Birla Institute of Technology & Science, Pilani
Pilani Campus
Department of Computer Science and Information Systems

COMPUTER NETWORKS (CS F303)
SECOND SEMESTER 2022-23
LAB-SHEET -
TOPIC: Exploring DHCP and ARP using Wireshark

Learning Objectives:

- **To learn about DHCP and understand its working using Wireshark.**
  - Triggering DHCP Packets by releasing and renewing IP information.
  - Analyze DHCP Packers in Wireshark
- **To learn about ARP and understand its working using Wireshark.**

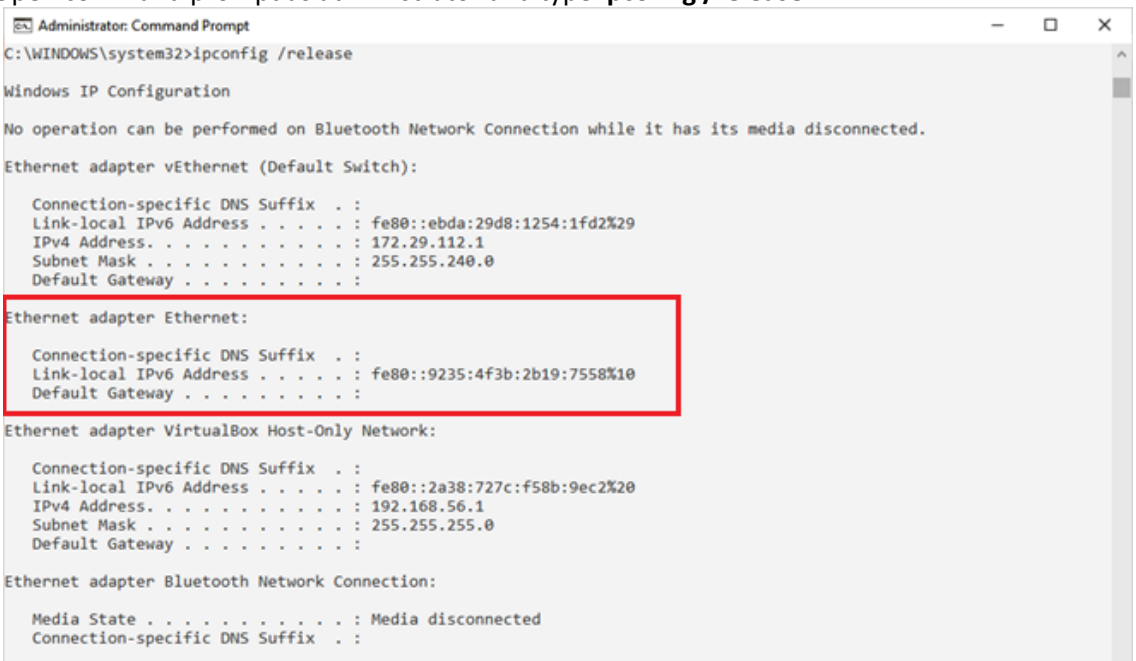
Dynamic Host Configuration Protocol (DHCP):

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses and other network configuration information to hosts. The other network configuration information includes subnet mask information, default gateway IP addresses and domain name system (DNS) addresses.

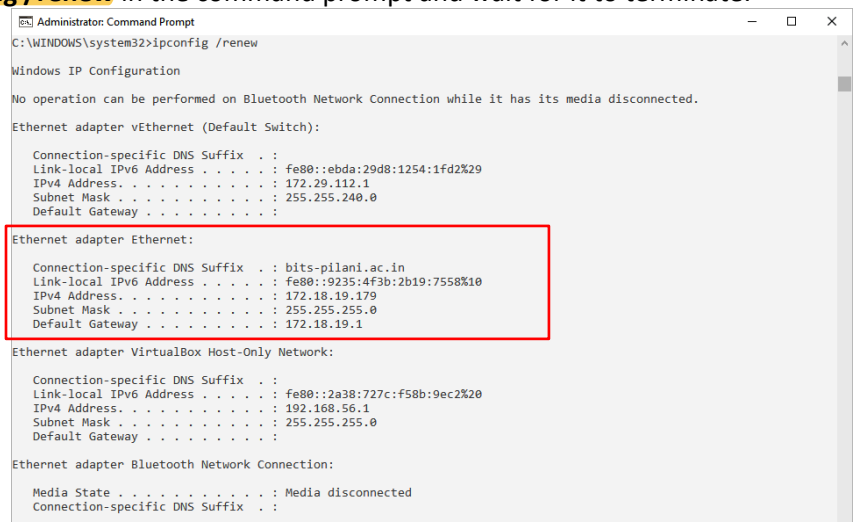
First, we take a quick look at DHCP. A DHCP server access is required to make configuration changes and see DHCP in action. Hence, we will only examine DHCP packets that are captured by a host.

