**IFT 166 Introduction to Internet Networking**

**Lab 20**  
**Examining DNS Traffic**

Co-authored by Nolan Flatt

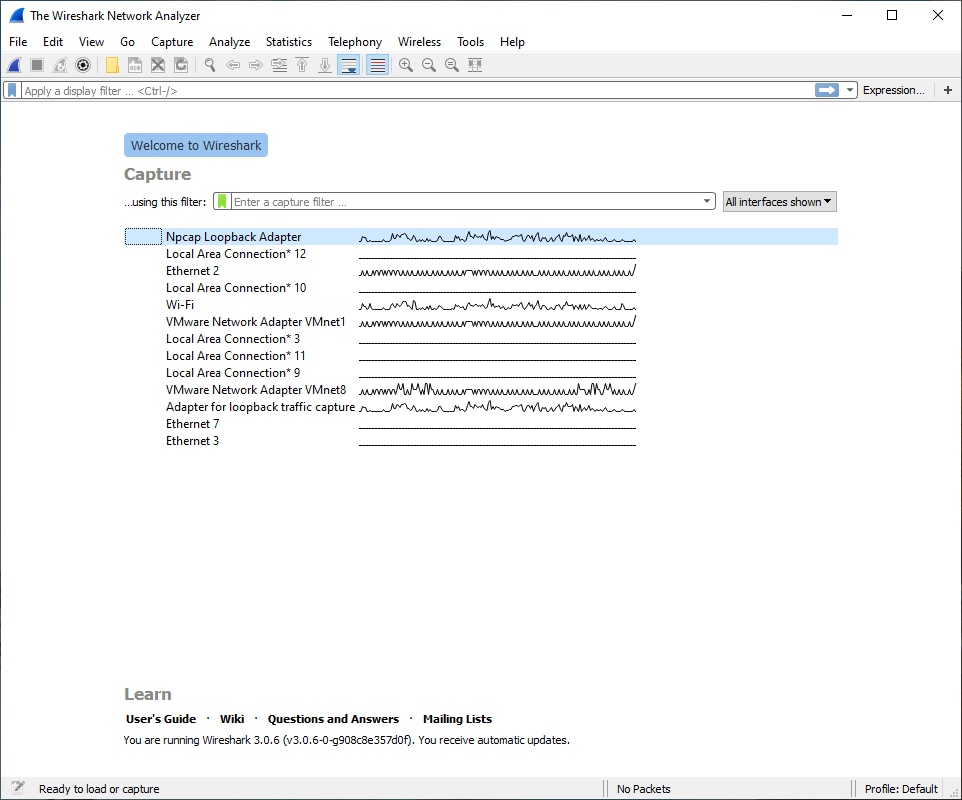
**Note:** If you do not have Wireshark installed, please visit <https://wireshark.org> and download it from there.

**Overview**

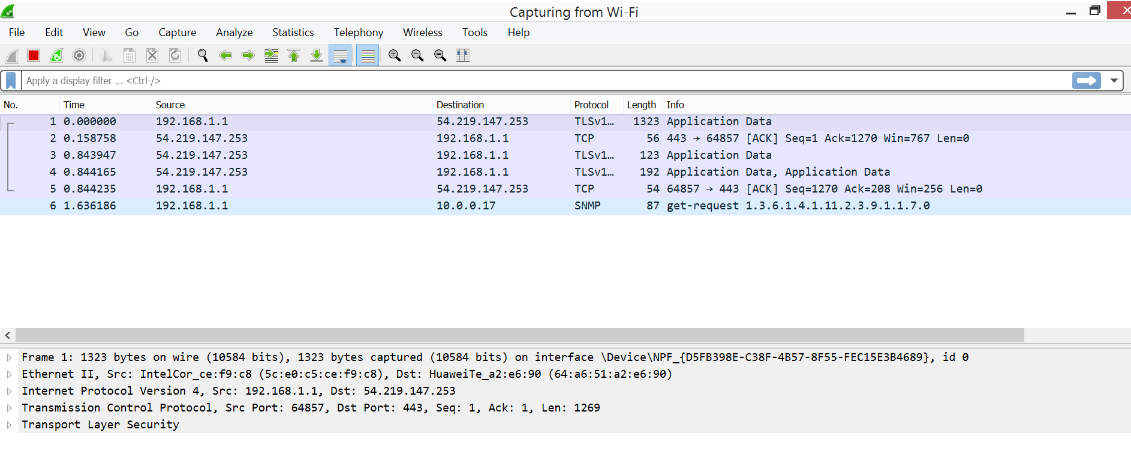
* Part 1: DNS Traffic Capture
* Part 2: DNS Query Traffic Explore
* Part 3: DNS Response Traffic Explore

