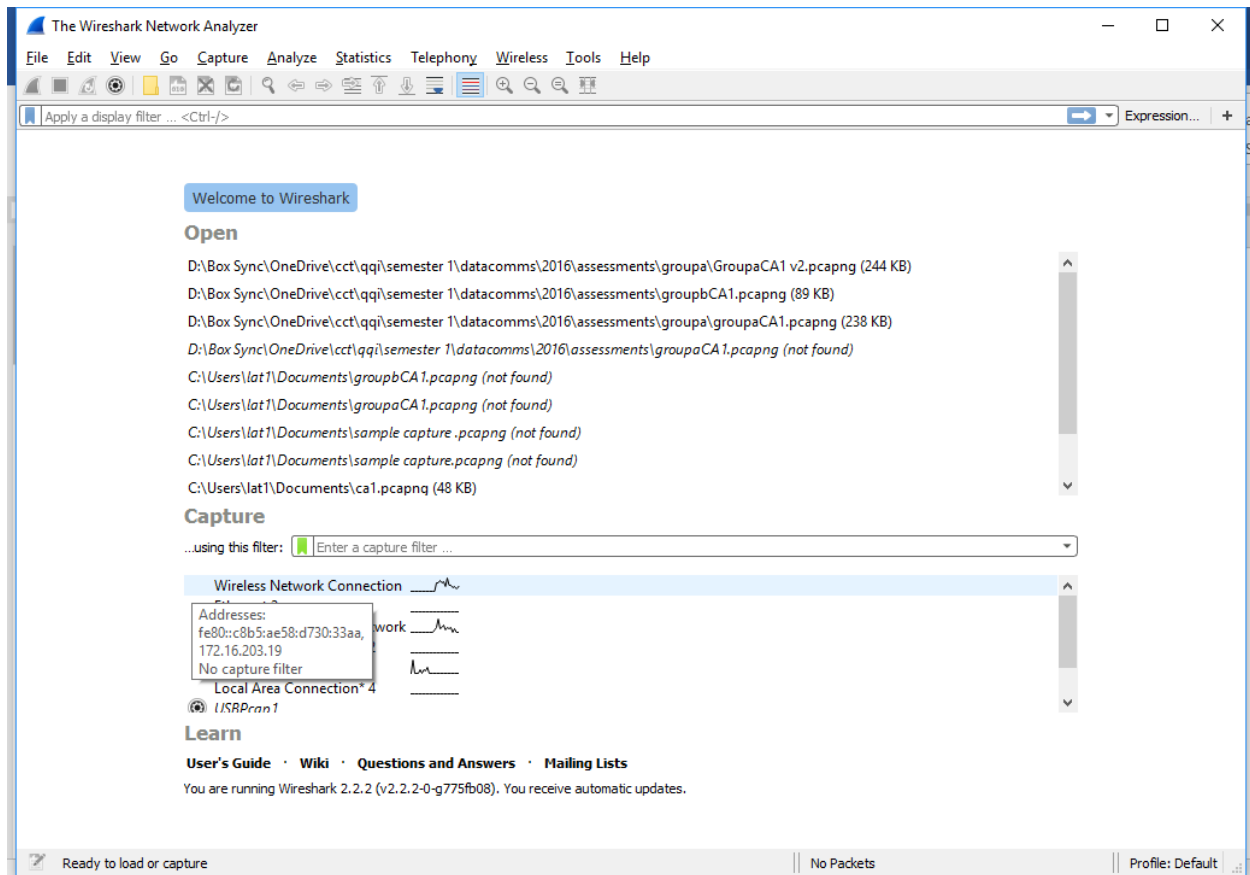