The system you are using already has an IP address assigned to it. To see DHCP packets in your system's network capture, we must release the DHCP supplied network configuration and renew it. Following steps will help you perform this experiment.

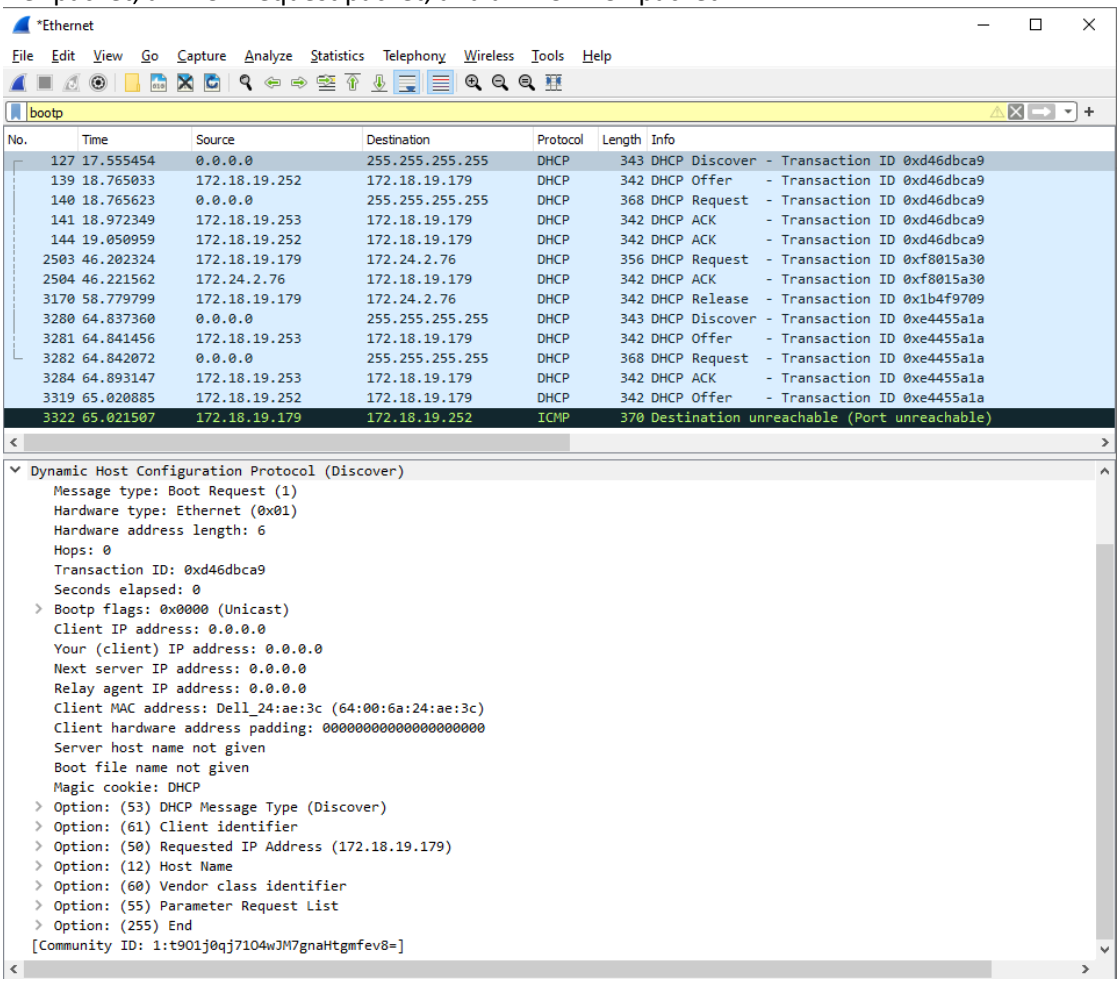
1. Release current IP address:
   Open command prompt as administrator and type **ipconfig /release**



2. Start Wireshark packet capture.
3. Renew IP address:
   Type **ipconfig /renew** in the command prompt and wait for it to terminate.