**Part 1: DNS Traffic Capture**

1. Open **Wireshark** and double click on the **network interface with traffic** that you primarily use to connect to the Internet (Ethernet, Ethernet 2, Wi-Fi). In this example, Wi-Fi is the primary network interface with traffic that I am currently connected to.

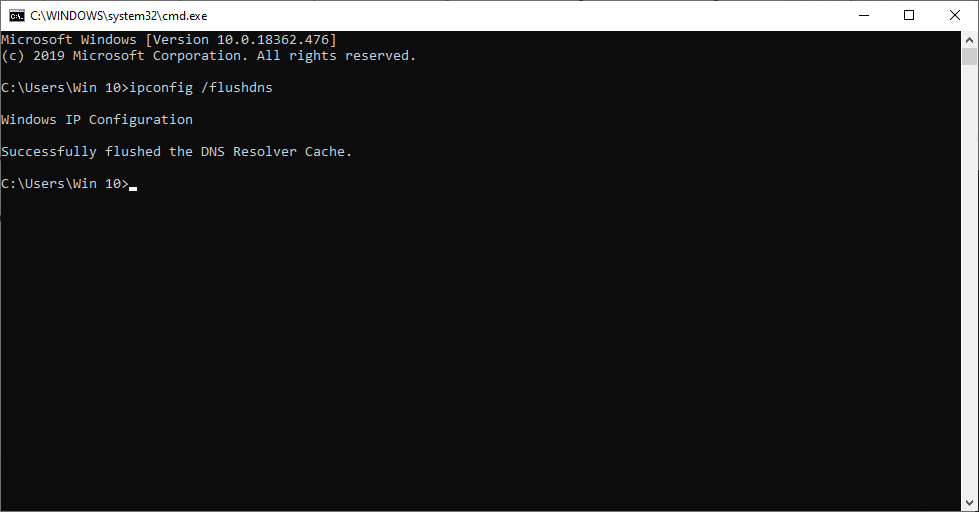


****

1. A screen like the one below will be displayed, showing information about the packets being captured on this interface.

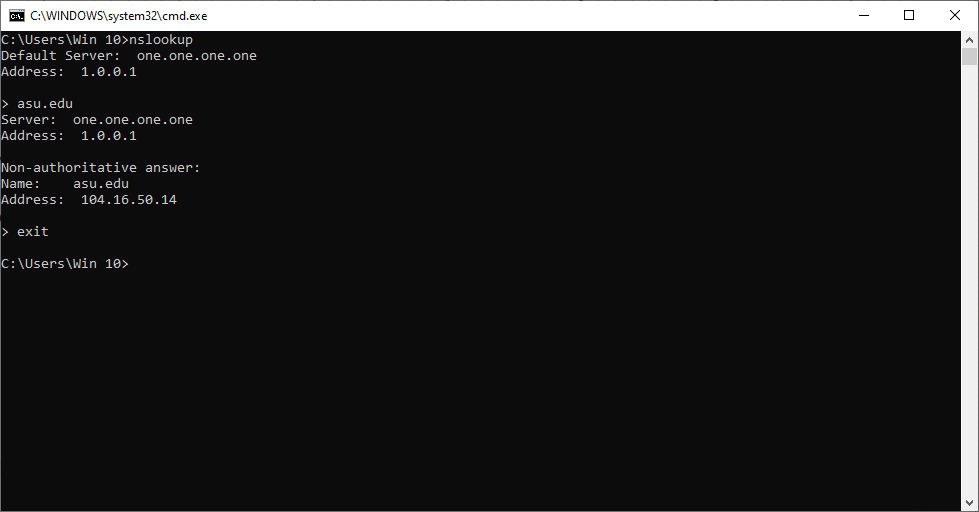
****

1. We will now start capturing packets on Wireshark. First we will stop capturing packets and then we will start a new capture “Start the capture” and carry out Steps 4 & 5.
2. In your local command prompt, type the command **ipconfig /flushdns** and press Enter to execute the command.