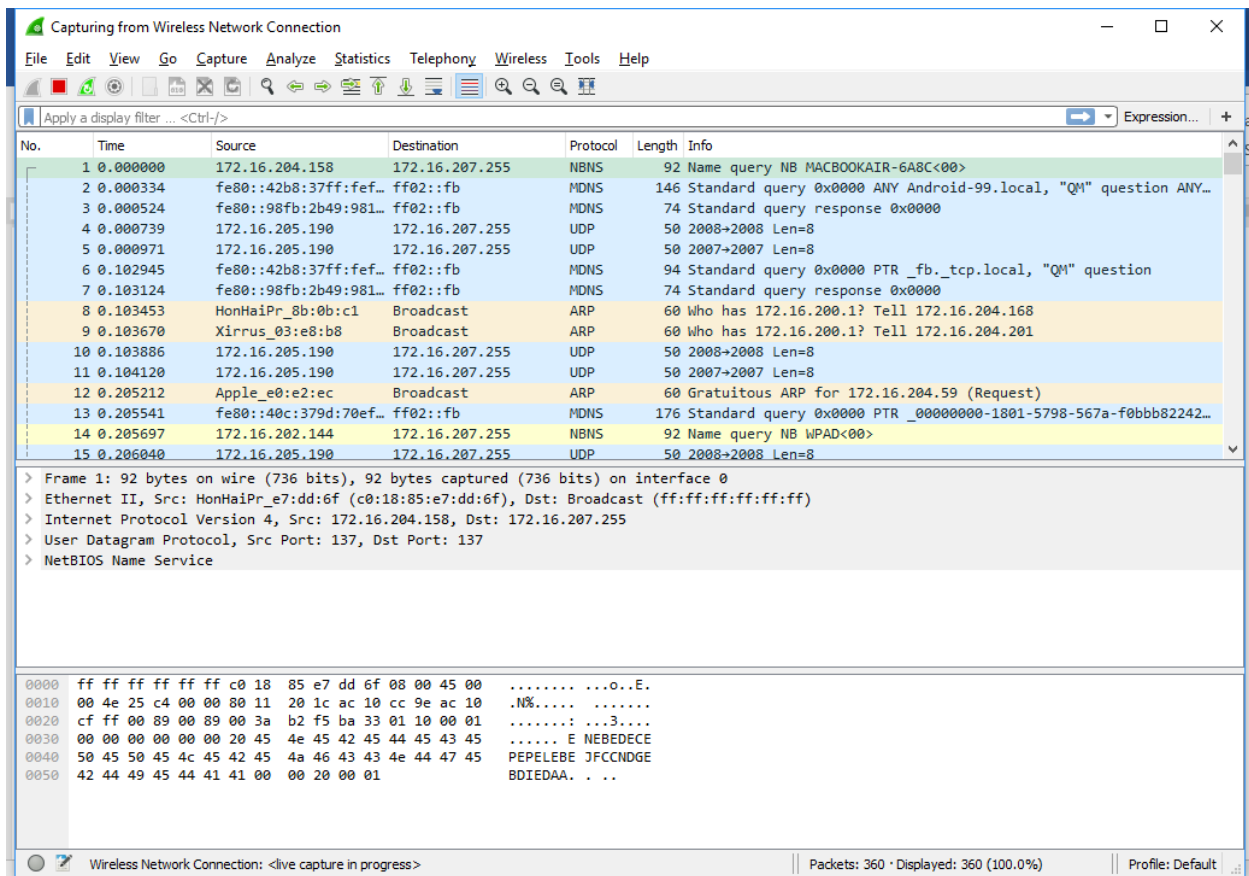


