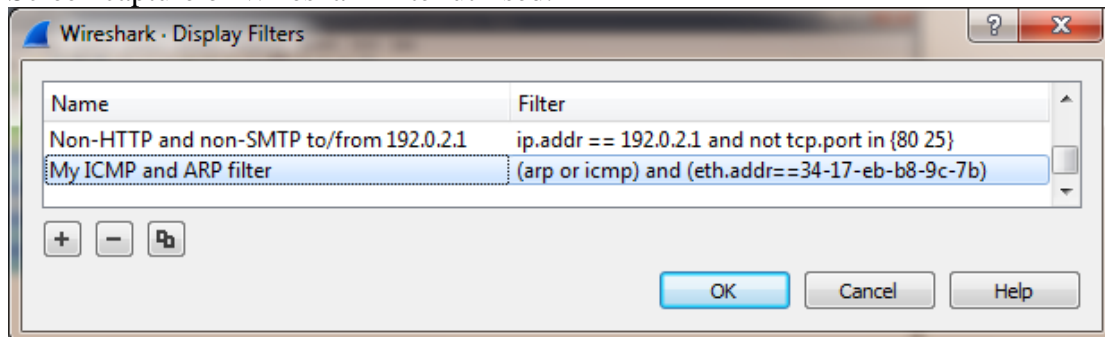
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : computing.dcu.ie
    Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
    Physical Address. . . . . : 34-17-EB-B8-9C-7B
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::3975:736:29a3:d2fd%13(Preferred)
    IPv4 Address. . . . . : 136.206.17.82(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 04 April 2018 16:33:20
    Lease Expires . . . . . : 05 April 2018 16:33:20
    Default Gateway . . . . . : 136.206.17.254
    DHCP Server . . . . . : 136.206.217.76
    DHCPv6 IAID . . . . . : 271849451
    DHCPv6 Client DUID. . . . . : 00-01-00-01-22-18-F3-E2-34-17-EB-B8-9C-7B

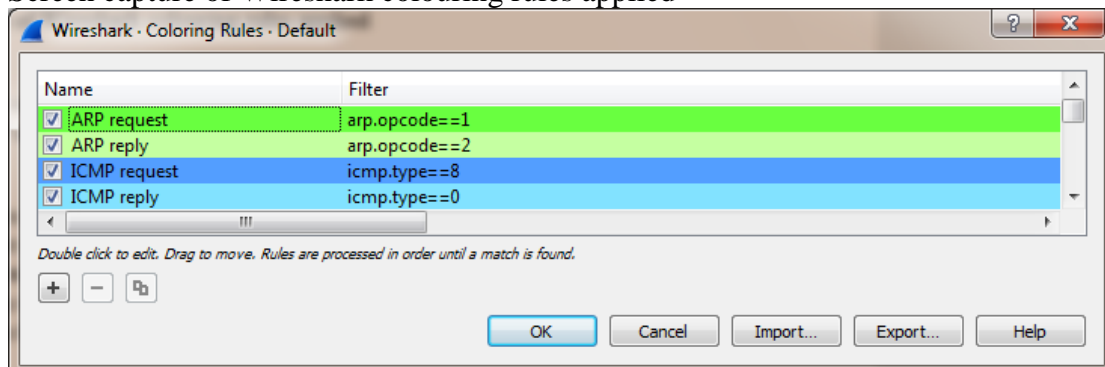
    DNS Servers . . . . . : 136.206.217.50
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VirtualBox Host-Only Network:
```

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
59	22.608958	Dell_b8:9c:7b	Broadcast	ARP	42	Who has 136.206.17.254? Tell 136.206.17.82
60	22.611611	JuniperN_92:85:00	Dell_b8:9c:7b	ARP	60	136.206.17.254 is at ec:13:db:92:85:00
65	22.634507	136.206.17.82	216.58.211.163	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 66)
66	22.635949	216.58.211.163	136.206.17.82	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=128 (request in 65)
67	23.627298	136.206.17.82	216.58.211.163	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128 (reply in 68)
68	23.628768	216.58.211.163	136.206.17.82	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=128 (request in 67)
70	24.632599	136.206.17.82	216.58.211.163	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 71)
71	24.634135	216.58.211.163	136.206.17.82	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=128 (request in 70)
73	25.632954	136.206.17.82	216.58.211.163	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 75)
75	25.636273	216.58.211.163	136.206.17.82	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=128 (request in 73)

Frame 73: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: Dell_b8:9c:7b (34:17:eb:b8:9c:7b), Dst: JuniperN_92:85:00 (ec:13:db:92:85:00)
 Internet Protocol Version 4, Src: 136.206.17.82, Dst: 216.58.211.163
 Internet Control Message Protocol
 Type: 8 (Echo (ping) request)

0000 ec 13 db 92 85 00 34 17 eb b8 9c 7b 08 00 45 004. ...{..E.