****

1. Type the command **nslookup** and press **Enter** to go into the interactive mode. Enter a website’s domain name (asu.edu, duckduckgo.com). In this example, the domain [www.asu.edu](http://www.asu.edu) is used. Type the command exit and close Command Prompt when finished.



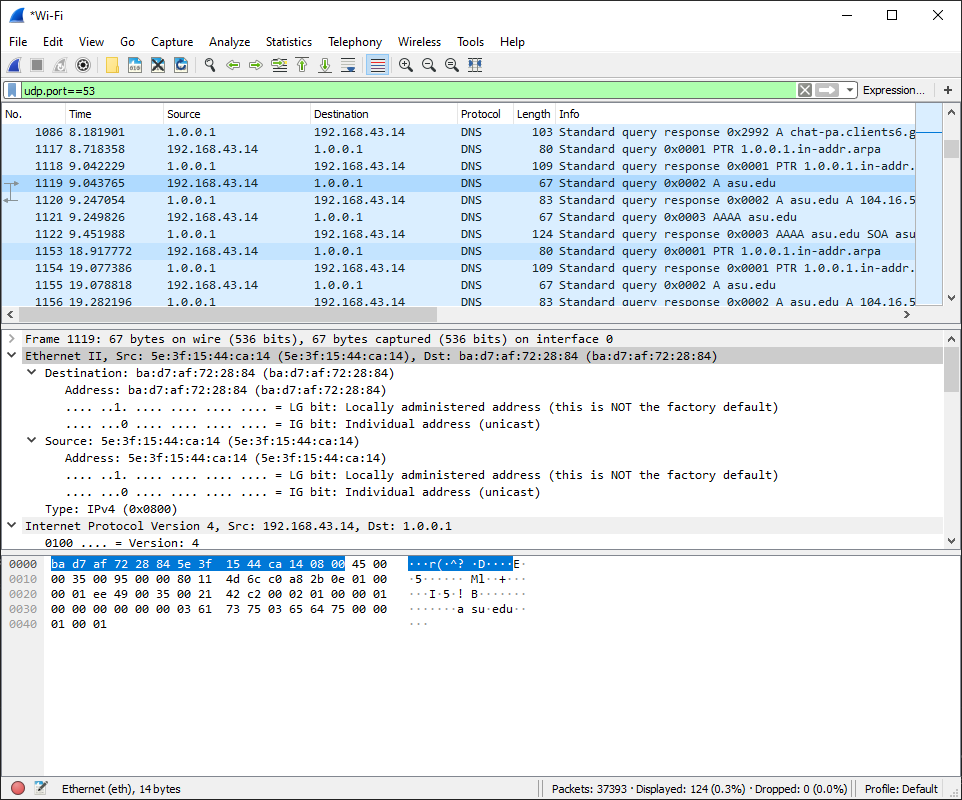
****

1. Now go back into Wireshark and Click **Stop capturing packets** to stop capturing packets.

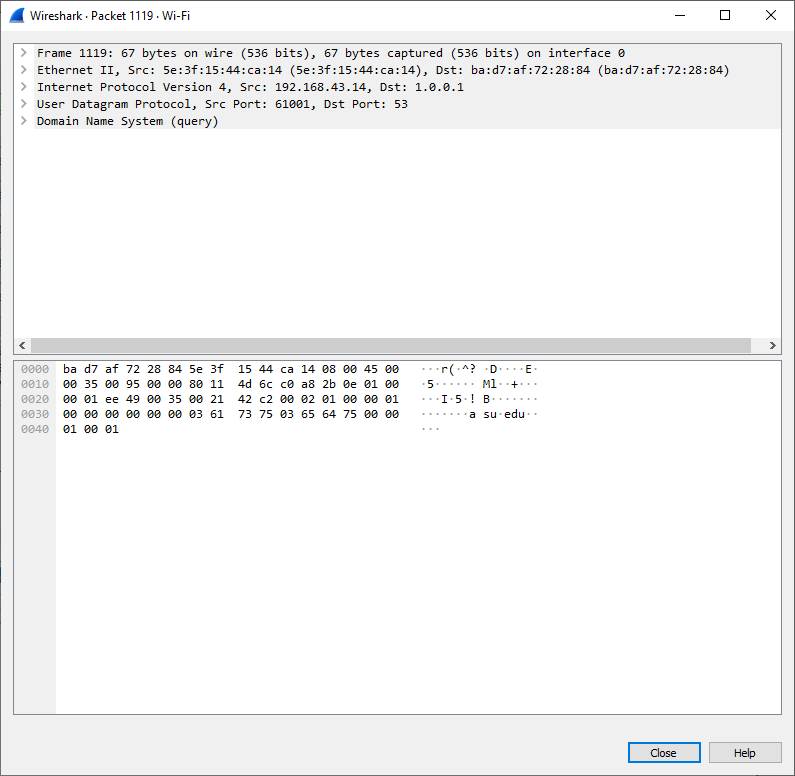
****

**Part 2: DNS Query Traffic Explore**

1. Look at the traffic being captured in the Wireshark Packet List pane. Enter the following