In this lab we will use Wireshark to observe the DHCP process.

First, start Wireshark and select your active Network Interface

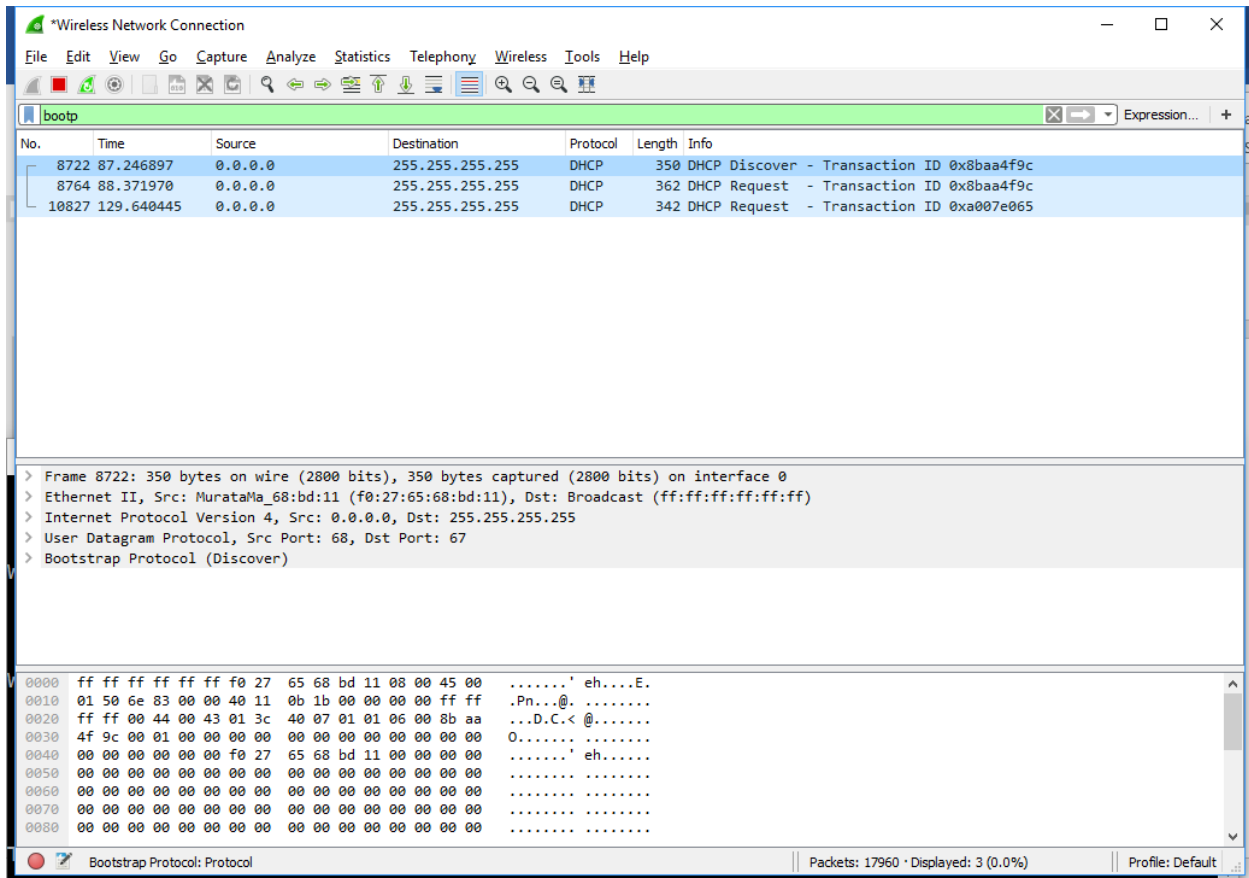


In the next Window you should see traffic for that interface, including any broadcasts that your machine is receiving.



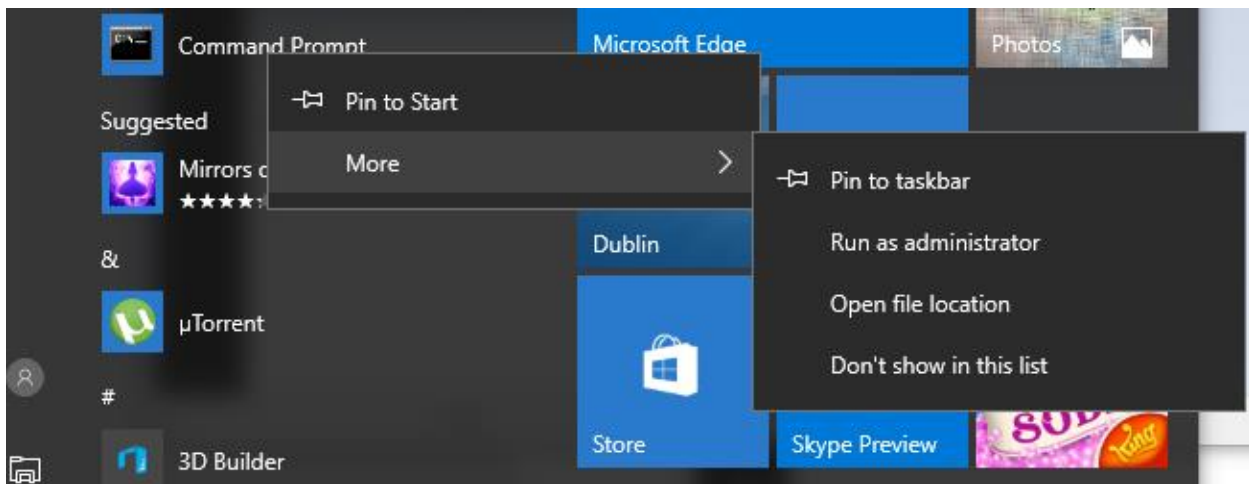
The traffic that we want to observe is small and we do not need to see all other traffic so we can apply a filter in Wireshark.

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

No.	Time	Source	Destination	Protocol	Length	Info
8722	87.246897	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0x8baa4f9c
8764	88.371970	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x8baa4f9c
10827	129.640445	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa007e065
17965	286.099967	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x83d605a9
18024	290.759692	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x83d605a9
18053	295.626631	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x83d605a9
18157	303.501884	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x83d605a9
18305	320.134343	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x3d83394
18327	324.597247	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x3d83394
18377	333.026571	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x3d83394

```

Administrator: Command Prompt
C:\WINDOWS\system32>

```

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?