# CA169 Networks Assignment Two

# Answer Sheets

| | |
|---|---|
| STUDENT NAME: | CONOR JOYCE |
| STUDENT NUMBER: | 19425804 |
| PROJECT NUMBER: | 2 |
| MODULE CODE: | CA169 |
| DEGREE: {CA\|EC\|CPSSD\|ECSA] | CA |
| LECTURER: | Dr Michael Scriney |

**Declaration**

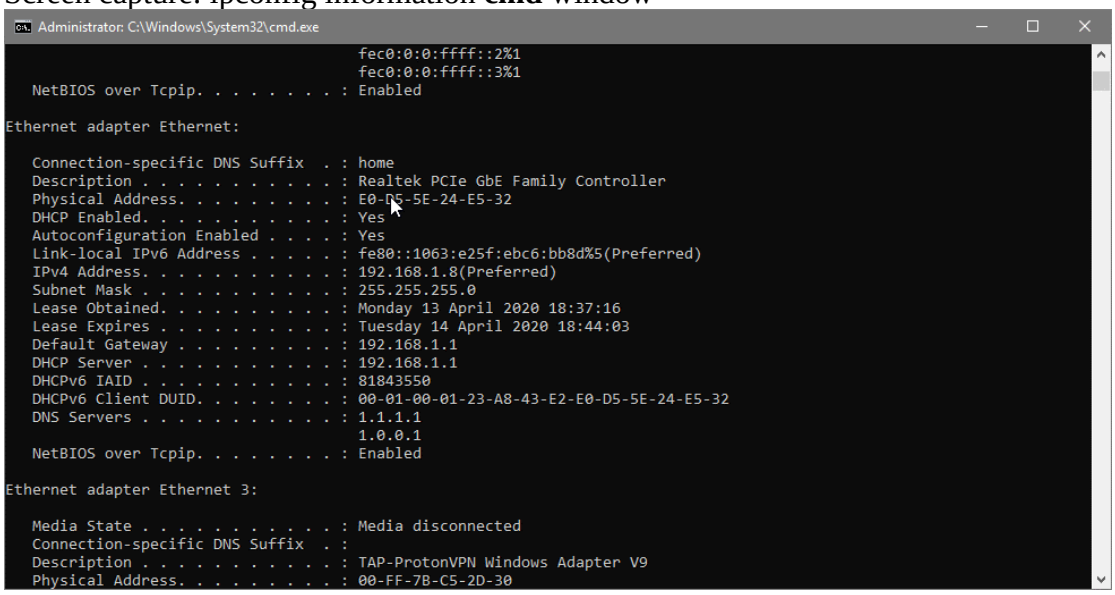
***In submitting this project, I declare that the project material, which I now submit, is my own work. Any assistance received by way of borrowing from the work of others has been cited and acknowledged within the work. I make this declaration in the knowledge that a breach of the rules pertaining to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

## *Part 1: DHCP traffic*

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

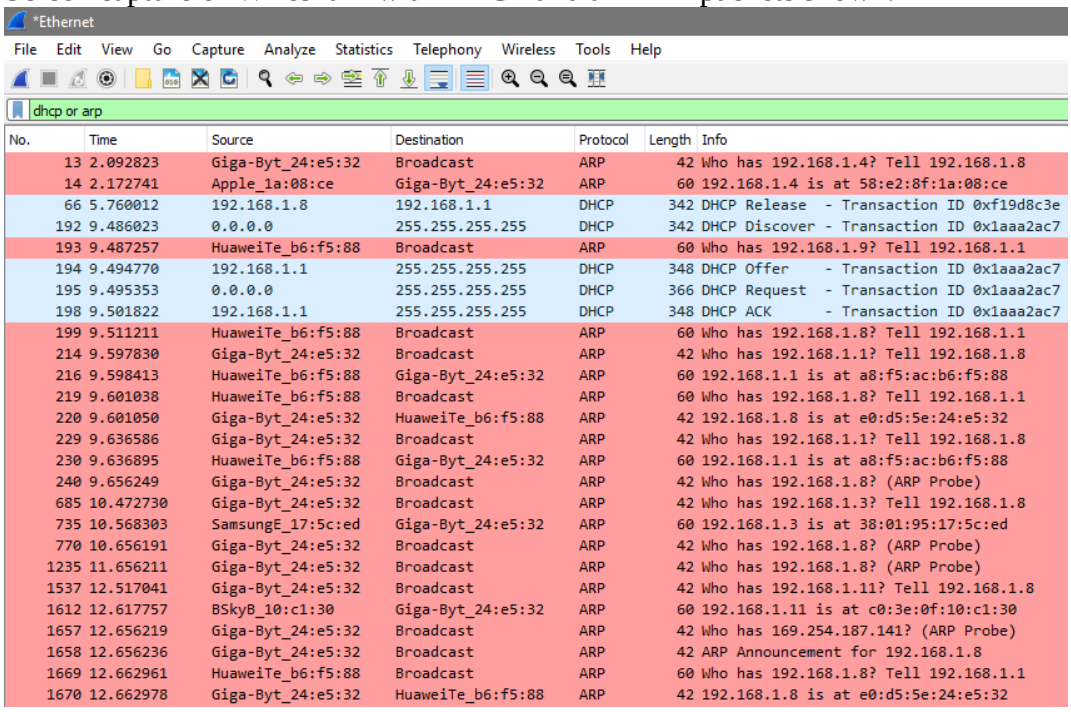
| | |
|---|---|
| 192.168.1.8 | E0-D5-5E-24-E5-32 |