4. DHCP packets can be filtered in Wireshark using "**bootp**". From the figure below, we can see that the first ipconfig renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.



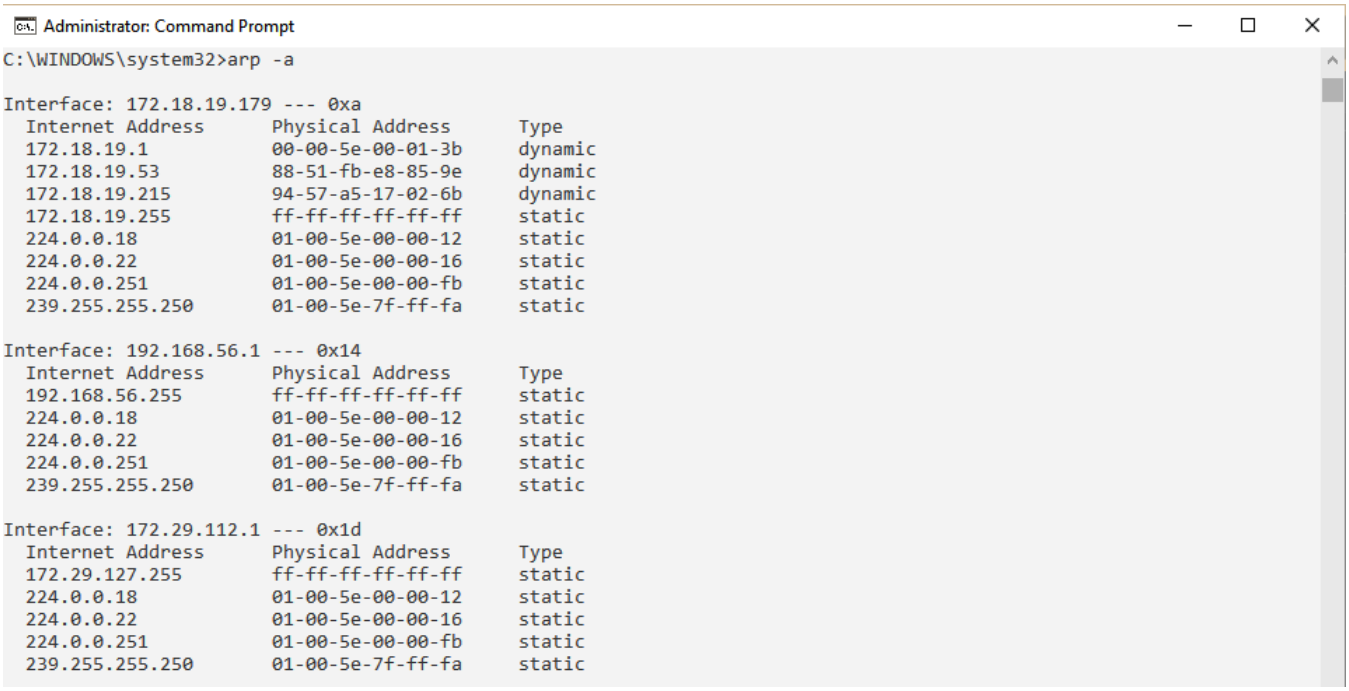
Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?
2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?
3. What is the link-layer (e.g., Ethernet) address of your host?
4. What values in the DHCP discover message differentiate this message from the DHCP request message?
5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
7. What is the IP address of your DHCP server?
8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so, what is the IP address of the agent?
10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?
12. Explain the purpose of the lease time. How long is the lease time in your experiment?
13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?
14. Clear the **bootp** filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

Address Resolution Protocol (ARP):

The ARP protocol maintains a cache of IP-to-Ethernet address translation pairs on your computer. The **arp** command (in both MSDOS and Linux/Unix) is used to view and manipulate the contents of this cache. Since the **arp** command and the ARP protocol have the same name, it's understandably easy to confuse them. But keep in mind that they are different - the **arp** command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on message transmission and receipt.