 0010 00 3c 5b 38 00 00 00 01 00 00 88 ce 11 52 d8 3a ...<[8.... ..R.:

wireshark_C81C098E-BC22-4D95-9745-39EE61C954CB_20180404164332_803252 | Packets: 152 · Displayed: 10 (6.6%) | Profile: Default

Packet numbers relevant to the experiment: **59, 60, 65, 66, 67, 68, 70, 71, 73, 75**

Explanation for each packet

- Function
- Explain why it is generated
- Explain the data contained in the packet

59: ARP request broadcast

- Asks for the MAC address of a computer, knowing its IP address.
- Here generated because my computer needs to find the MAC of (empty ARP cache) and send data to the gateway (to get the gateway to ask via proxy ARP for the MAC of the pinged computer on another network)
- Major data includes (besides the encapsulating Ethernet frame) the protocol type used (IPv4), corresponding protocol size (address length – 4 for IPv4), hardware size (hardware address length – 6 for Ethernet), opcode set to 1 (request packet), IP and MAC of sender/receiver (receiver's MAC set to all 0's to indicate a broadcast/unknown MAC)

60: ARP response

- The computer with the requested IP replies to the requesting computer with its MAC
- Generated in response to an ARP request
- Contents same as in ARP request packet, except that hardware type is explicitly stated (Ethernet), the opcode is set to 2 ('reply'), and now the sender includes its MAC.

65, 67, 70, 73: ICMP echo ping request.

- Functions as an internal checker of a computer's availability.
- Generated by the usage of the 'ping' command.
- Significant data (in the payload of the Ethernet frame and IP packet) includes the control message 'echo request' (from 'type' and 'code' fields), an error-detecting checksum, an echo request identifier and sequence number (request's number, incremented each time one is sent) (big endian and little endian formats)

66, 68, 71, 75: ICMP echo ping reply.

