# CSUF SPRING 2021

COMPUTER COMMUNICATIONS CPSC 471 - 01/05

PROJECT #3

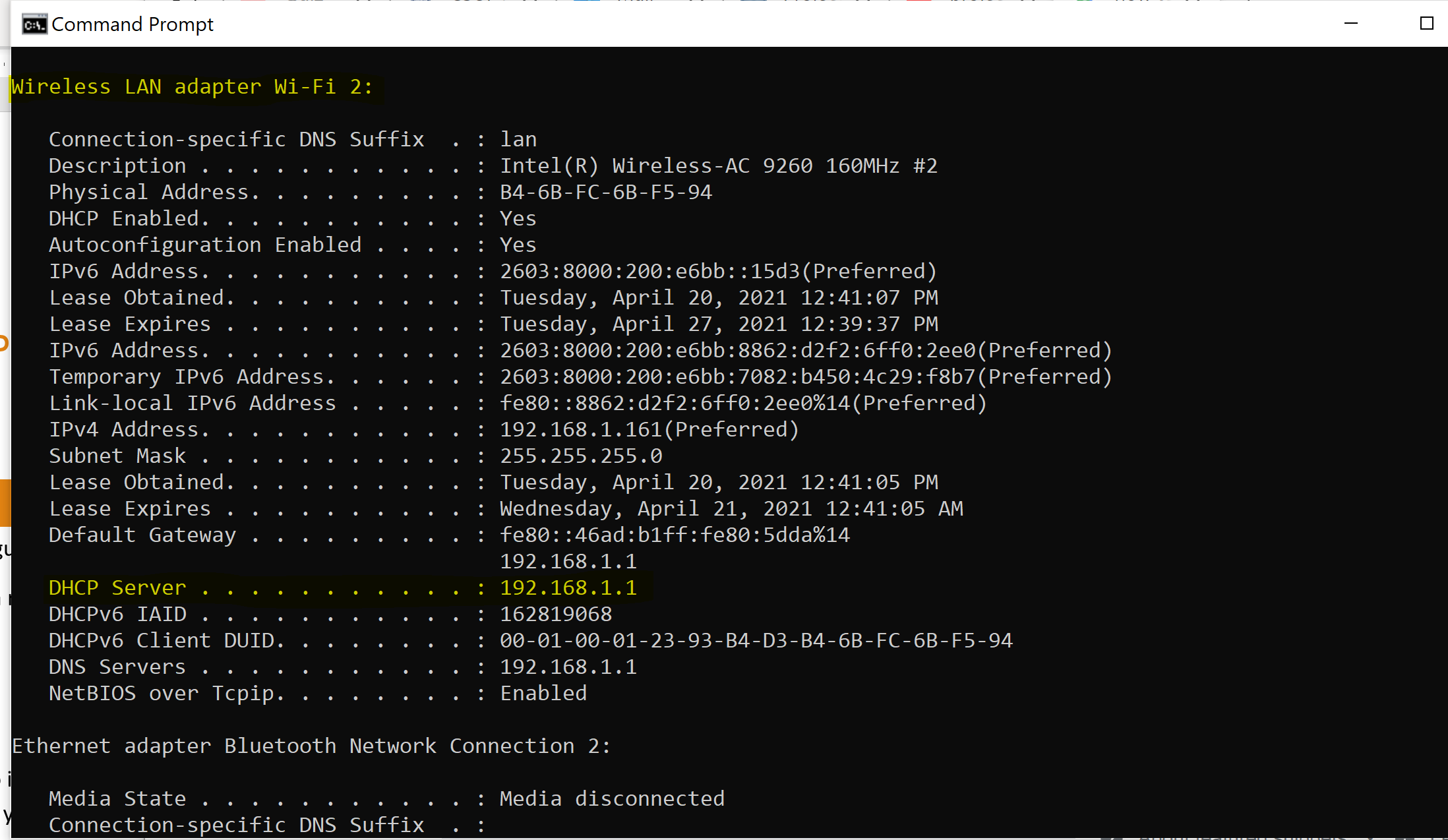
PROJECT SUBMISSION AND YOUR RESPONSIBILITY

Answer the following questions:

1. Identify the DHCP server of your home network.
   1. What is the IP address of your DHCP server?

192.168.1.1

* 1. Provide screen capture(s) showing your DHCP server information.



1. Identify your PC addresses.
   1. What is your PC IP address?

192.168.1.161

* 1. What is your PC MAC address?

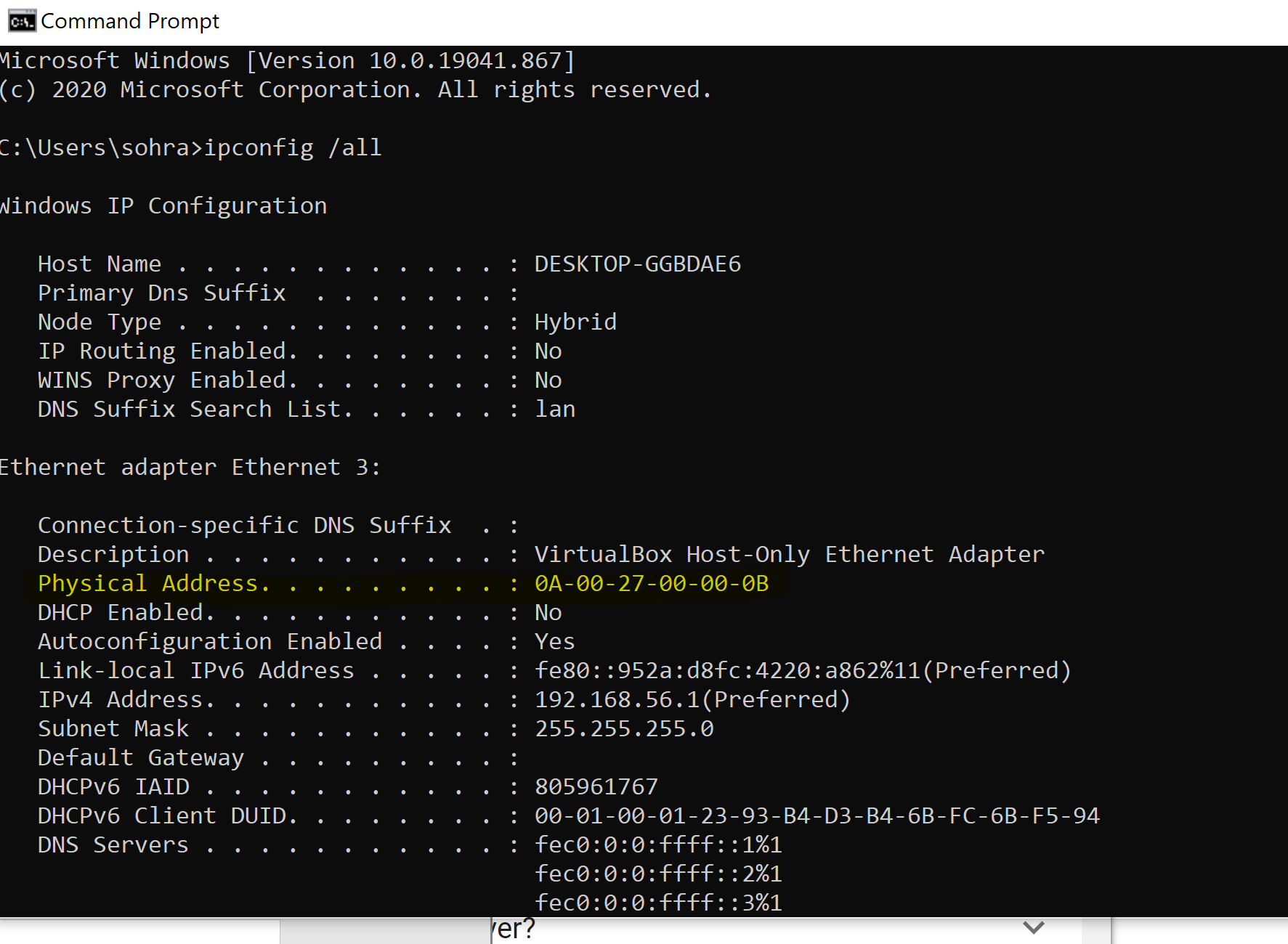
B4-6B-FC-6B-F5-94

* 1. From where did you get this information, from the PC or the DHCP server?