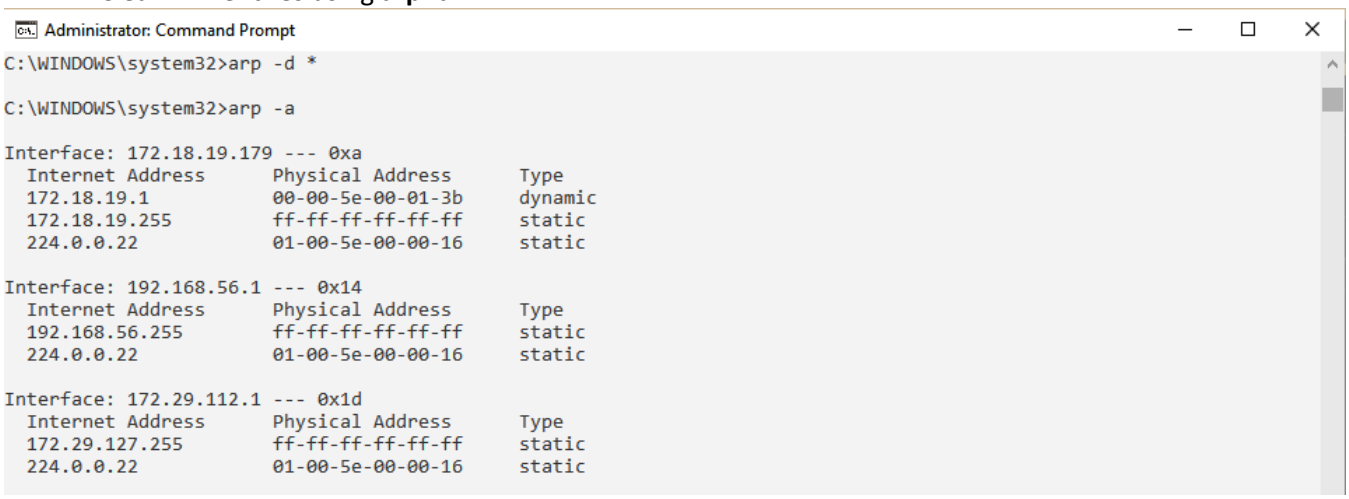
We can check ARP entries using **arp -a** in command prompt/terminal.



Write down the contents of your computer's ARP cache. What is the meaning of each column value?