Screen capture: ipconfig information **cmd** window




IPv4 Address: my ip
Physical Address: my mac address

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




Filter is set to “dhcp or arp” to show only these protocols

Packet numbers relevant to the DHCP interaction:

a. DHCP DISCOVER
   - 192
b. DHCP OFFER
   - 194
c. DHCP Request
   - 195
d. DHCP Acknowledgement
   - 198
e. DHCP Release (if you release using `ipconfig /release`)
   - 66
f. All ARP packets used
   - 13, 14, 193, 199-1670

Function of each packet

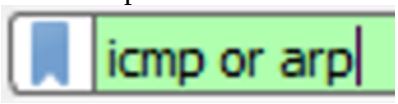
a. DHCP DISCOVER
   - Find dhcp server
b. DHCP OFFER
   - Router offering an ip to a device
c. DHCP Request
   - Device accepting the ip being offered
d. DHCP Acknowledgement
   - Router acknowledging device accepting its new ip
e. DHCP Release (if you release using `ipconfig /release`)
   - Device telling router it doesn't want its ip address anymore
f. ARP
   - Devices on network figuring out which device has what ip

## *Part 2:* ***`ping` traffic***

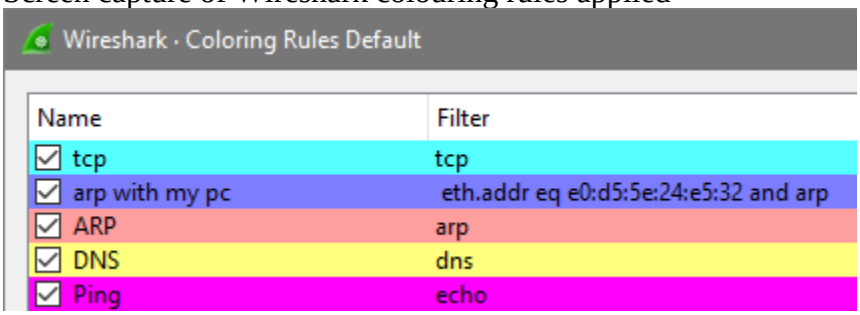
Your IP & MAC address for this experiment (use ipconfig)

| | |
|---|---|
| 192.168.1.101 | E0-D5-5E-24-E5-32 |

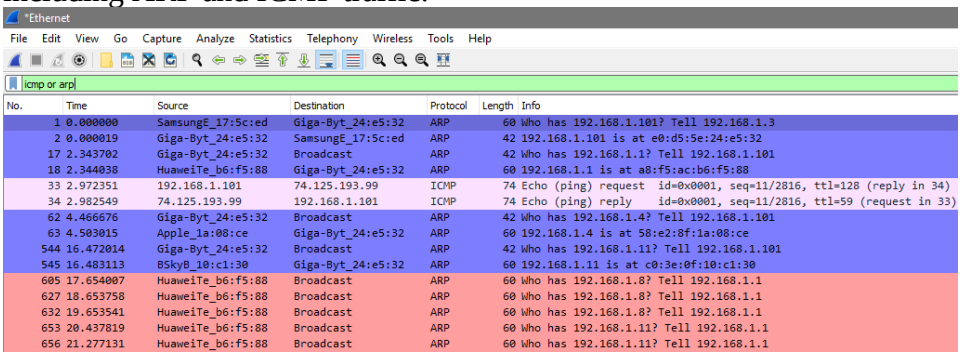
Screen capture of Wireshark filter utilised




Screen capture of Wireshark colouring rules applied




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




All pings (echo request and reply) are in pink
ARP packets involving my pc are in blue
ARP broadcast from router is in red

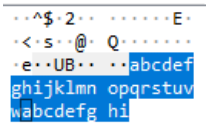
Packet numbers relevant to the experiment:
Explanation for each packet

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

33:

- echo request (pinging a server)
- generated by device expecting a response from a server
- packet contains type 8 meaning echo request, code 0, checksum, identifier, seq. no. and the payload which is garbage text ending in hi

Payload →



34:

- echo reply (response from server)
- sent from server after receiving an echo request
- type 0 (echo reply), code 0, checksum, identifier, seq. no. and the same payload

17:

- arp broadcast
- my pc asking what mac addresses have a certain ip
- packet contains the ip whose mac address is being searched for, and the senders ip

18:

- arp response
- my router responding to my pc's broadcast telling my pc the routers mac address
- packets contains the ip being asked for and the mac address who owns that ip