I found the information in the DHCP server

* 1. Provide screen capture(s) showing the above IP and MAC addresses and the

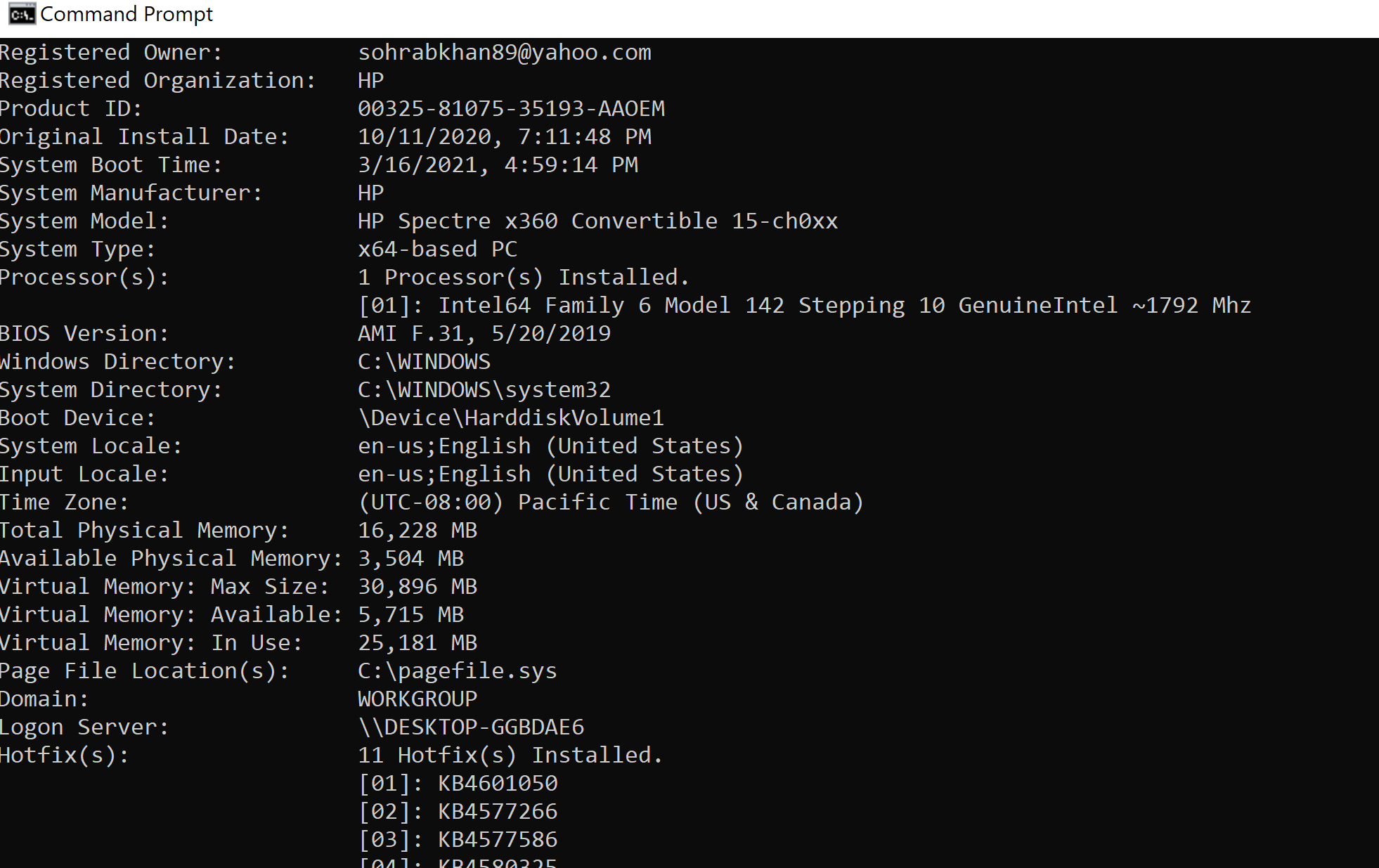
source of the information (PC or DHCP server screen).



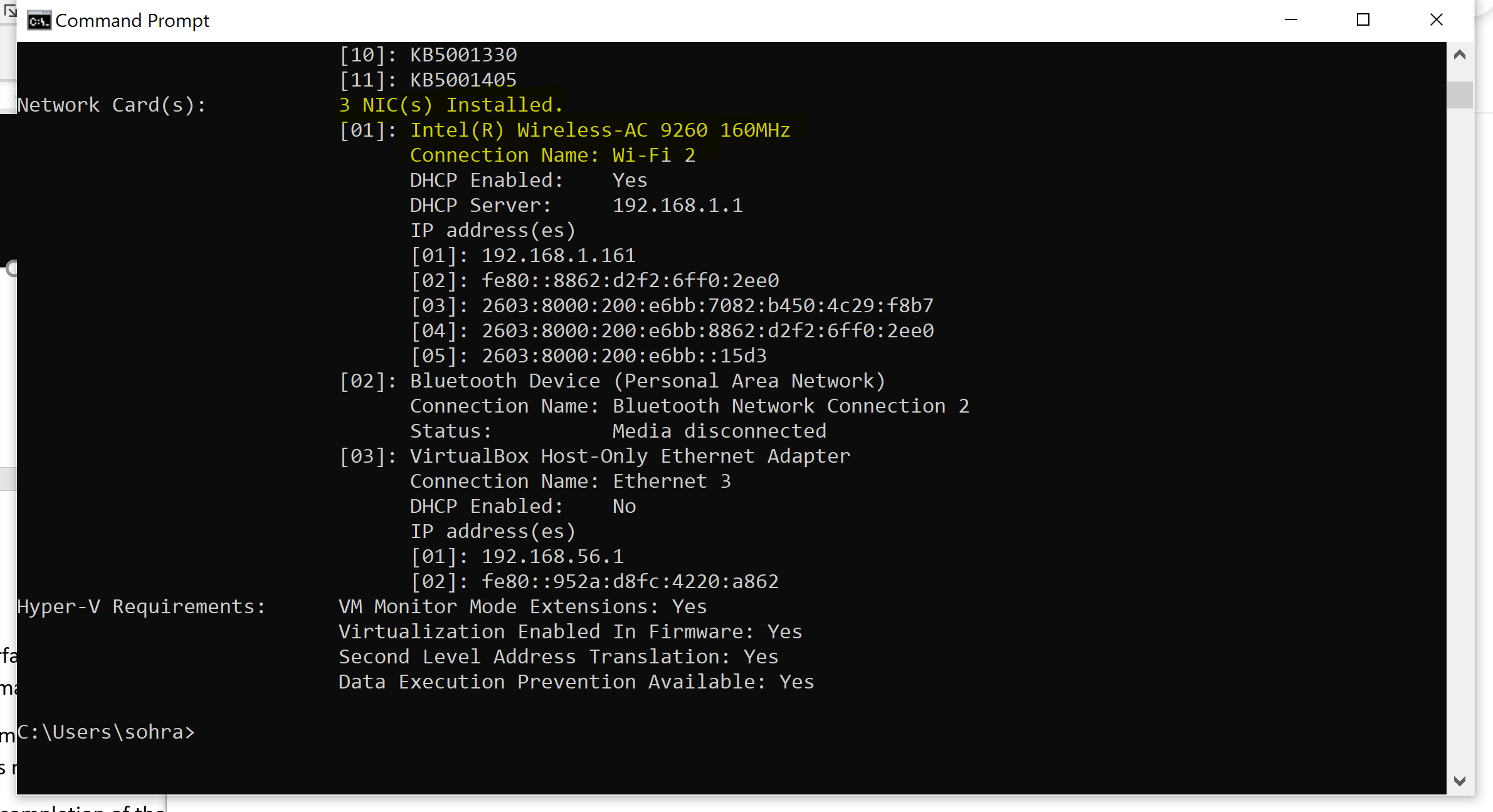
1. Depending on your PC operating system, find and study the command that you can use to **release** the PC IP address from the DHCP server lease.
   1. What is your operating system and release version number? Provide a screen capture for this information.

OS Name: Microsoft Windows 10 Home

Version Number: 10.0.19041 N/A Build 19041



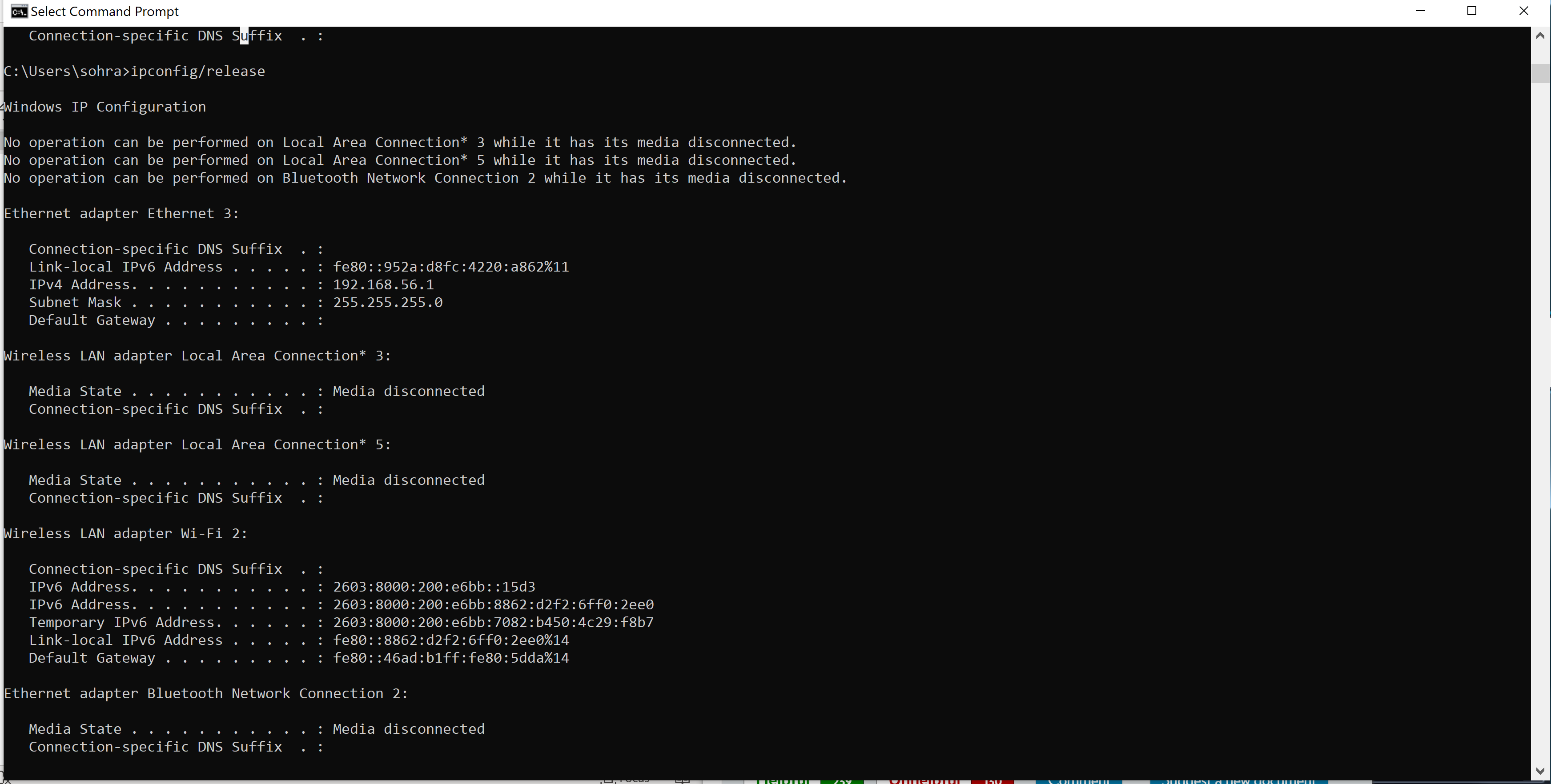
* 1. What is the name of the network interface you are using for this experiment? Provide a screen capture for this information.