text into the filter box **udp.port == 53** and click the arrow or press enter for only DNS packets to be displayed.

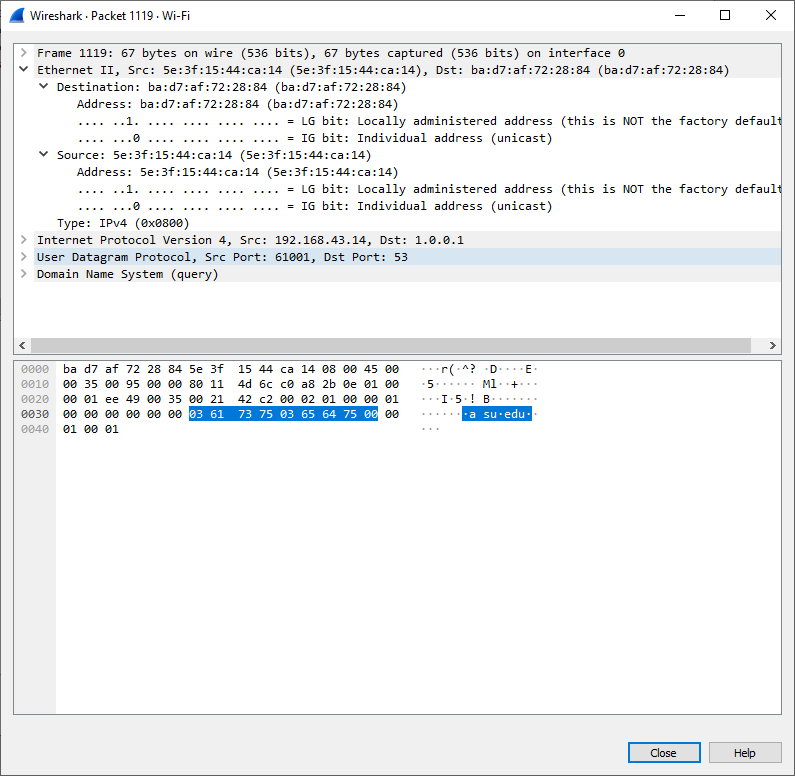
  
****

1. Select the DNS packet that is labeled **Standard query 0x0002 A asu.edu** and open it in a new window by double clicking on it.



****

1. In the Packet Details pane (bottom part of window), observe that the packet is composed of Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).  
     
   Expand the **Ethernet II** section to further view the details. Look closely at the field’s labelled **source** and **destination**.

