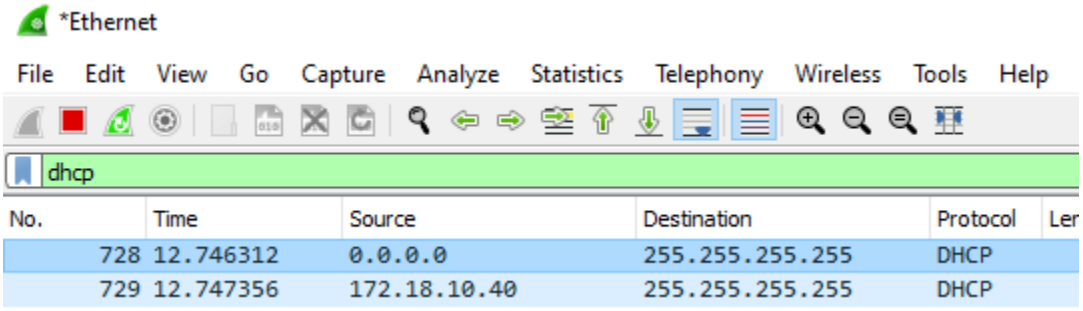
# Network Lab 4 DHCP

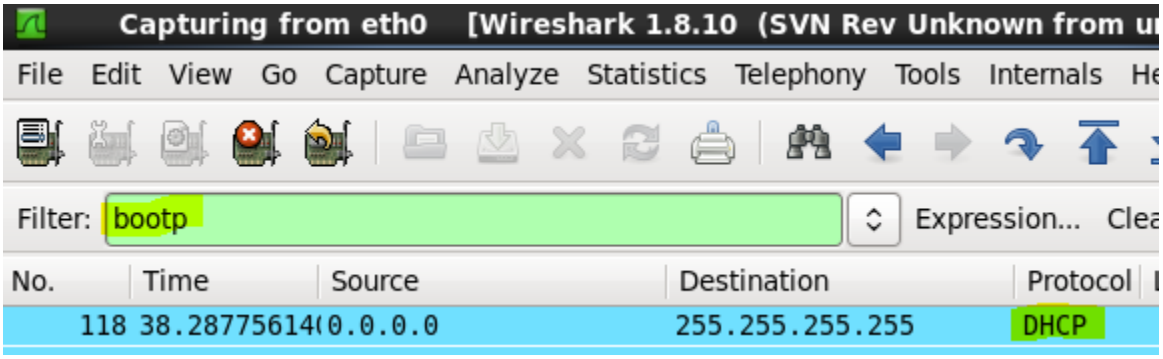
You can use either your Linux VM, Windows VM, or Windows host to do this lab. For whichever you choose, write down its MAC address (Windows: *ipconfig /all*, look for physical address; Linux: *ip link* , look for link/ether address.)

The file dhcp-example.pcapng is available in Canvas. You can open it in Wireshark, and it will show you what a complete DHCP exchange should look like.

1) Start Wireshark on the machine you are using and set it to capture on the machine's Ethernet interface. In the display filter window, enter "dhcp".




Note: Older versions of Wireshark use the name of the older protocol, bootp, as the filter for both dhcp and bootp. If dhcp doesn't work in the display filter, try bootp. It will show dhcp in the protocol column of the packet window.




2) Force your machine's dhcp client to get a new address lease.
   a. Windows
      i. from an elevated command prompt, type "ipconfig /release"
      ii. go to the network control panel (ncpa.cpl) and set the IP address to some random address (10.0.0.x is fine, you do not need a default gateway or DNS), click OK twice to finish
      iii. go back to the network control panel, set "Obtain an IP address automatically" and click OK twice. As soon as you do, you should see the DHCP packets appear in Wireshark
   b. Linux:
      i. enter "ip address" and find the name of your interface. On Ubuntu it is often ens33. Older Linux uses eth0

ii. enter "sudo dhclient -r {interface, ie ens33 or eth0}" to remove the address
iii. enter “sudo dhclient" to start the request process

3) Once the commands have completed, stop the packet capture.
4) In Wireshark, find a dhcp discover packet that came from your machine. The Ethernet source address will be the same as your machine's MAC address. Note: if you are using your VM, there probably won’t be any other DHCP traffic. If you use your host computer, you may have to sort through DHCP traffic from other computers on the school network.
   Note: if you have difficulty in finding the DHCP transaction for your computer, open dhcp-example.pcapng in Wireshark to see an example without the other traffic.
5) What are the destination Ethernet and IP addresses of your dhcp discover packet? Does this make sense? (At the beginning, your machine does not know where the dhcp server is.)
6) Not far after the dhcp discover packet, you should be able to find a dhcp offer packet. What are the source Ethernet and IP addresses of the offer packet? What are the destination Ethernet and IP addresses? How does your machine know this offer belongs to it? (In the packet details window, expand Bootstrap Protocol (offer) and you should find the answer.)
7) Find the dhcp request packet. Who sent it? Note that it is still sent to broadcast addresses. How does the dhcp server know this request is addressed to it? Hint: Look for something like a serial number that is common to all the packets in the DORA sequence.
8) Find the dhcp ack packet. You should be able to find the address that has been assigned to your computer. Examine the dhcp options in the ack packet. Normally you will see Options 1, 3, 6, and 15, which all contain useful data. What useful information do you find there?

## Hand In

Turn in the answers to the underlined questions, above.