* 1. Write the complete command line (command with all parameters) you used to release DHCP leased IP address for this network interface:

**ipconfig /release**

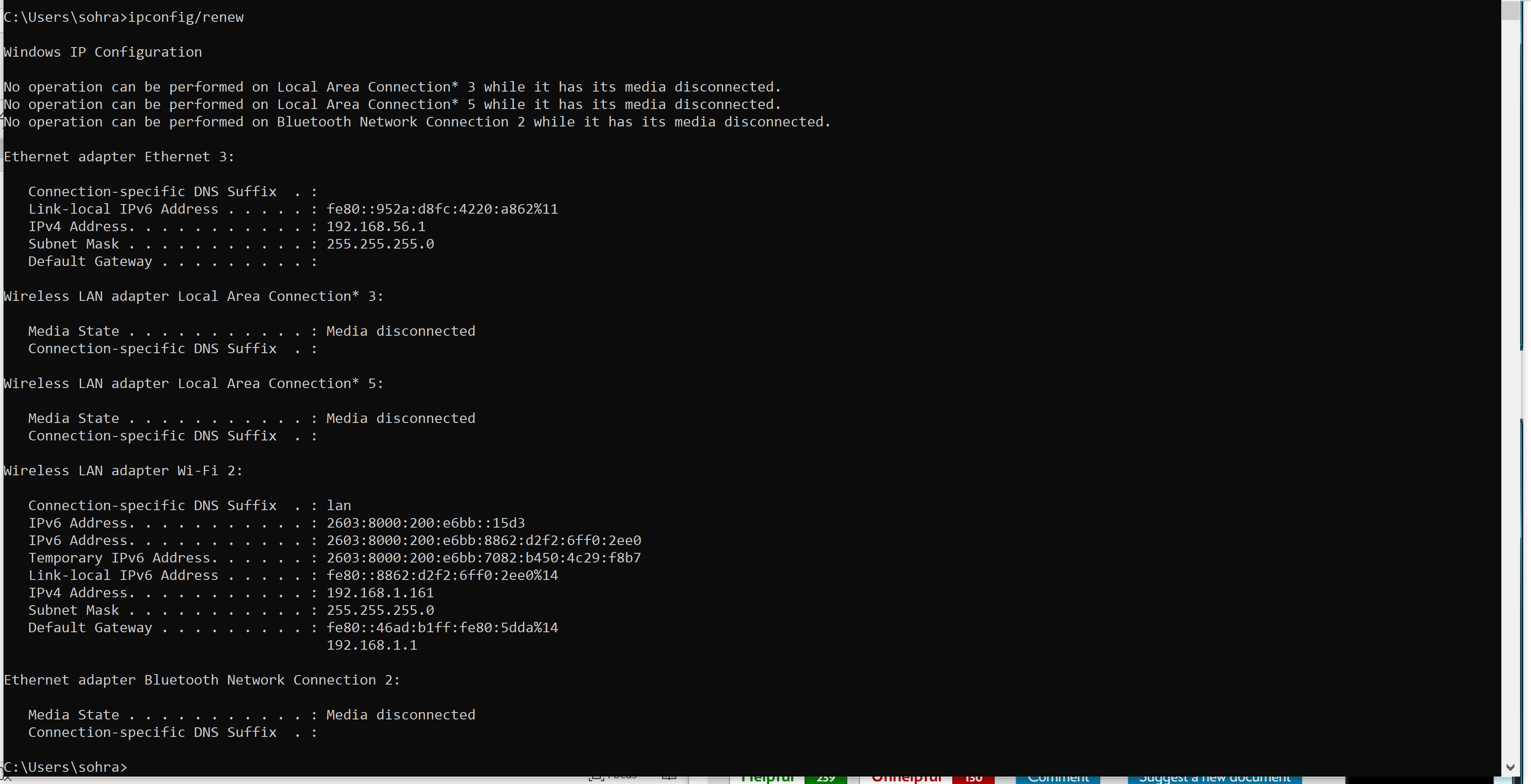
* 1. Provide a screen capture showing the completion of the command.



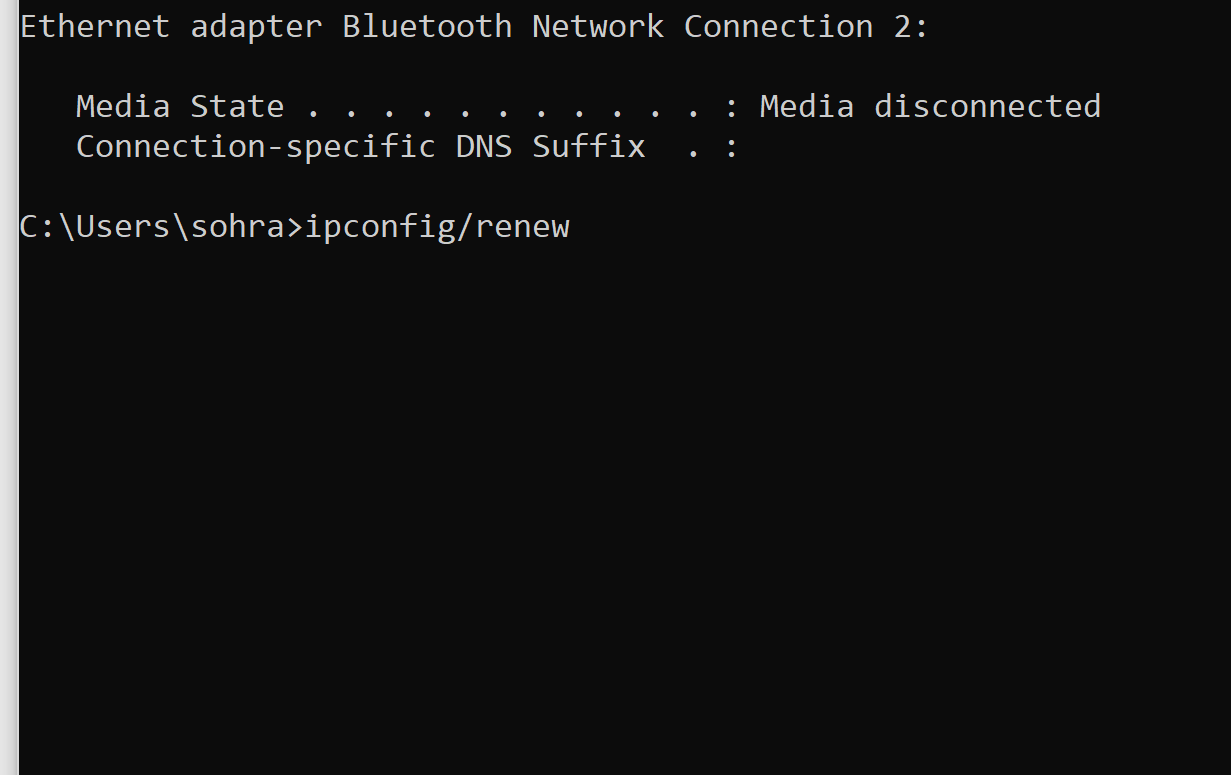
1. Depending on your PC operating system, find and study the command that you can use to **renew** the IP address for the PC.

**ipconfig /renew**

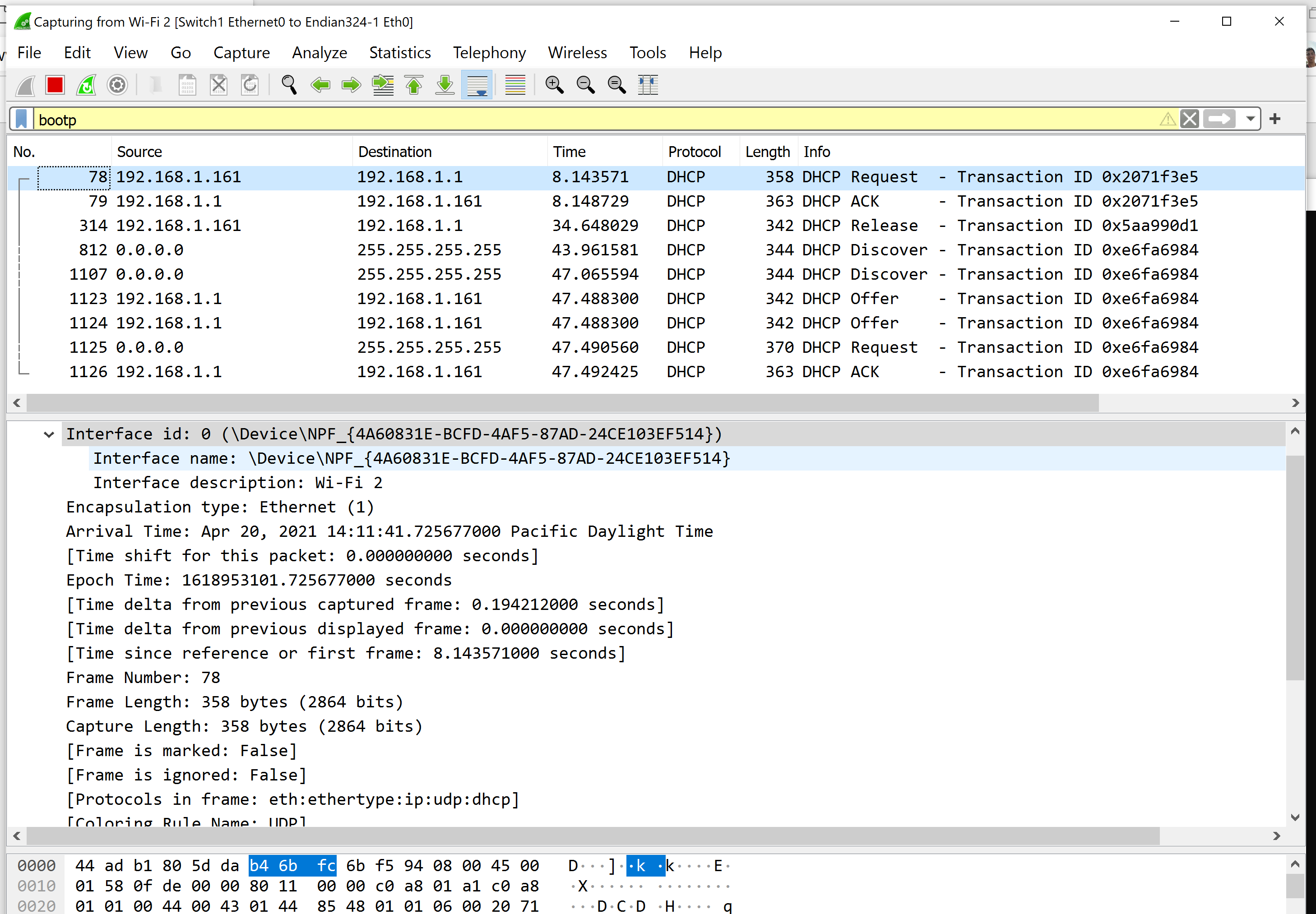
* 1. Provide the complete command line (command with all parameters) you plan to use to renew the IP address for your PC.



