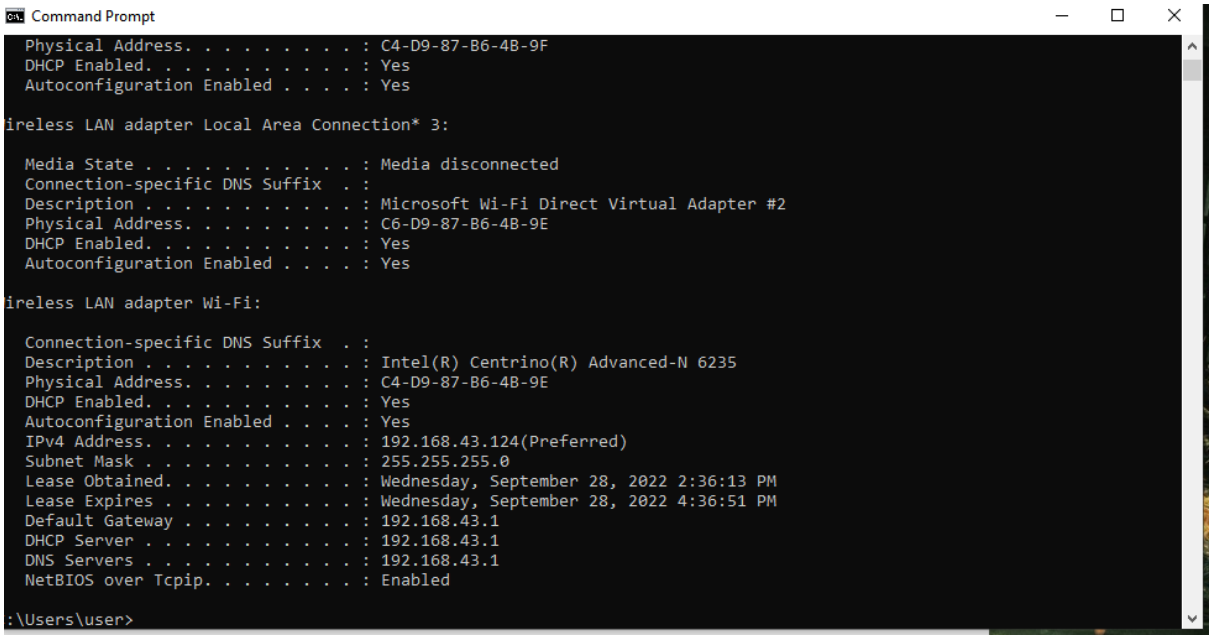
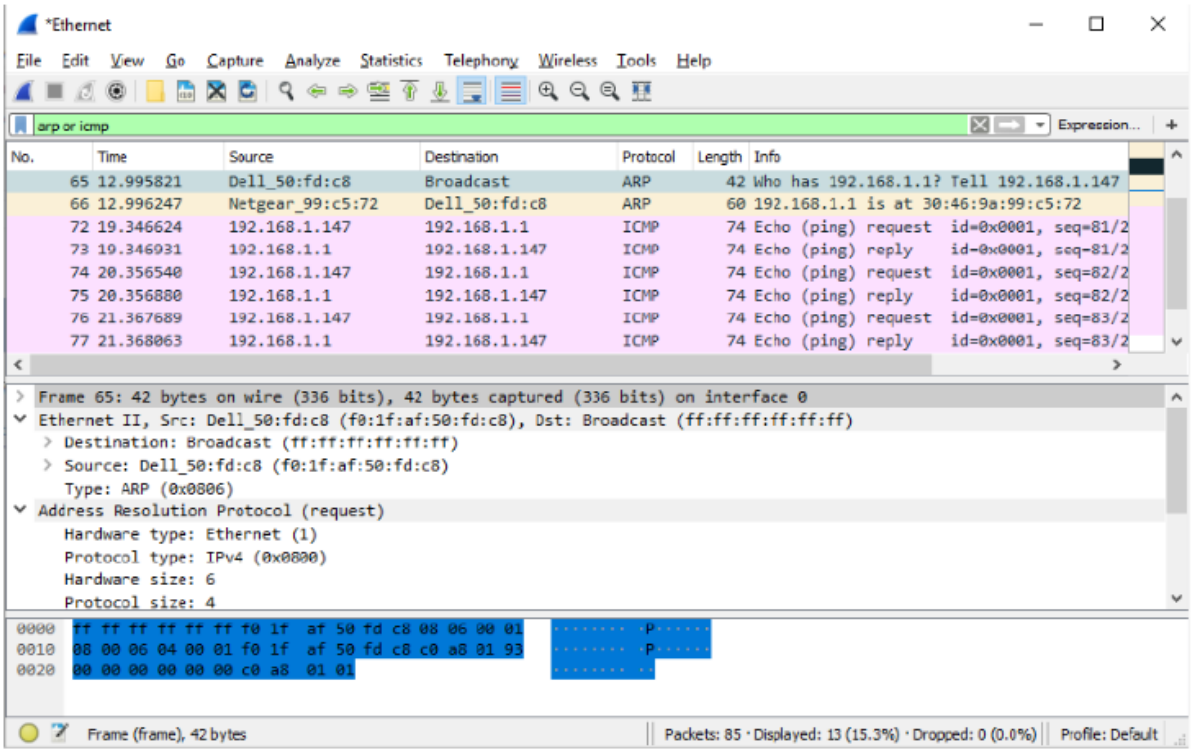
Lab - Use Wireshark to Examine Ethernet Frames