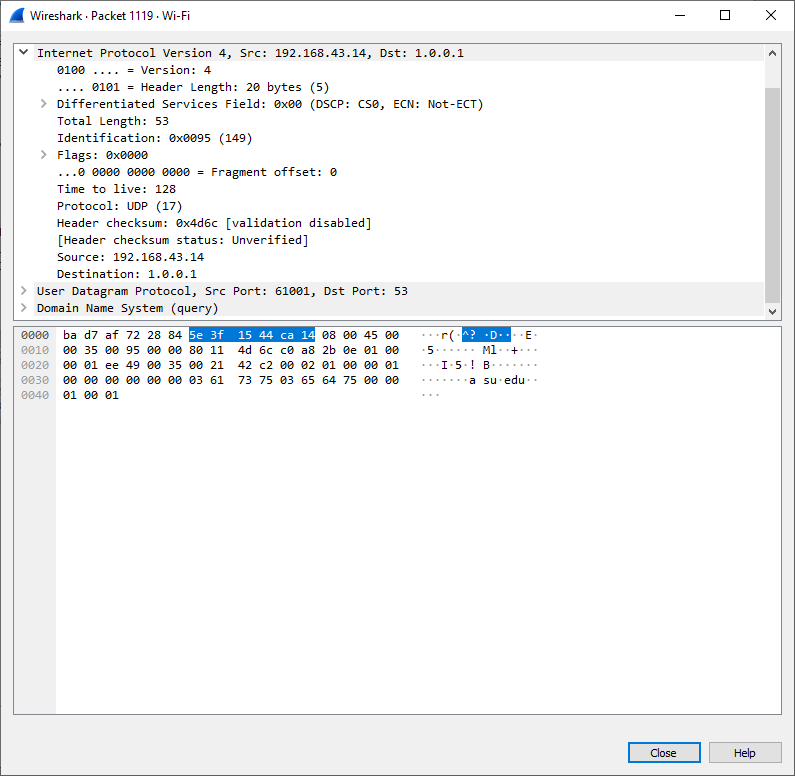


What are the **destination** and **source MAC addresses** in this packet?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which **network interface** has an association with the **MAC addresses** in this packet?

1. Expand the section **Internet Protocol Version 4.** Look at the IPv4 addresses for the **source** and **destination**.



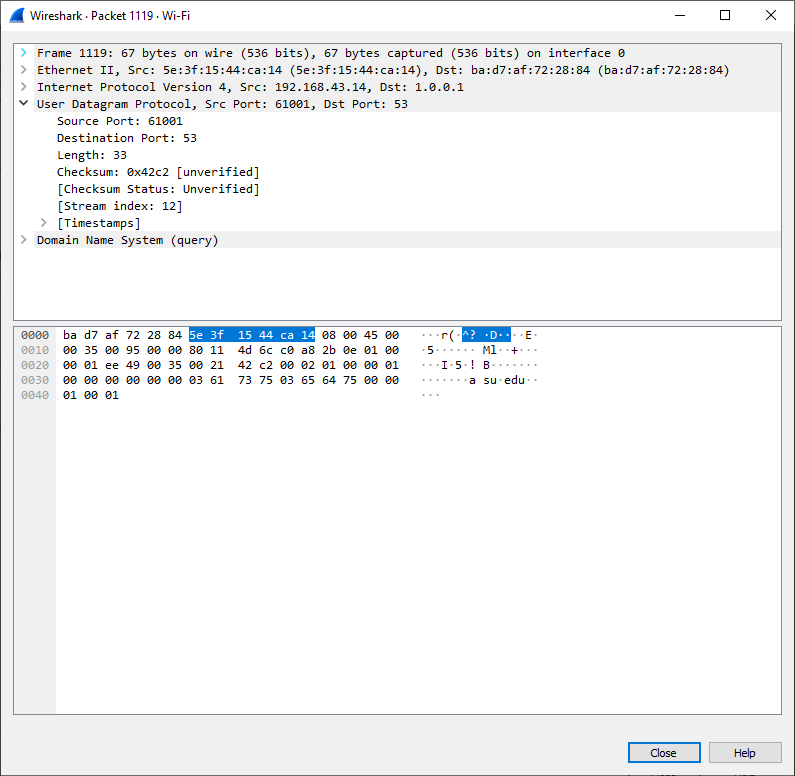
What are the **destination** and **source IP addresses** in this packet?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Which **network interface** has an association with the **IP addresses** in this packet?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Expand the section **User Datagram Protocol.** Pay attention to the source and destination ports.



What are the **destination** and **source ports** in this packet?