- Responds to a ICMP request
- Generated by the target host
- Data inside particularly includes the control message 'echo ping reply', and a sequence number that corresponds to the request packet's sequence number

Part 3:

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

136.206.17.178

50-9A-4C-3D-8D-A2

```
C:\Windows\system32\cmd.exe
C:\Users\baltrut2>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LG27-29
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-8D-A2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1951:7a09:5729:98b3<Preferred>
IPv4 Address. . . . . : 136.206.17.178<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 09 April 2018 15:35:55
Lease Expires . . . . . : 10 April 2018 15:56:21
Default Gateway . . . . . : 136.206.17.254
DHCP Server . . . . . : 136.206.217.76
DHCPv6 IAID . . . . . : 273717836
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-1C-DB-A4-50-9A-4C-3D-8D-A2

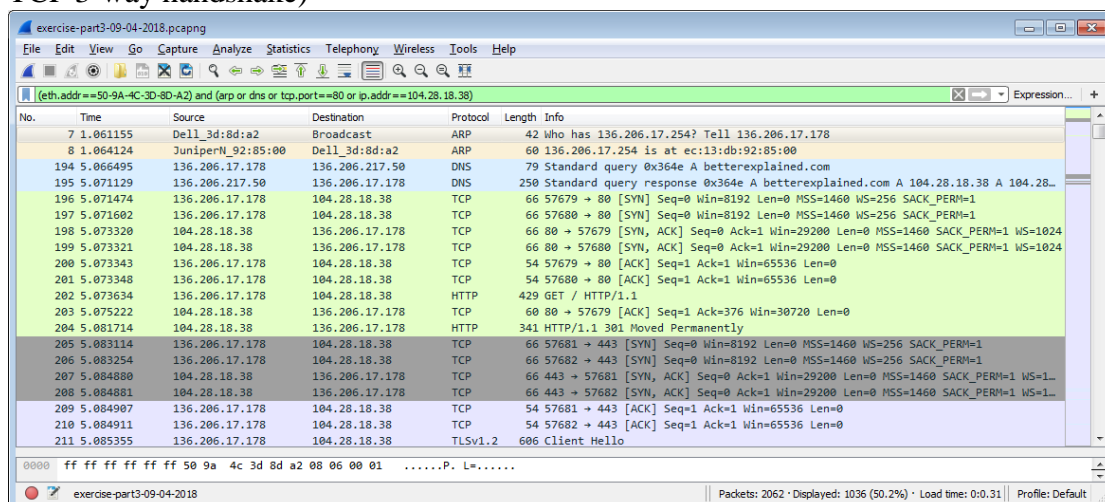
DNS Servers . . . . . : 136.206.217.50
NetBIOS over Tcpip. . . . . : Enabled
```

Filter to show only traffic concerning the test machine

Filter	(eth.addr==50-9A-4C-3D-8D-A2) and (arp or dns or tcp.port==80 or ip.addr==104.28.18.38)
--------	---

Explain how you found the start of the interaction between your PC and the website.
Used parts of the filter above and the filter ‘frame contains betterexplained’ (name of the site I pinged)

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.
196, 198, 200 (port 57679)

Explain what is happening with these 3 packets.

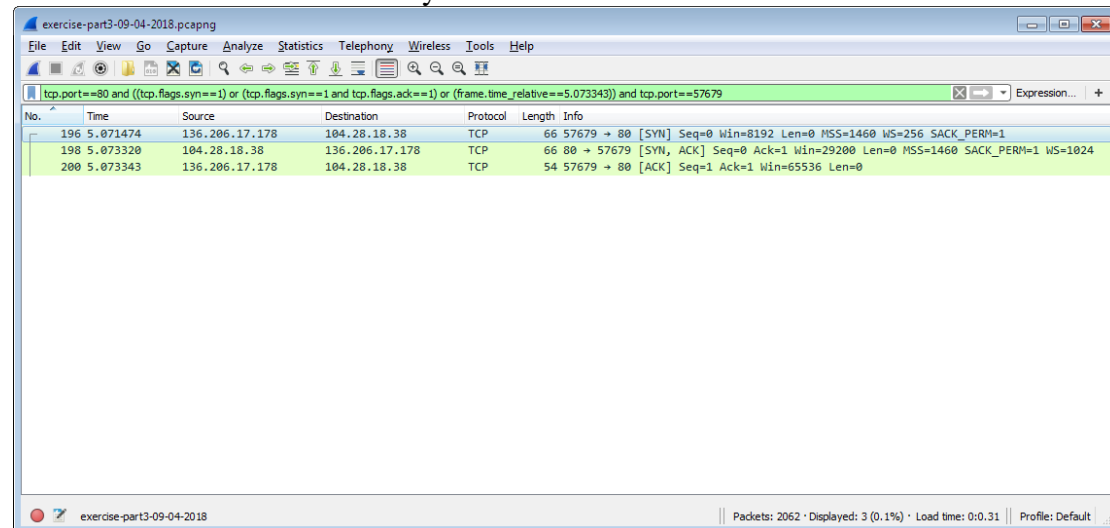
The client and server are trying to establish a TCP connection. The client sends a SYN(synchronise) packet to the server. The server acknowledges(ACK's) the packet and sends back a SYN to the client. The client acknowledges the server's SYN. Now the client and server can communicate.