* 1. Type the command line above in the terminal window prompt, BUT DO NOT EX- ECUTE IT YET (this is only to get ready for the next step).

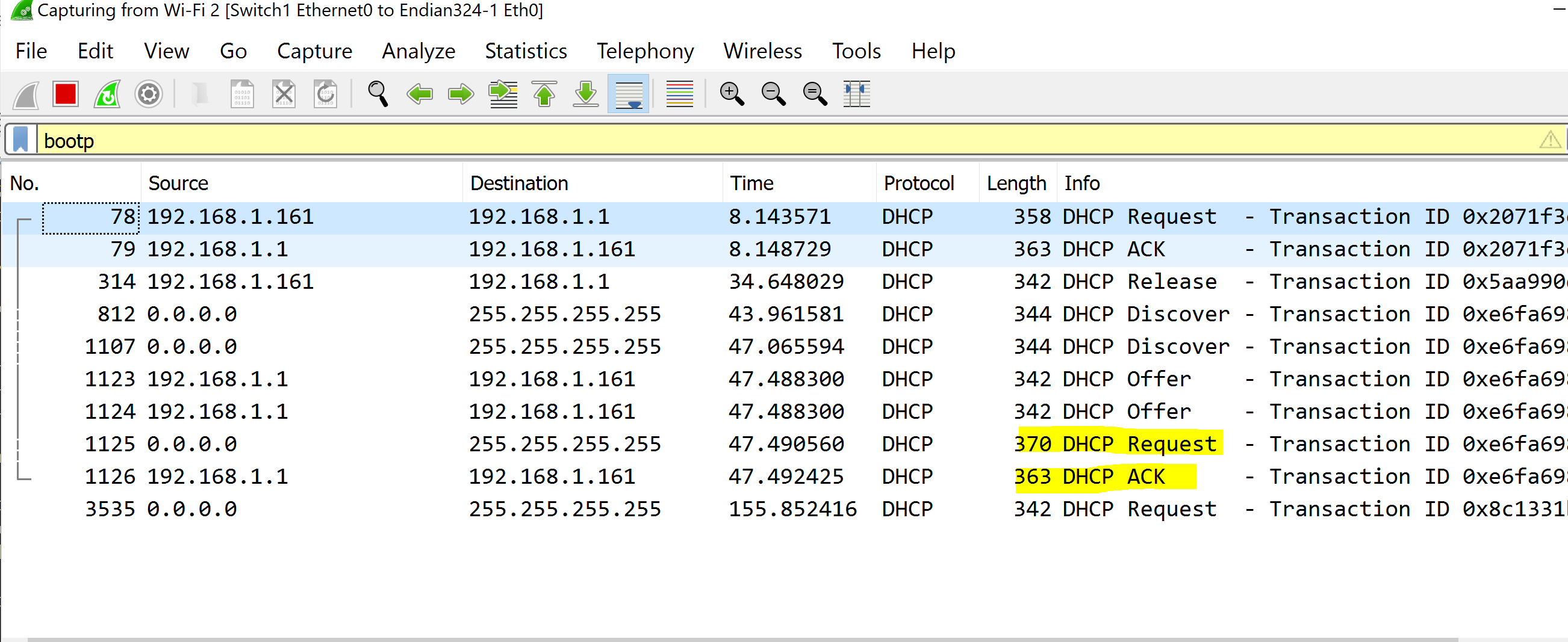


1. Start Wireshark capture using the network interface above, and execute the above IP renew command. Wait until the command completes and then stop Wireshark capture.

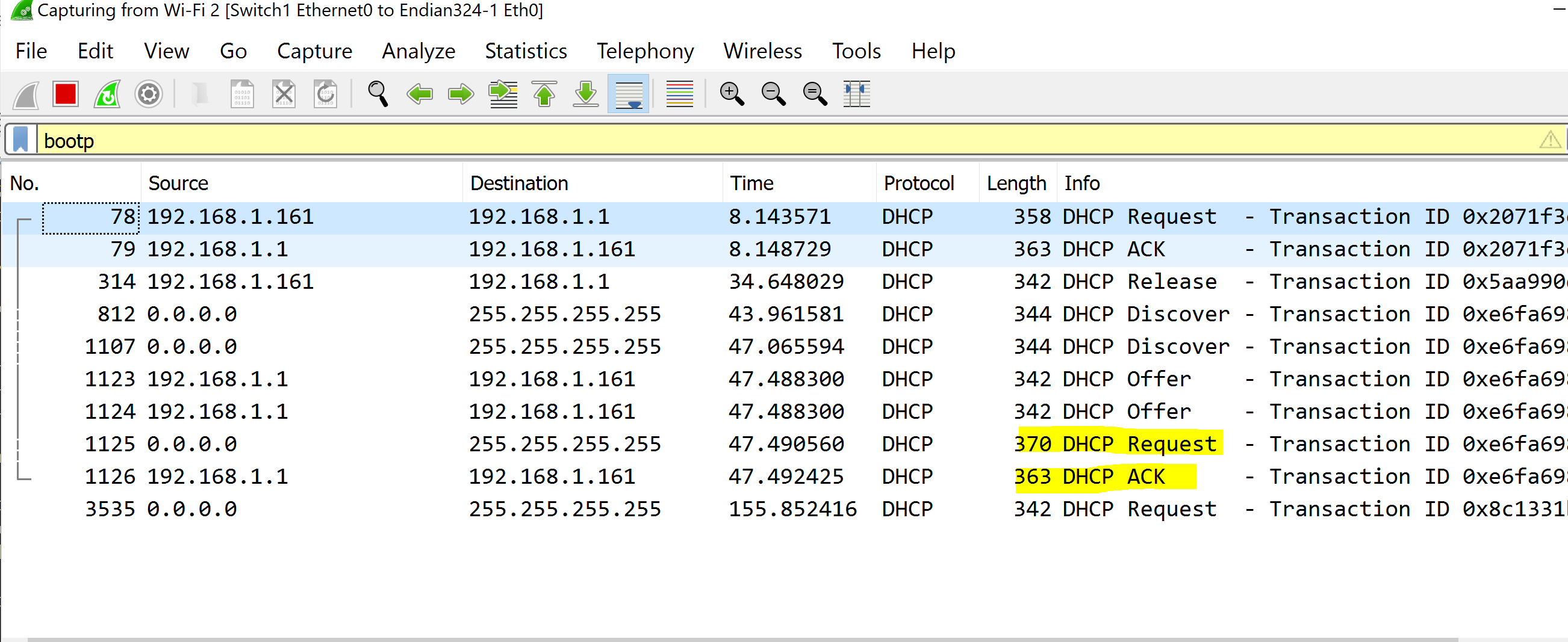


1. From Wireshark capture, locate the corresponding DHCP discover, DHCP offer, DHCP re- quest, and DHCP ACK messages we learned from chapter 4.