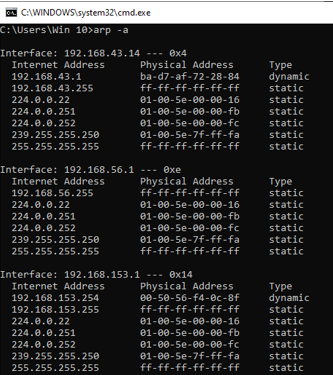
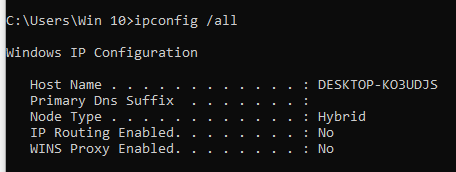
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

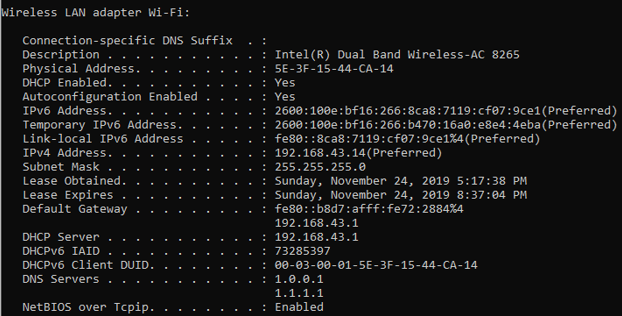
Which is the **default port number** for **DNS**?

**Hint: It is the destination port in the above packet.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Open Command Prompt and enter the command **arp -a** followed by the command **ipconfig /all** for recording the MAC and IP addresses of the PC. In this example, the Wi-Fi adapter information is included as that is what I am using as my primary Internet connection.