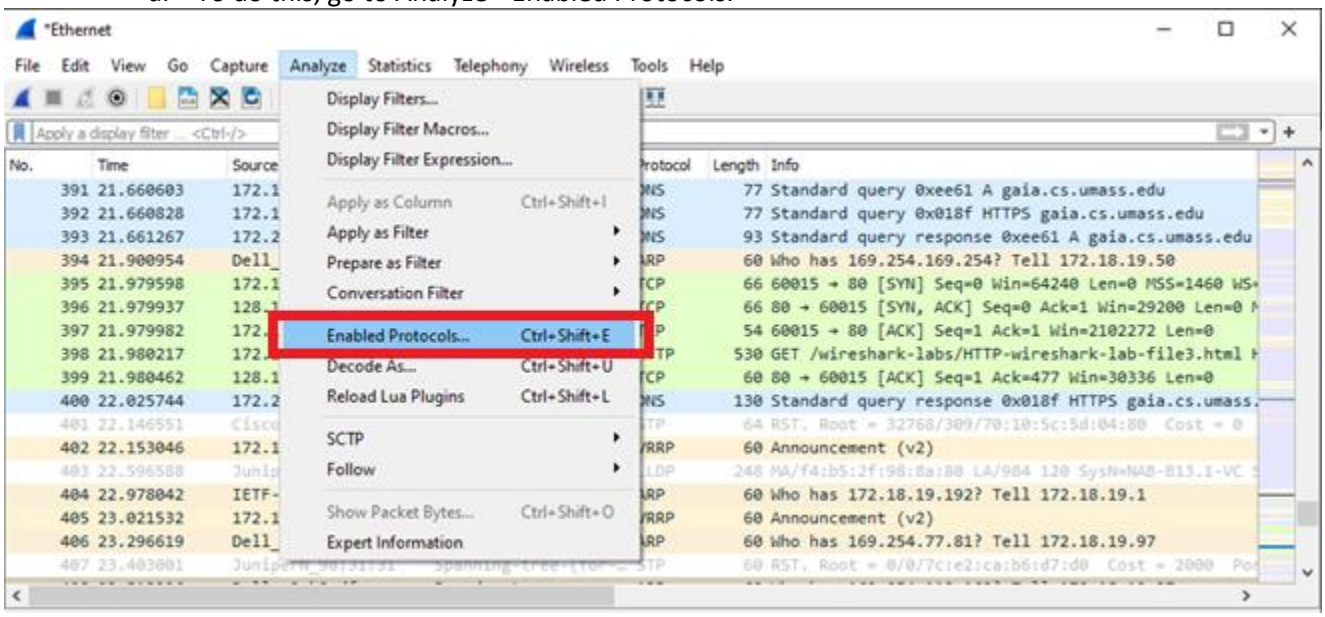
Now, lets perform an experiment to capture and analyze ARP packets in Wireshark.