Yes I did located it

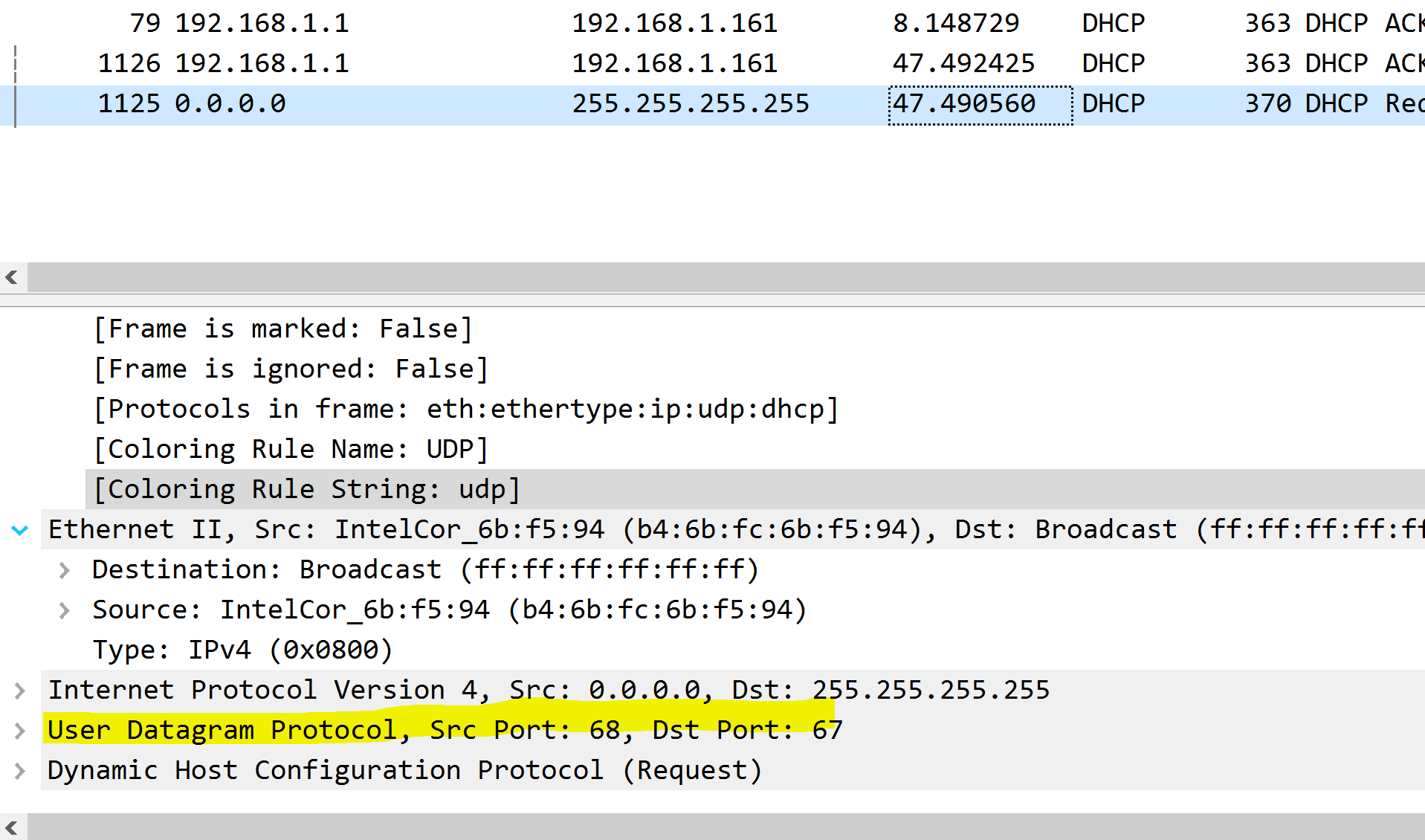


1. Provide a screen capture showing the series of DHCP discover, DHCP offer, DHCP re- quest, and DHCP ACK messages that were captured in Wireshark.



1. Does DHCP use UDP or TCP? What are the source and destination port numbers? Pro- vide screen capture(s) to prove your answer.

It uses UDP and source and destination port is 68 and 67



1. From the Dynamic Host Configuration Protocol Discover message provide the followings
   1. Describe in your own words the purpose of this message.

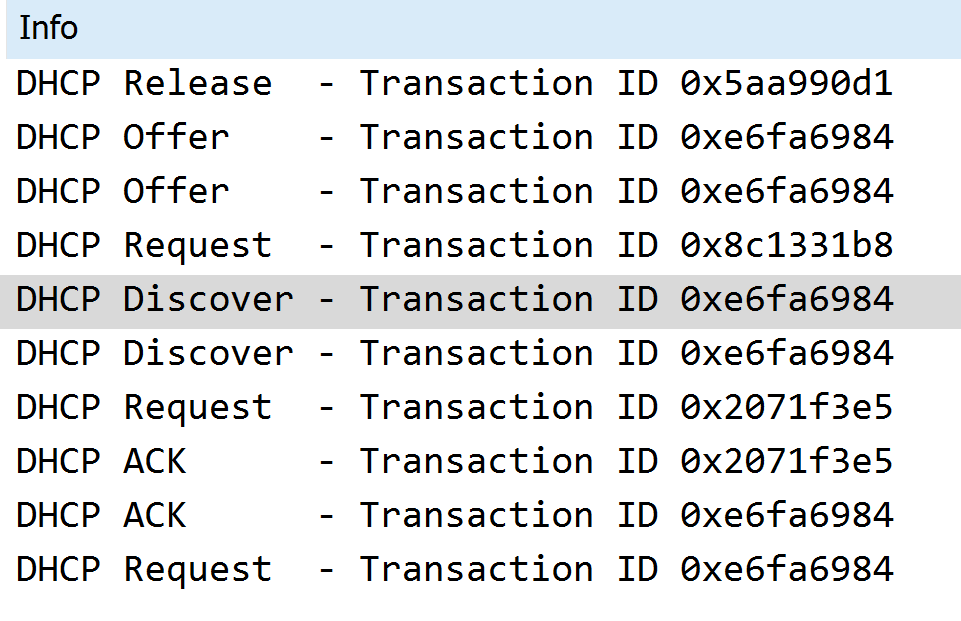
Identify the source and destination IP addresses used in the message and explain the relevance of these values. The purpose of the discover message is to attempt to reconnect to the network

So in DHCP uses Discover which is interaction between Client/ server.

Second uses Offer which is sent by the server to the client in response to a Discover this includes IP address, lease time, and the network configuration parameter to the client. The router line indicates to the client what its default gateway should be. The subnet mask line tells the client which subnet mask it should use.

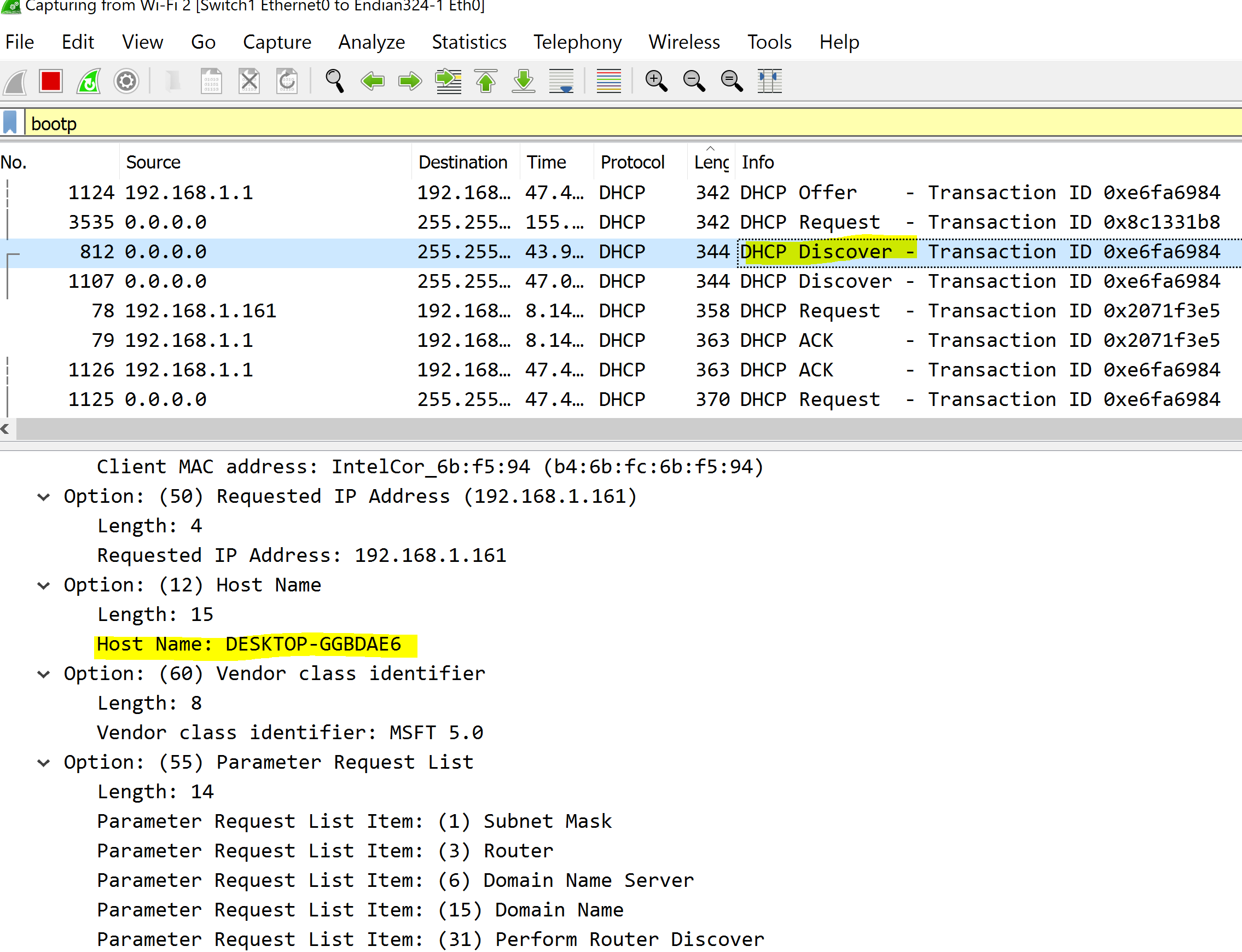
Source IP = 0.0.0.0. Destination: 255.255.255.255. The source is the PC and the destination is the local network.

ACK is sent by the server to the client which acknowledging the request.