What is significant about the contents of the destination address field?

All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the default gateway.



Why does the PC send out a broadcast ARP prior to sending the first ping request? The PC cannot send a ping request to a host until it determines the destination MAC address, so that it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.

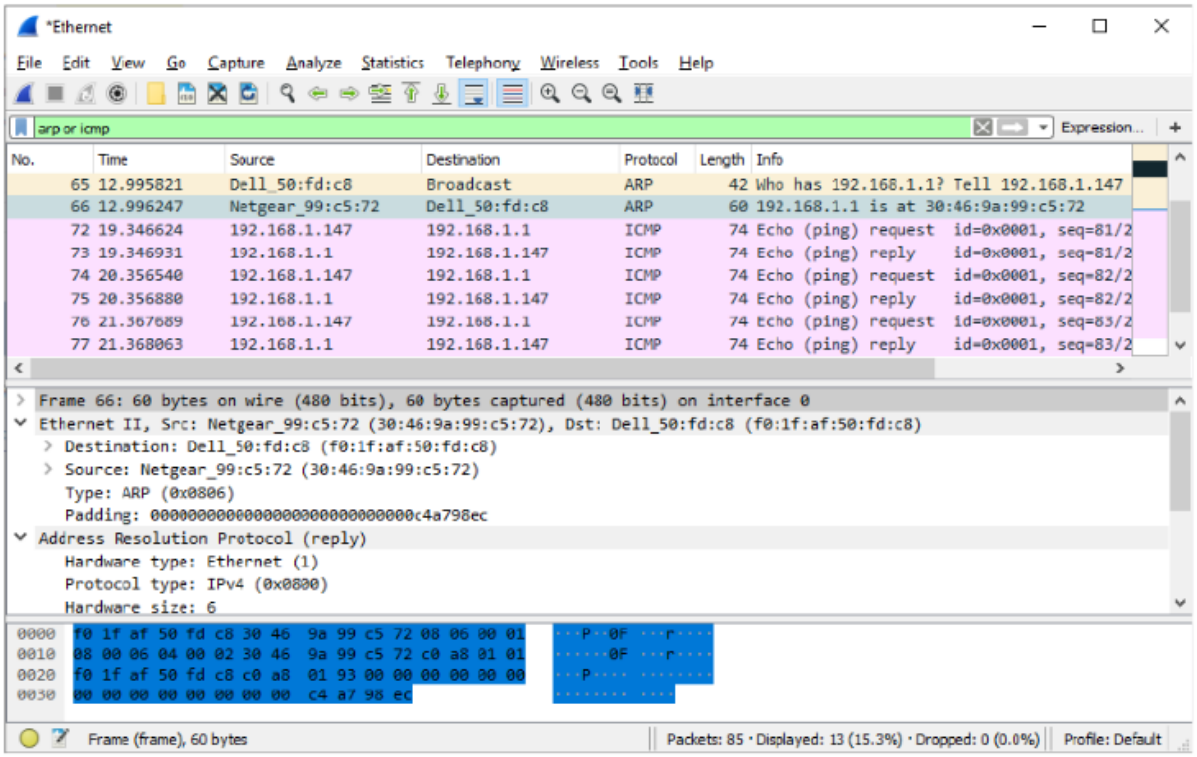
What is the MAC address of the source in the first frame?

f0:1f:af:50:fd:c8.

What is the Vendor ID (OUI) of the Source NIC in the ARP reply? Netgear.

What portion of the MAC address is the OUI? The first 3 octets of the MAC address indicate the OUI.

What is the NIC serial number of the source? It may vary, it is 99:c5:72 in this case.



Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Step 1: Determine the IP address of the default gateway on your PC

192.168.43.1

The second line in the packet details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed. What is the MAC address of the PC NIC?

What is the default gateway's MAC address?

C4-D9-87-B6-4B-9E

What type of frame is displayed? IPv4 frame type.

The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address? 192.168.43.124

What is the destination IP address? 192.168.43.19