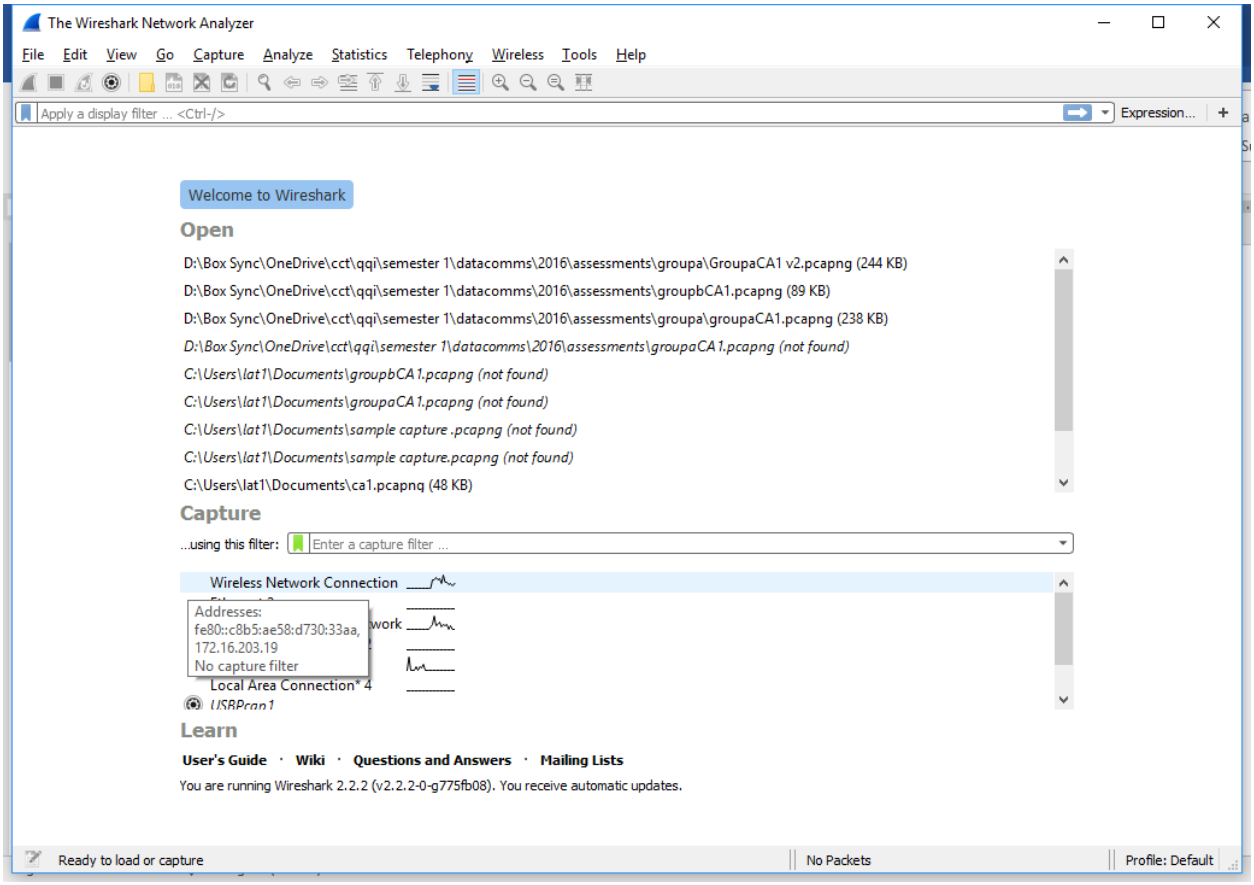
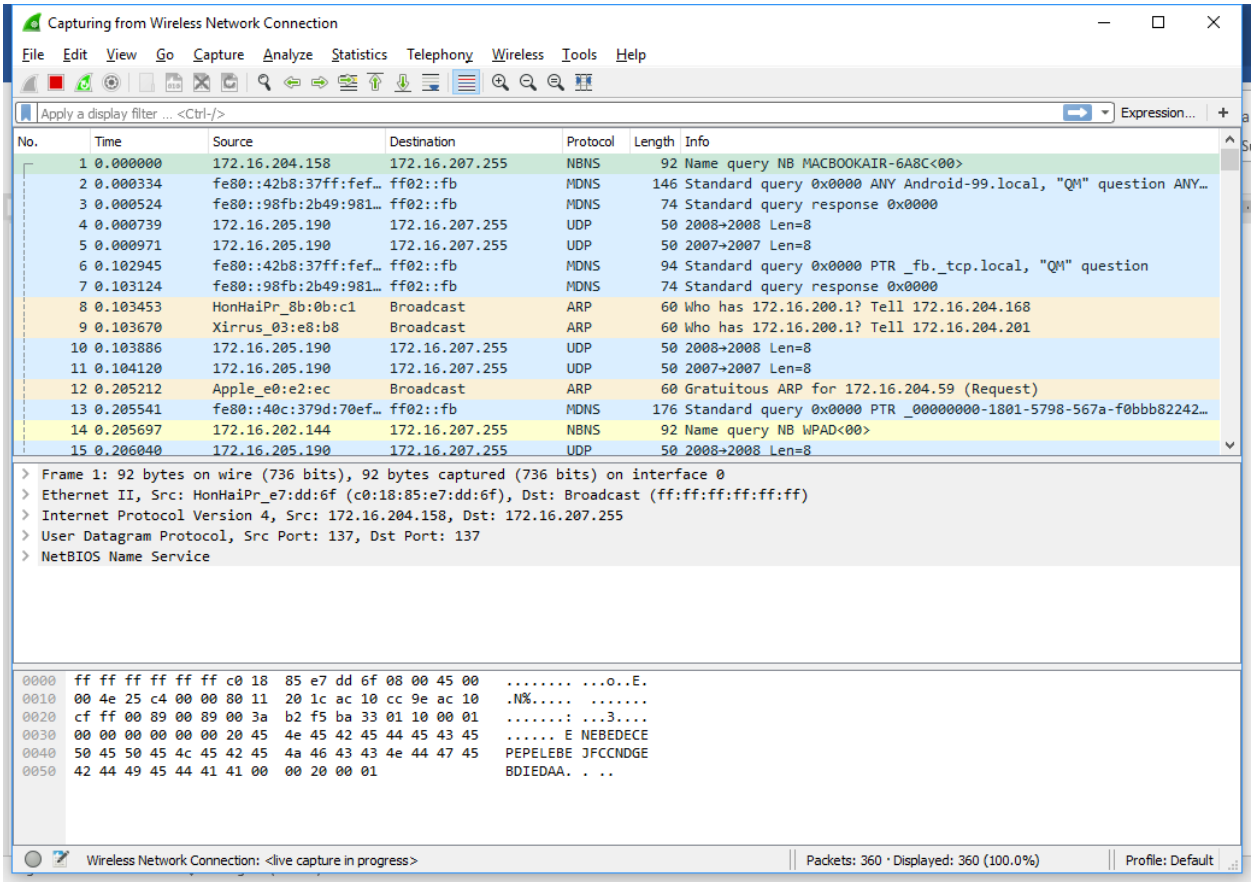
In this lab we will use Wireshark to observe the DHCP process.