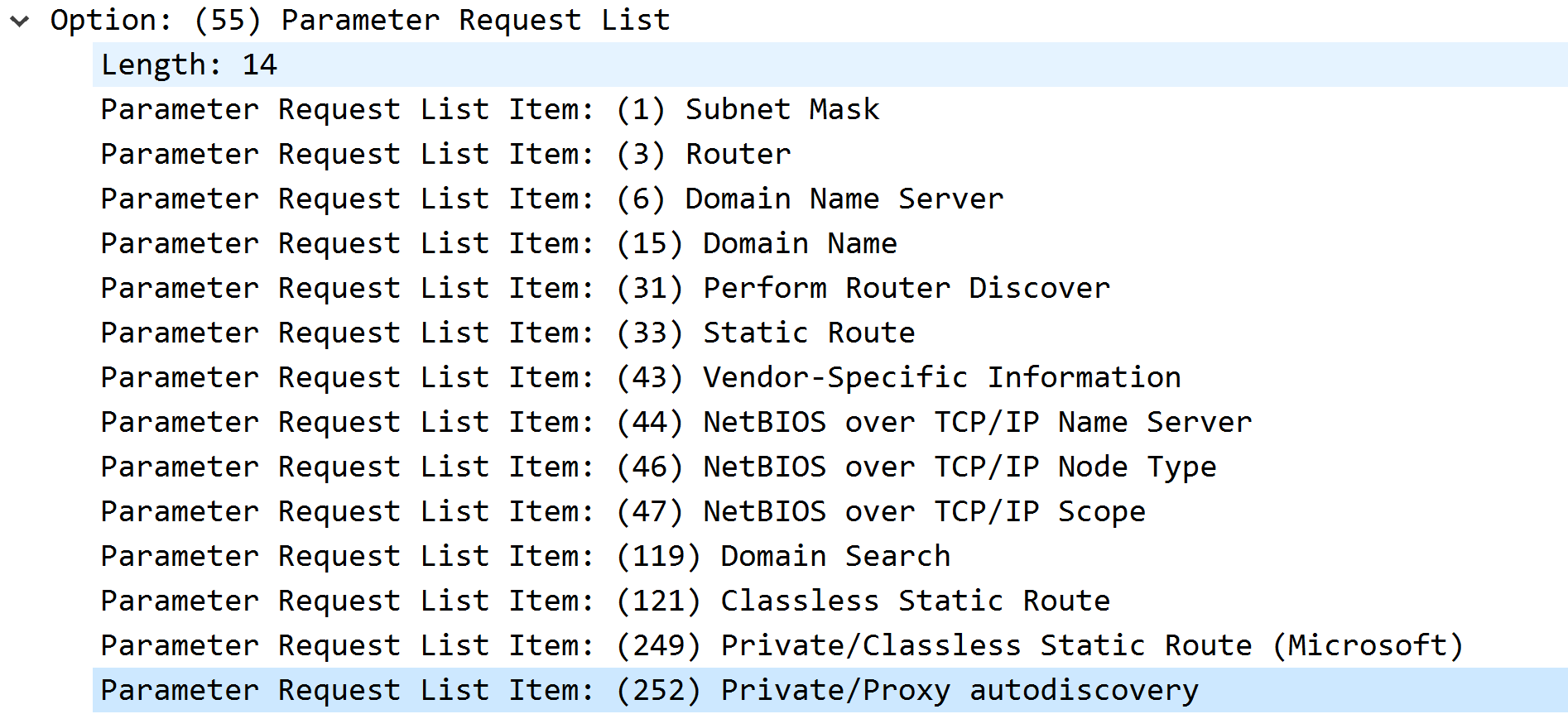


* 1. Does this message contain the host name of the requesting PC?

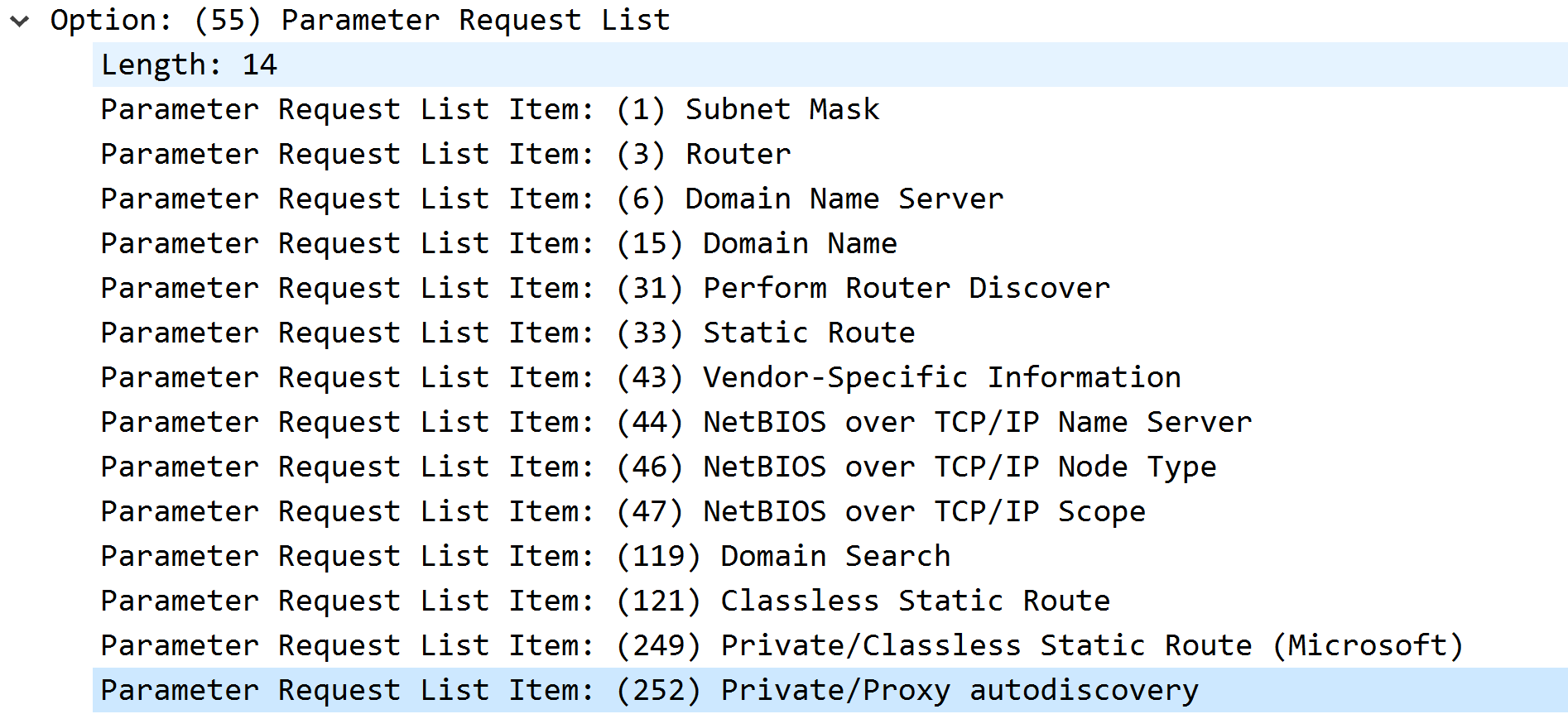
YES



* 1. List the items requested by the PC.



* 1. Provide screen capture(s) that are relevant to your answers above.



1. From the Dynamic Host Configuration Protocol Offer message provide the followings
   1. Describe in your own words the purpose of this message. Identify the source and destination IP addresses used in the message and explain the relevance of these values.

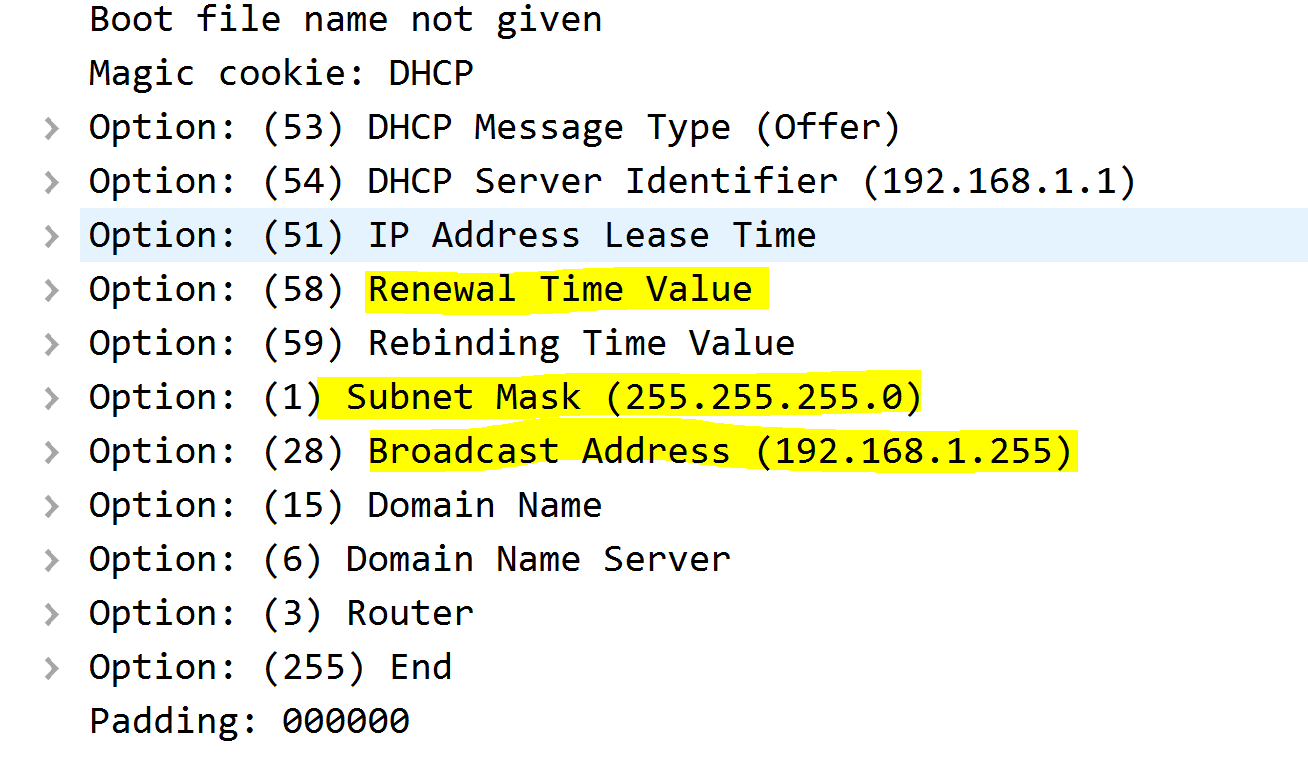
Second uses Offer which is sent by the server to the client in response to a Discover this includes IP address, lease time, and the network configuration parameter to the client.

DHCP servers on a network that receive a DHCP Discover message respond with a DHCP Offer message, which offers the client an ipv4 lease.

* 1. List the items offered by the DHCP server.

Ip address, subnet musk

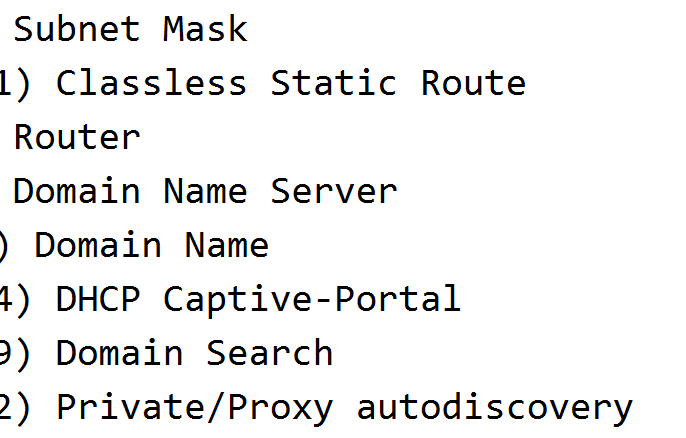
* 1. Provide screen capture(s) that are relevant to your answers above.