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

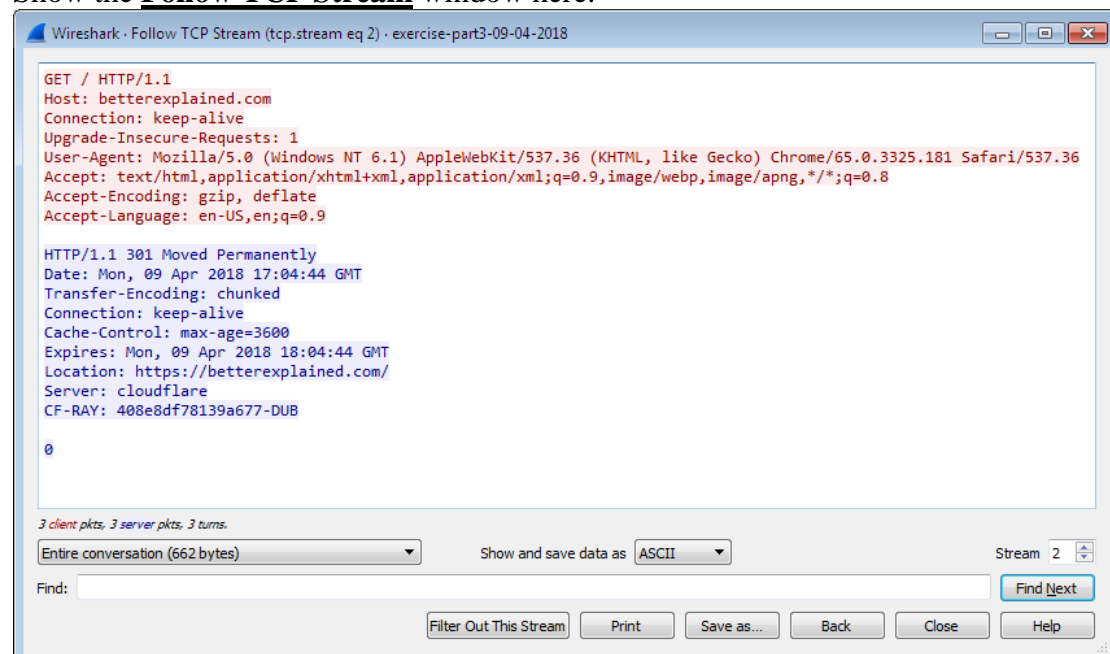
Filter	tcp.port==80 and ((tcp.flags.syn==1) or (tcp.flags.syn==1 and tcp.flags.ack==1) or (frame.time_relative==5.073343)) and tcp.port==57679
--------	--

(I wasn't able to make the filter independent of the particular port used for the 3-way handshake and couldn't filter the last ACK packet, as many other TCP packets came with the ACK flag set)

Wireshark window for the 3-way-handshake



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



Your notes on...

- a. The GET requests made
 - i. **One request: '/ HTTP/1.1', which asks for all the files (going from root directory), using HTTP version 1.1. A few 'request headers' follow.**
- b. The responses from the server
 - i. **A response: The website has been 'moved permanently'. I think this is because the server is 'cloudflare' (DDoS protection service)**
- c. The HTTP response codes used in the interaction and what they mean (look them up yourself on the Web)
 - i. **The code: 301 or 'Moved Permanently'. Means that the URL has changed and needs to be updated. The site can still be accessed through URL forwarding (the 'Location' header provides a secure URL)**

Thank you for reading