First, start Wireshark and select your active Network Interface

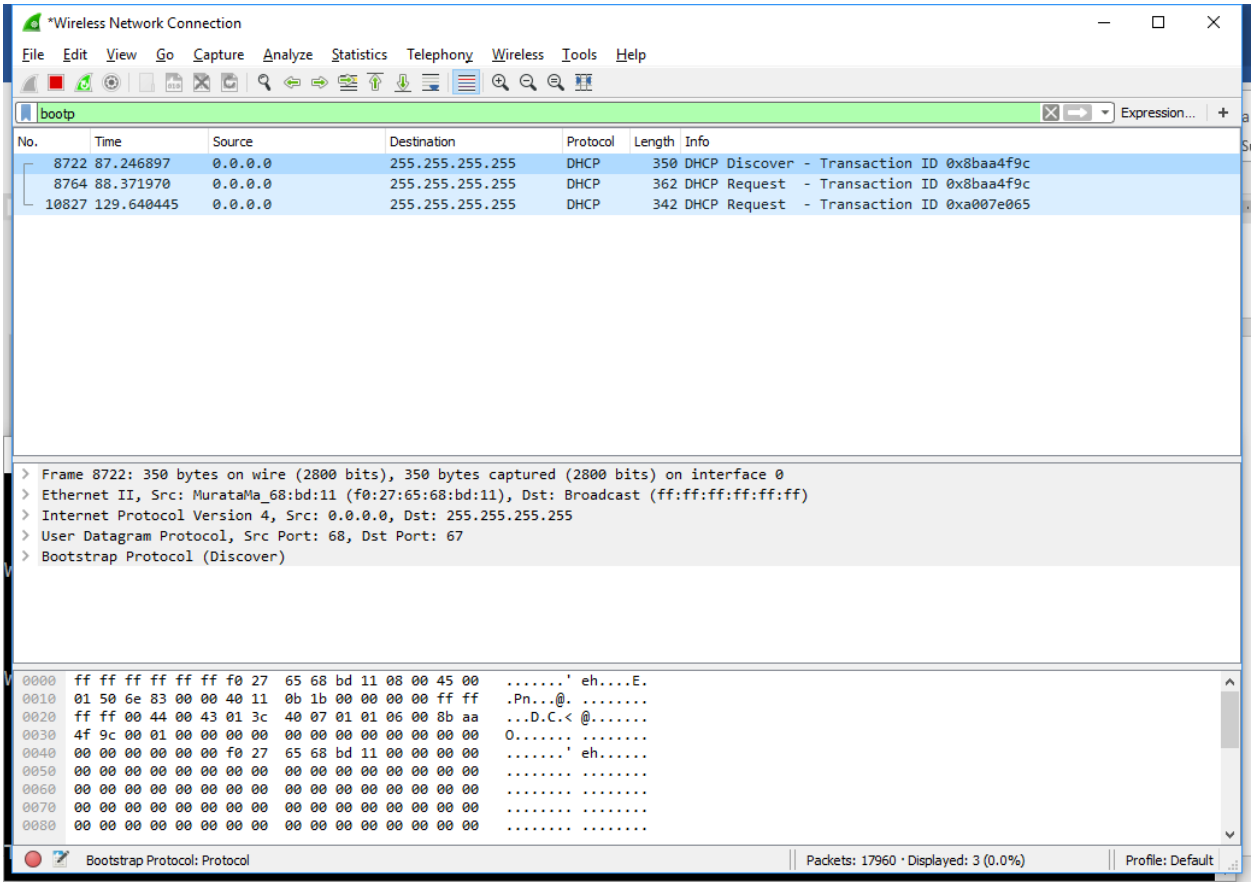


In the next Window you should see traffic for that interface, including any broadcasts that your machine is receiving.



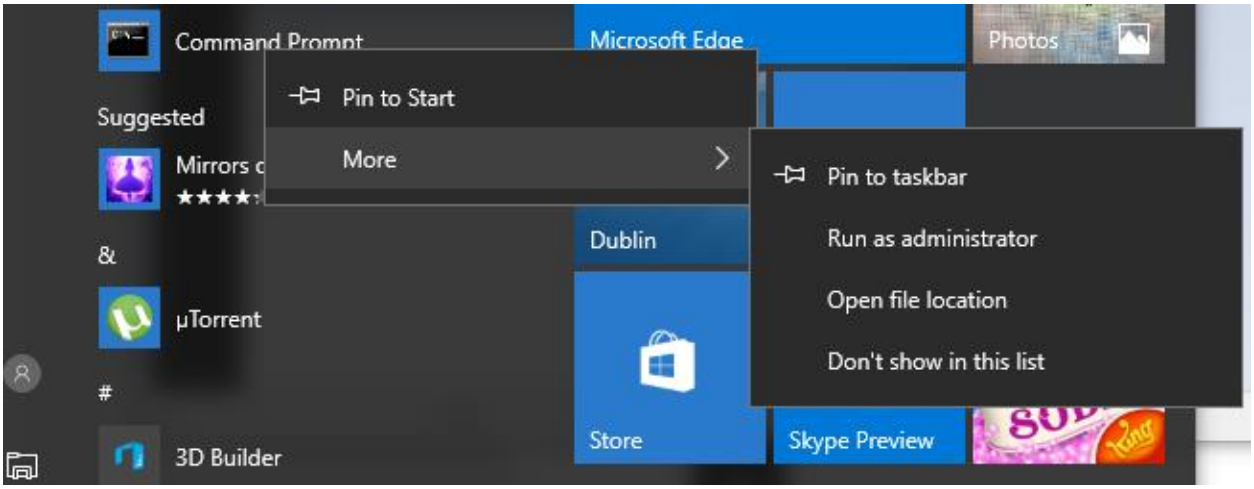
The traffic that we want to observe is small and we do not need to see all other traffic so we can apply a filter in wireshark.