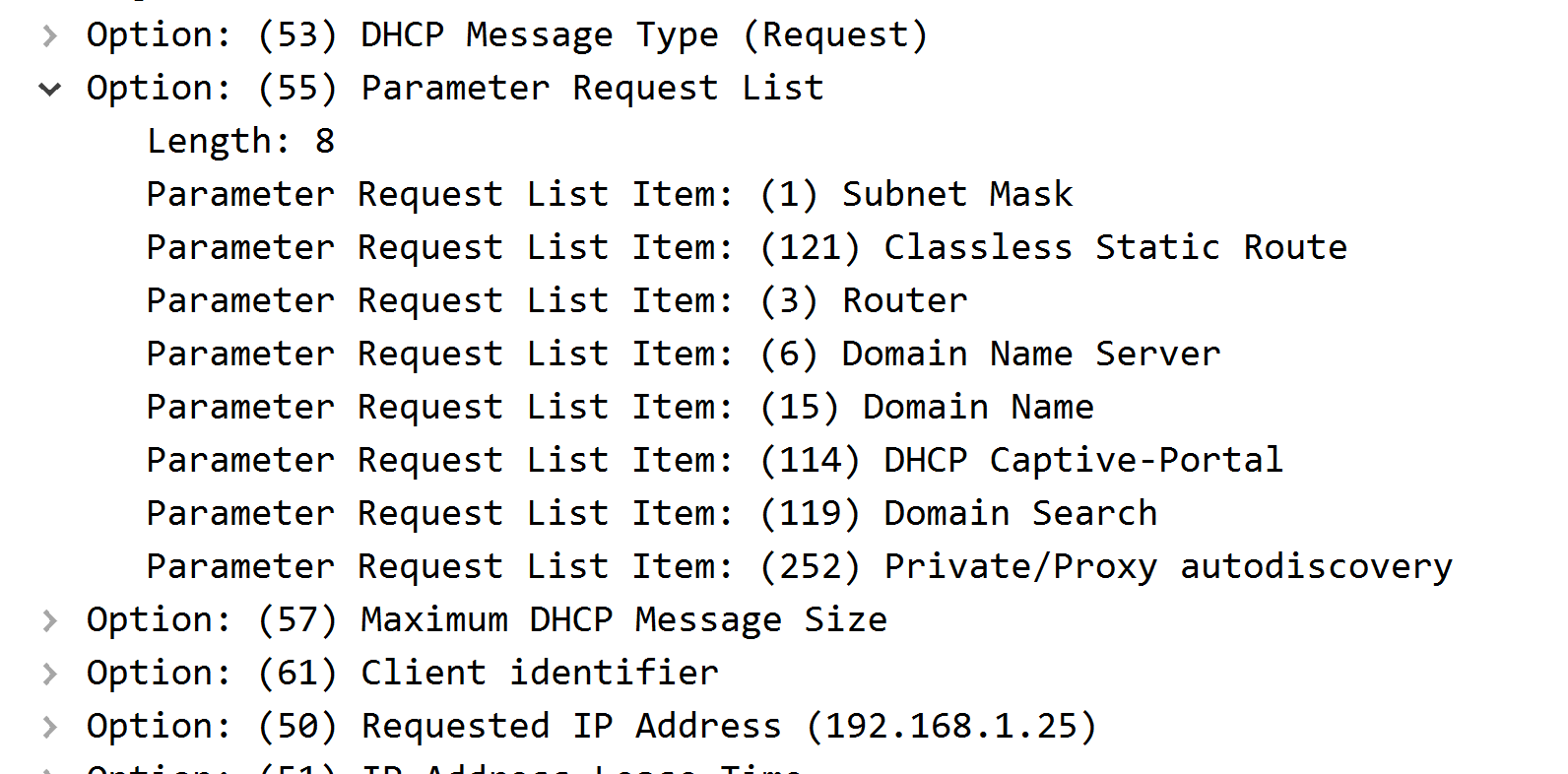
1. From the Dynamic Host Configuration Protocol Request message provide the followings
   1. Describe in your own words the purpose of this message. Identify the source and destination IP addresses used in the message and explain the relevance of these values.

The dhcp request message may contain the IP address that the client will use and dhcp request message is sent broadcast using 255.255.255.255 IP address. The transaction in a dhcp request message will be used to associate this message with previous message send by this client.

* 1. List the items requested by the PC.



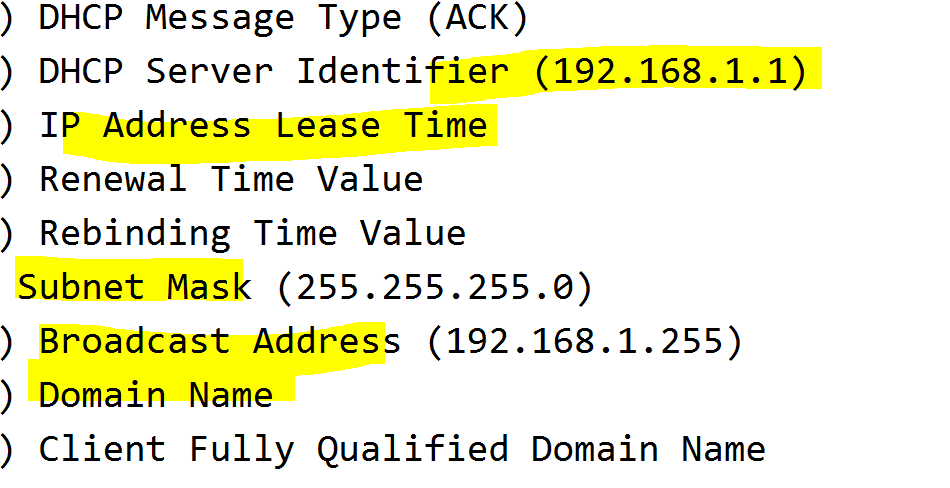
* 1. Provide screen capture(s) that are relevant to your answers above.



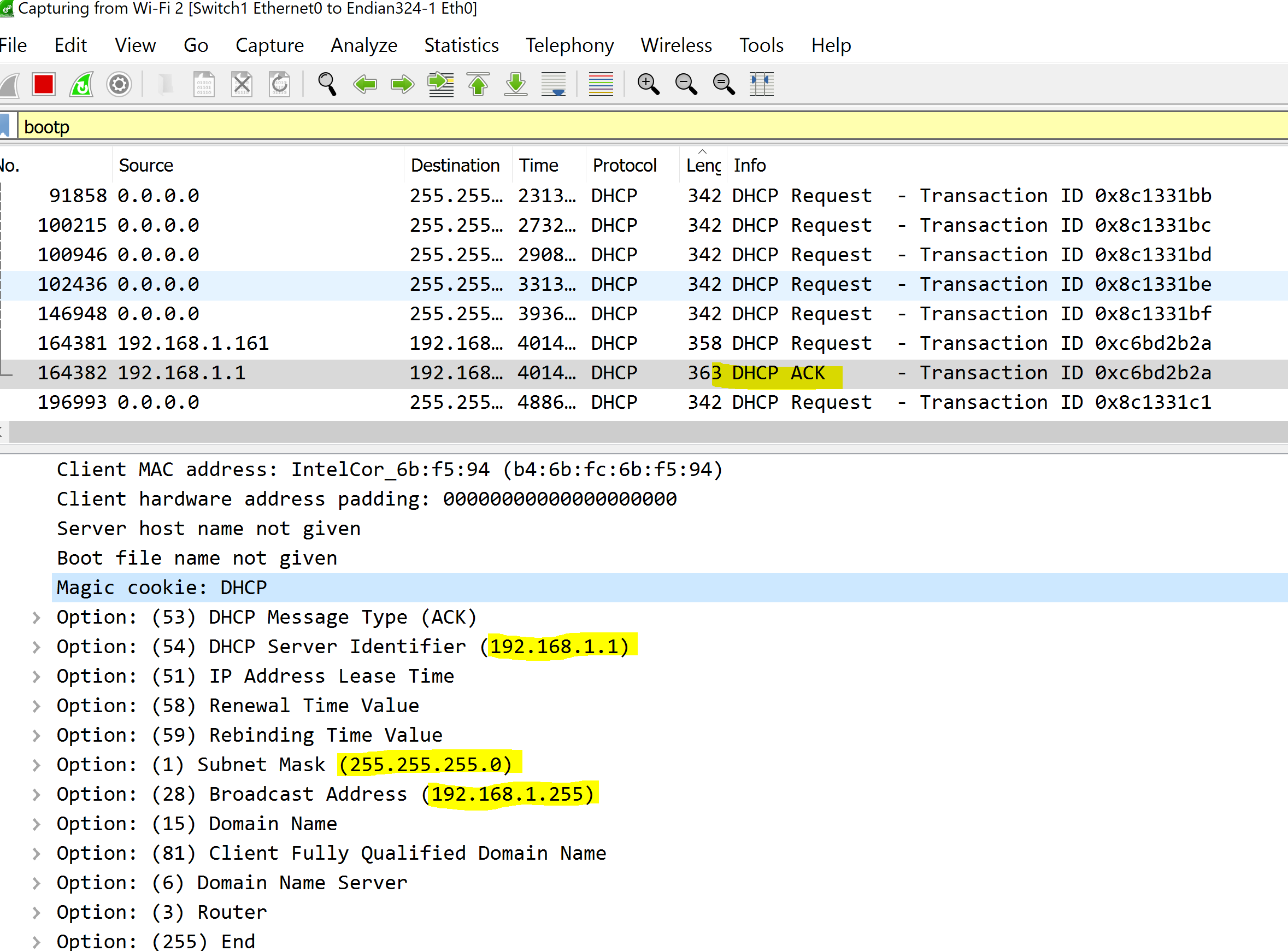
1. From the Dynamic Host Configuration Protocol ACK message provide the followings
   1. Describe in your own words the purpose of this message. Identify the source and destination IP addresses used in the message and explain the relevance of these values.