1. Clear ARP entries using **arp -d ***

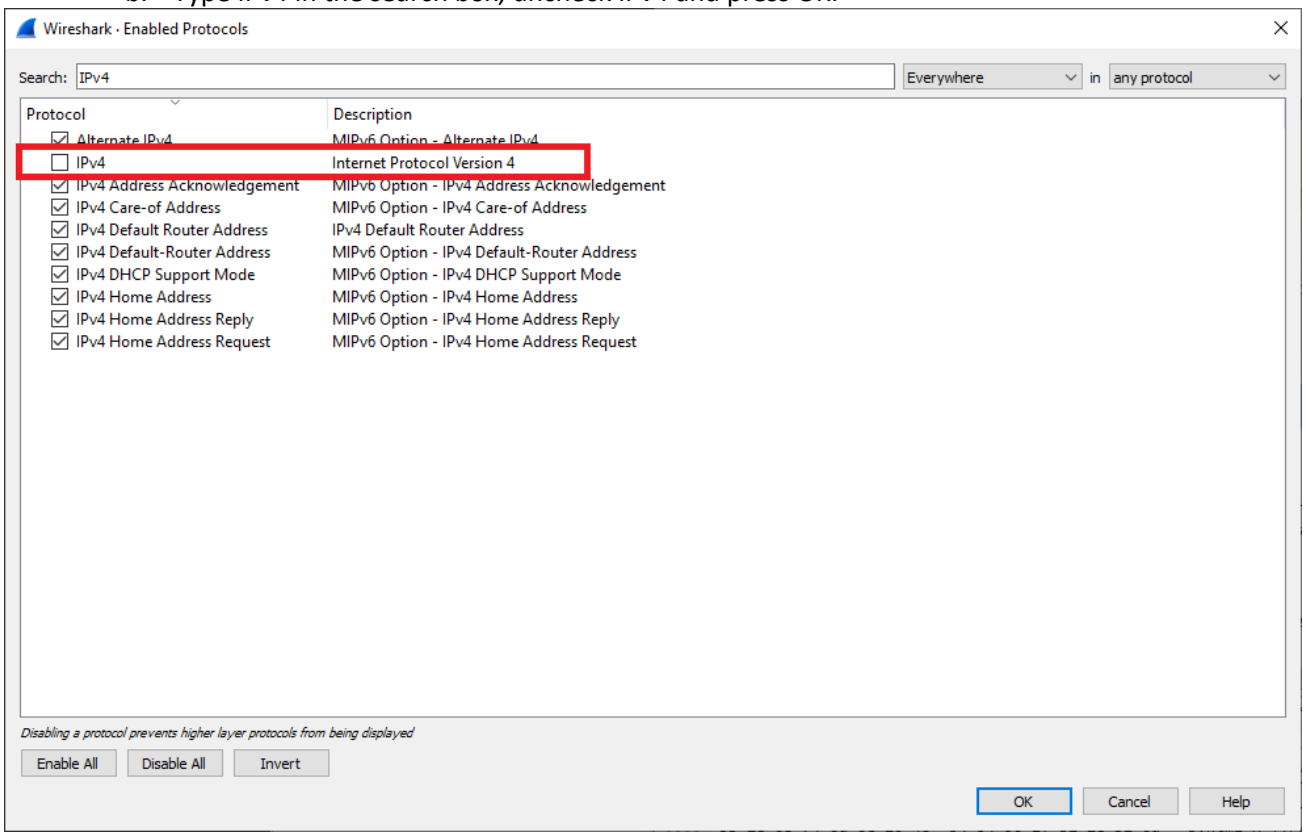


2. Clear cache of the browser or open incognito mode.
3. Start Wireshark Packet Capture
4. Visit the Website: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html
5. Stop the Wireshark packet capture.
6. (optional) The ARP entries are repopulated and can be checked by entering **arp -a** in the command prompt or terminal.

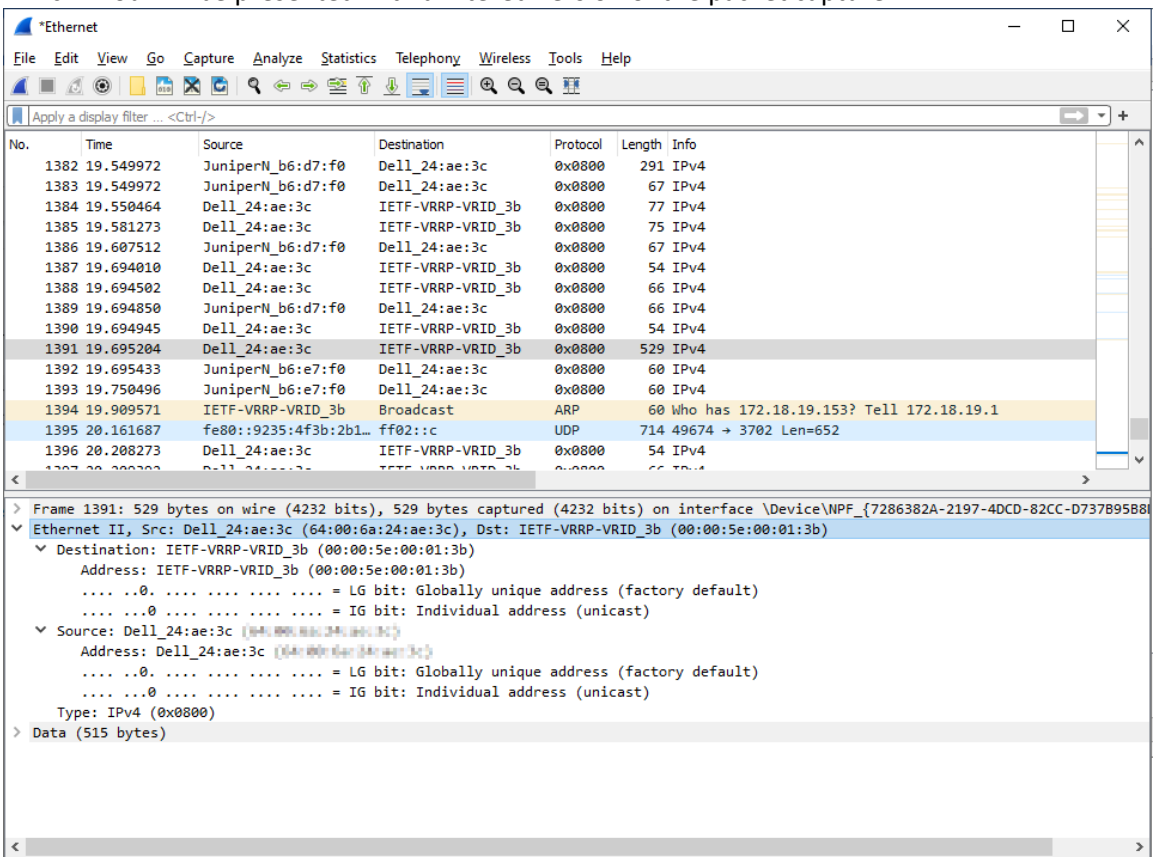
7. Back in Wireshark, type “http” in the display filter to filter out the packets corresponding to the HTTP request for accessing the website. Note down the packet numbers for the GET request and OK response.
8. Filter and remove higher layer protocols by unselecting the IP protocol from Enabled Protocols for display in Wireshark.
    a. To do this, go to Analyze->Enabled Protocols.