## *Part 3:*

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

| | |
|---|---|
| 192.168.1.101 | E0-D5-5E-24-E5-32 |

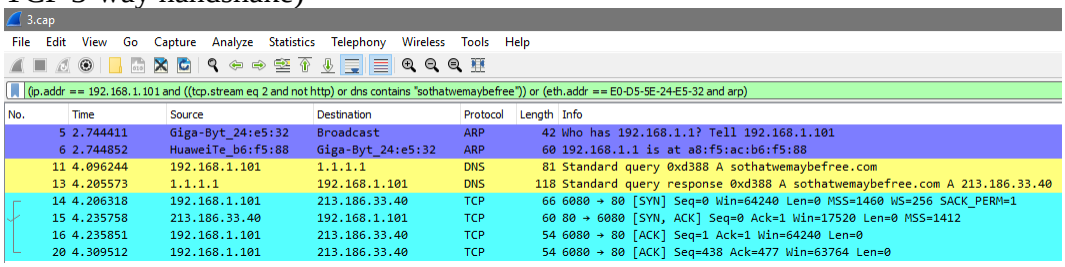
Filter to show only traffic concerning the test machine

| | |
|---|---|
| Filter | (ip.addr == 192.168.1.101 and ((tcp.stream eq 2 and not http) or dns contains "sothatwemaybefree")) or (eth.addr == E0-D5-5E-24-E5-32 and arp) |

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

- noticed my pc talking to dns server and after dns response, my pc initiates 3-way tcp handshake with the website

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



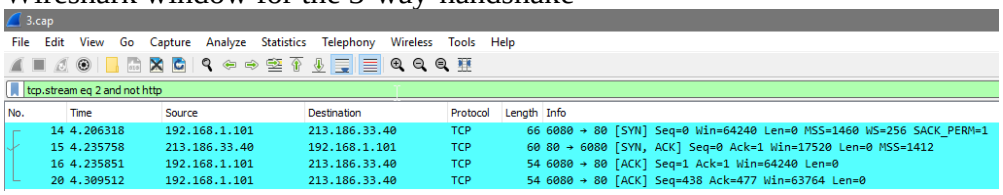

Write down the numbers of the packets with the 3-way handshake.
Explain what is happening with these 3 packets.

- 14: syn, initialise connection
- 15: syn from server + ack of previous syn
- 16: ack from device

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

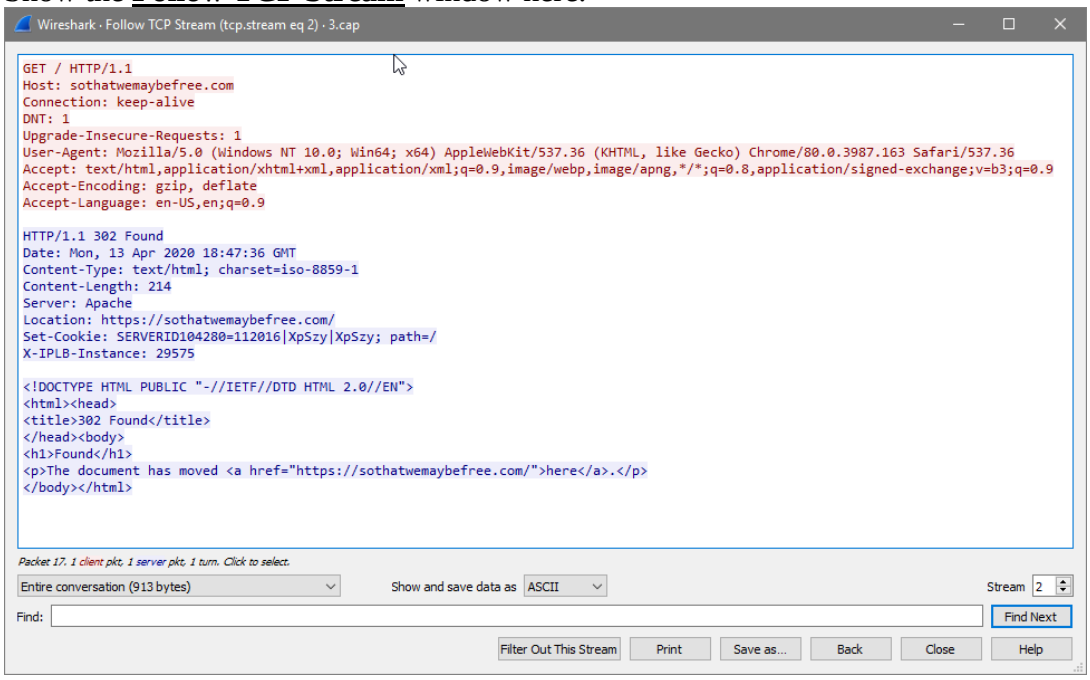
| | |
|---|---|
| Filter | tcp.stream eq 2 and not http |

Wireshark window for the 3-way-handshake




First 3 packets are the handshake (syn, syn/ack, and ack)

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




Your notes on…

a. The GET requests made
   - There is a get request for the html of the website
b. The responses from the server
   - After the get request the server responds with the location of the html which is just https://sothatwemaybefree.com/ - the typical location, so this is a fairly basic website
c. The HTTP response codes used in the interaction and what they mean (look them up yourself on the Web)
   - 302 Found – redirects us to the location of the html file