The DHCP Ack message is the last message sent which including network configuration data such as the client IP address, subnet mask, default gateway IP address, DNS IP address and lease time, to the client. Once this process is completed, the client can keep its current IP address for the extended lease time as specified in the DHCP Ack message. Ack can identify the DHCP server using the server’s ip address which is effective method.

* 1. List the items confirmed by the DHCP server.



* 1. Provide screen capture(s) that are relevant to your answers above.



ADDRESS RESOLUTION PROTOCOL (ARP)

Observe the events occurring right after the DHCP handshake. Did you see the ARP messages?

ARP stands for Address Resolution Protocol. Use the World-Wide Web to find out about ARP and answer the following questions.

1. What ARP is used for?

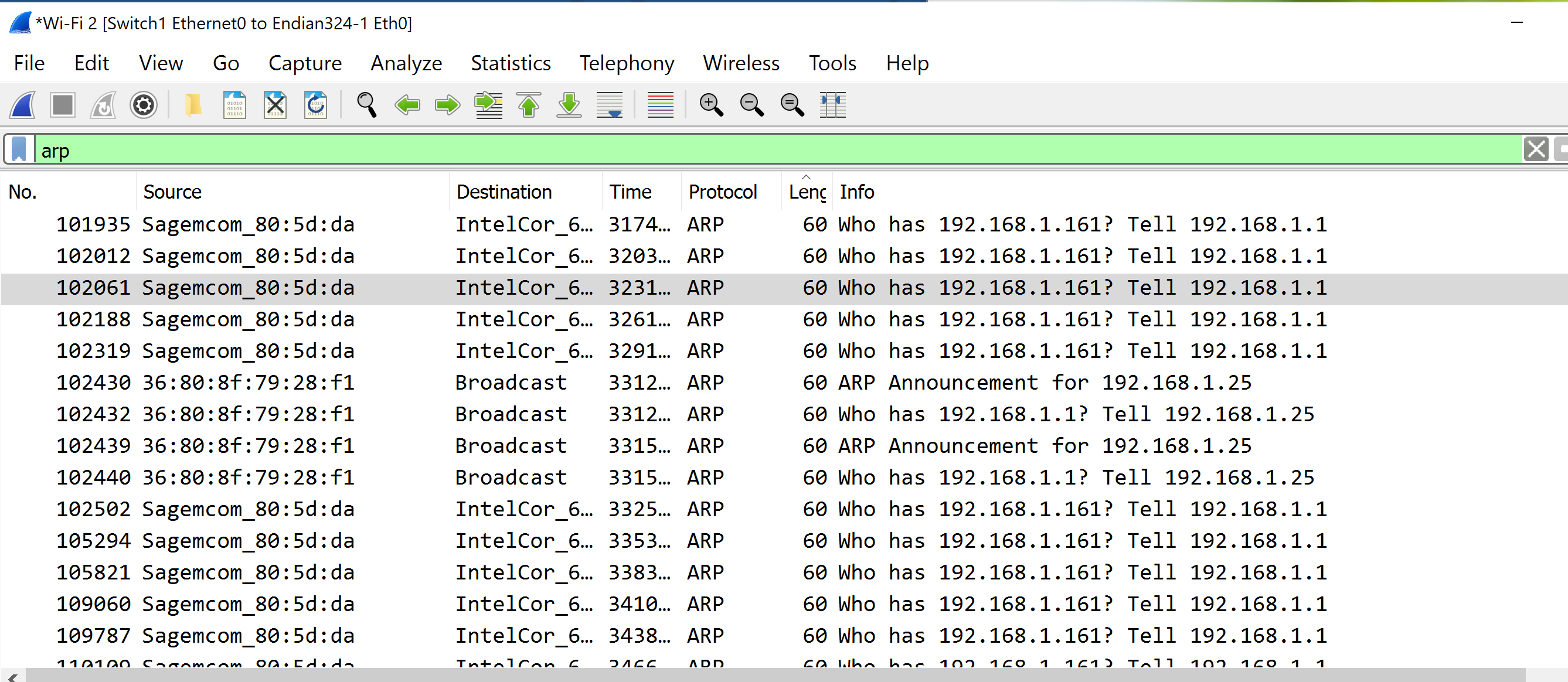
ARP is used to dynamically discover the mapping of layer 3 and layer 2 and it works between OSI network and OSI link layers.

1. Why is ARP needed?

ARP provides information about physical address of a particular IP. If there is a device which requests for a physical address of an IP, it sends an ARP request. If there is a physical address present in that network, then its address is given to the device which is requesting.

1. Explain the sequence of ARP message exchanges seen from Wireshark capture and pro- vide screen capture(s) that are relevant to the details of your answer.

Viewing an ARP cache on a PC displays the IPv4 address and the MAC address of each device on the LAN with which the PC has exchanged ARP messages.



1. Is ARP secure? Explain your answer and provide an example to illustrate your reasoning that ARP is secure or non-secure.

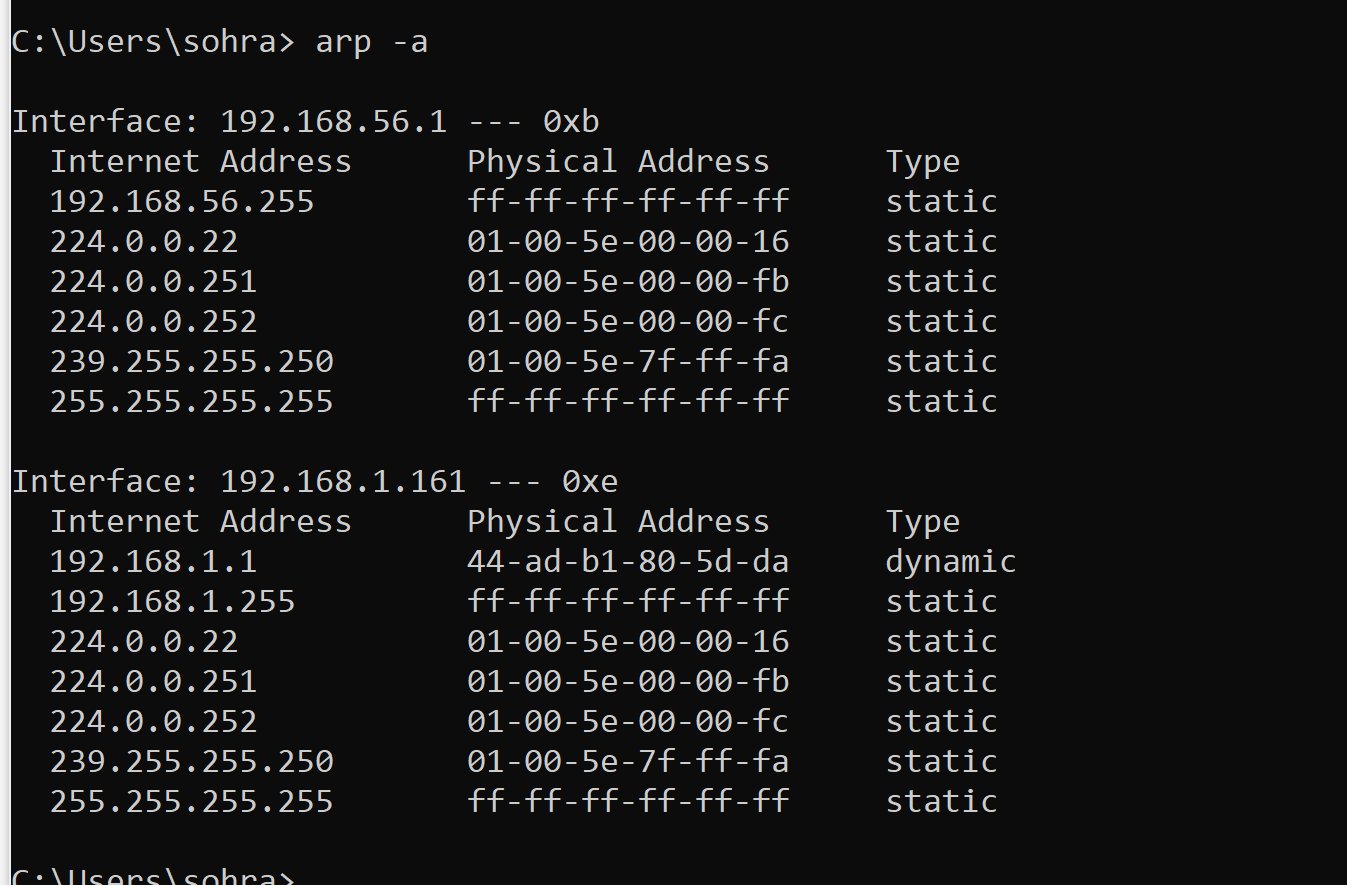
No it is not secure since any one can send a fake ARP messages to a LAN with the intention of linking their MAC address with the IP address and this link would allow the data from the victim’s computer to be sent to the attacker’s computer. And there have been dangerous attacks done using arp messaging and it is proven. Second ARP is not designed for security

1. Describe what is an ARP attack?

ARP attack are also known as Poisoning where this allows the attacker to intercept communication between network devices. Where this attack must have access to the network where this will allow the attacker to access to IP addresses. So ARP attack is where the someone can get in to your computer network using fake arp messages via LAN and starts collecting all kinds of data and example is pushing dangerous malicious file to workstations across the network.

1. Describe a method to detect an ARP attack and present a system command that can be used to identify or confirm that ARP attack had occurred.

To detect an ARP attack we can use command arp -a in computer command prompt and you will get this



1. Describe a way to prevent ARP attacks and identify the positives and negatives of such method.

To prevent ARP attacks we must use VPN which stands for virtual private network

This allows the network to internet through secure and encrypted tunnels.

Second someone can use Static ARP this will prevent the device from being listed in Arp responses.

Third use packet filtering this will identify all the attacks and will stop them before they reach the devices.

End of Project 3