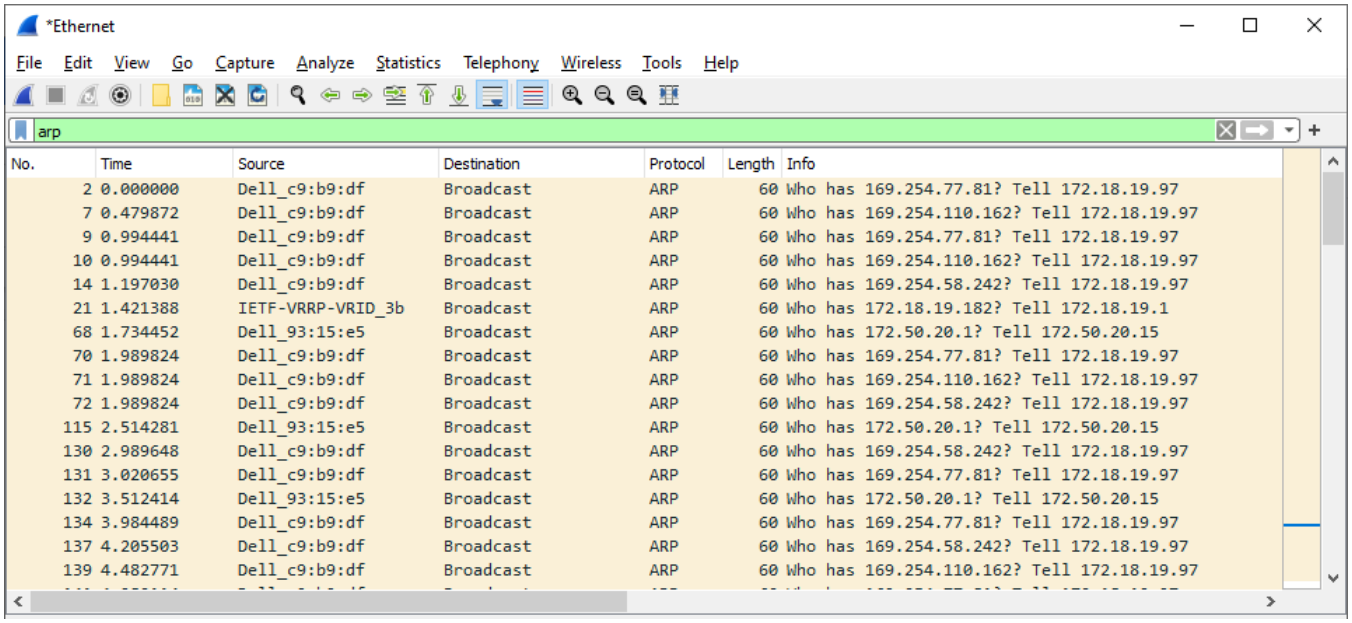
    b. Type IPv4 in the search box, uncheck IPv4 and press OK.



c. You will be presented with a filtered version of the packet capture.



9. Type “arp” in the search box to further filter out the packets from the capture. Look for packets that have packet number between the request and response packet numbers of the HTTP request for accessing the website.



Now answer the following questions:

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
2. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
3. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html
    a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
    b. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
    c. Does the ARP message contain the IP address of the sender?
    d. Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
4. Now find the ARP reply that was sent in response to the ARP request.
    a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
    b. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
    c. Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
5. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

*****