In the filter box type *bootp* and press enter, this should remove a lot of unnecessary traffic from our view.

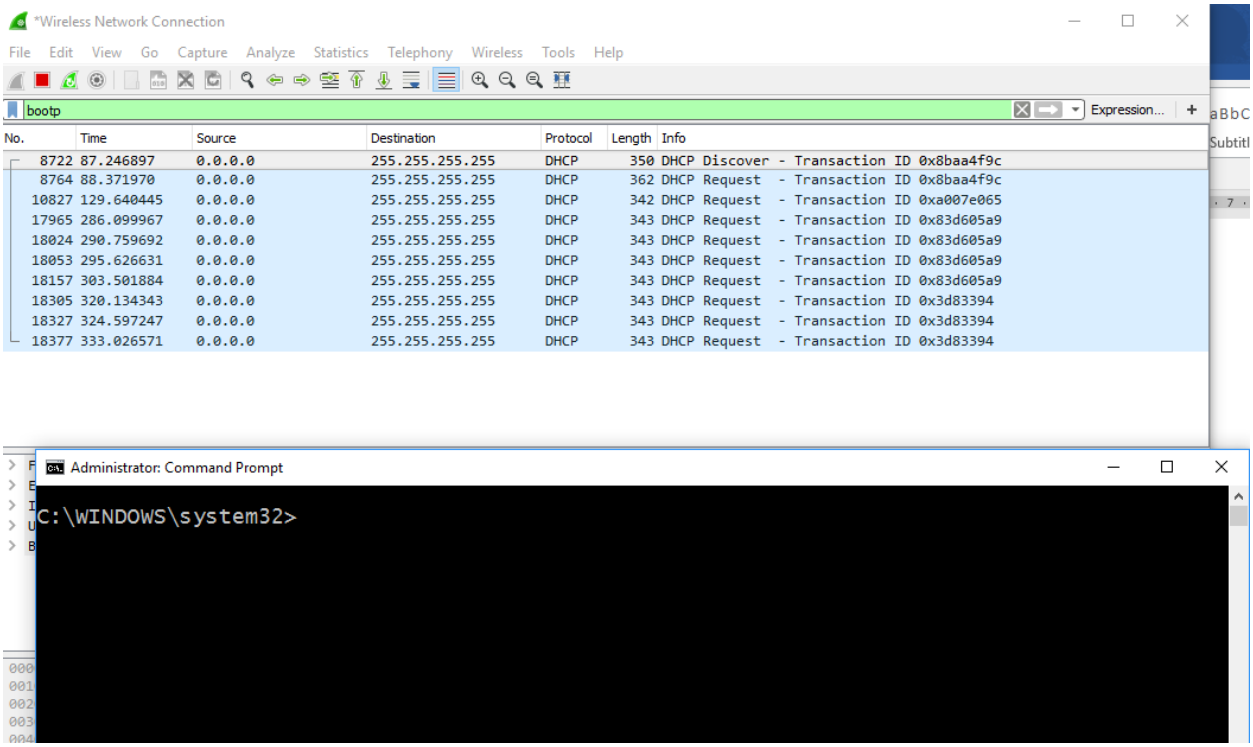


Next we want to generate some DHCP traffic so minimise the Wireshark window, leaving the capture running.

Click START and type CMD, then right-click on the command prompt to RUN AS ADMINISTRATOR



Arrange the command prompt so you can see it and the live Wireshark capture in the background



In the command prompt type *ipconfig /release* and press ENTER.

Then type *ipconfig /renew* and press ENTER.

Return to the Wireshark capture and look for the Discover, Offer, Request, and Acknowledgement.

```
25626 478.707808    0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0xf32c7ce2
25703 479.721248    172.16.200.1     172.16.203.19      DHCP     342 DHCP Offer    - Transaction ID 0xf32c7ce2
25704 479.721645    0.0.0.0          255.255.255.255    DHCP     349 DHCP Request  - Transaction ID 0xf32c7ce2
25710 479.834160    172.16.200.1     172.16.203.19      DHCP     342 DHCP ACK      - Transaction ID 0xf32c7ce2
```

Expand each one to view the details.

What is the Source MAC address of the Discover?

What is the Destination Port of the Offer?