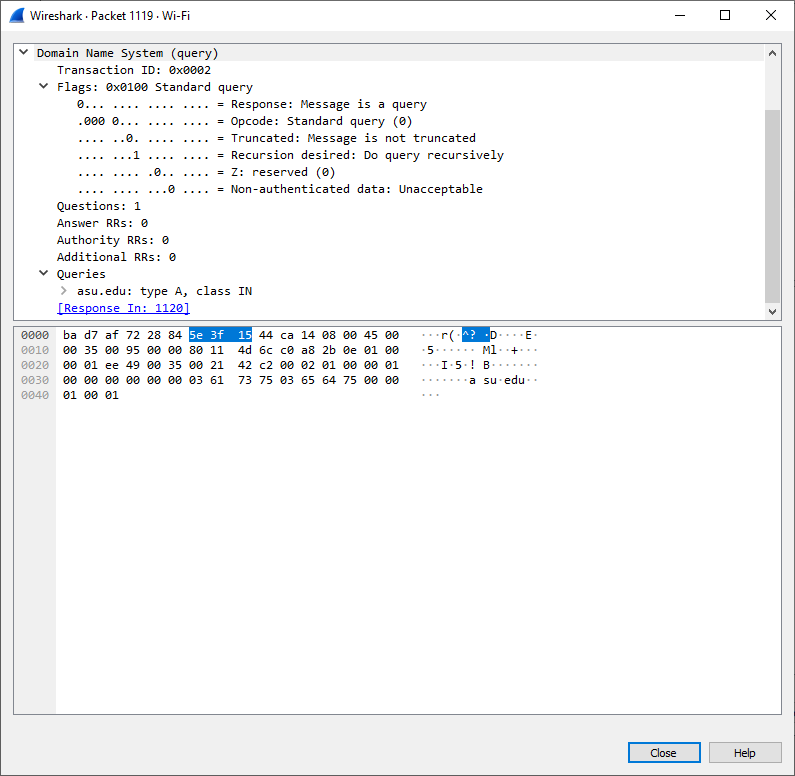


****

1. Compare the MAC and IP addresses from Wireshark to the results obtained from the arp -a and ipconfig /all commands.  
     
   What did you observe?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

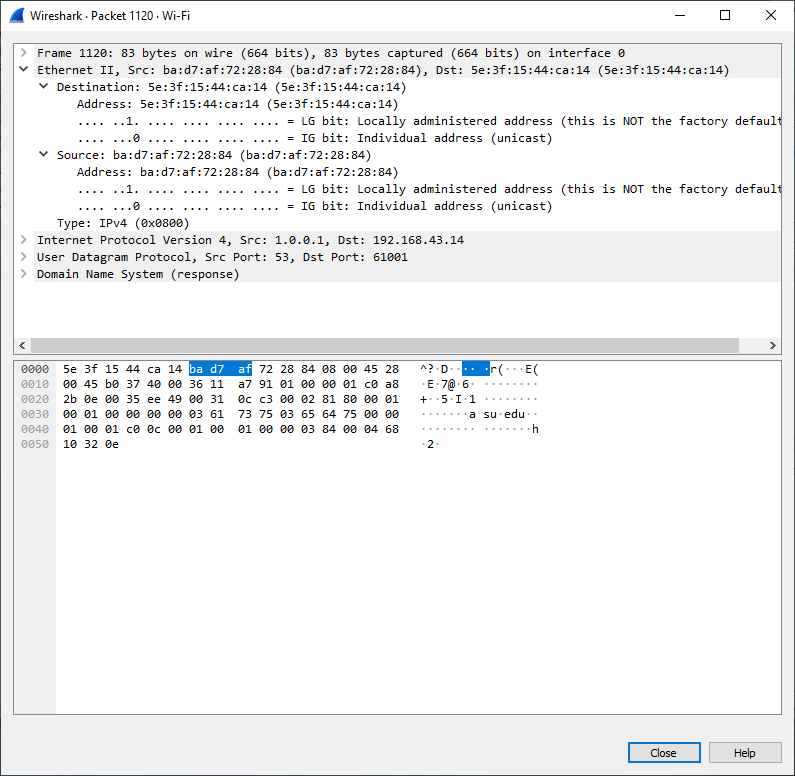
1. Expand the tab titled **Domain Name System (query)** in the Packet Details pane. Next expand the **Flags** and **Queries.**
2. Take a look at the results. The flag recursively queries the IP address to [www.asu.edu](http://www.asu.edu).

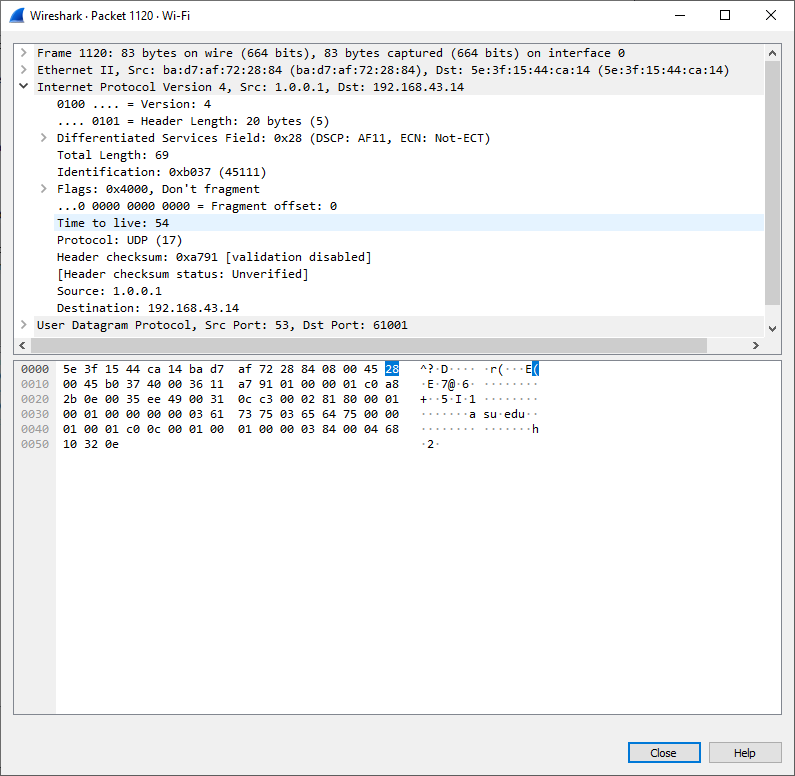


****

**Part 3: DNS Response Traffic Explore**

1. Select the response DNS packet that matches the following title **Standard query response 0x000# A** www.asu.eduand open it in a new window by double clicking on it.





What are the **destination** and **source MAC** and **IP addresses** and **port numbers** in this packet?

The format of your answer should be similar to the following:

**Destination MAC: 5e:3f:15:44:ca:14** **Source MAC: ba:d7:af:72:28:84 Destination IP: 192.168.43.14 Source IP: 1.0.0.1 Destination port: 61001 Source port: 53**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

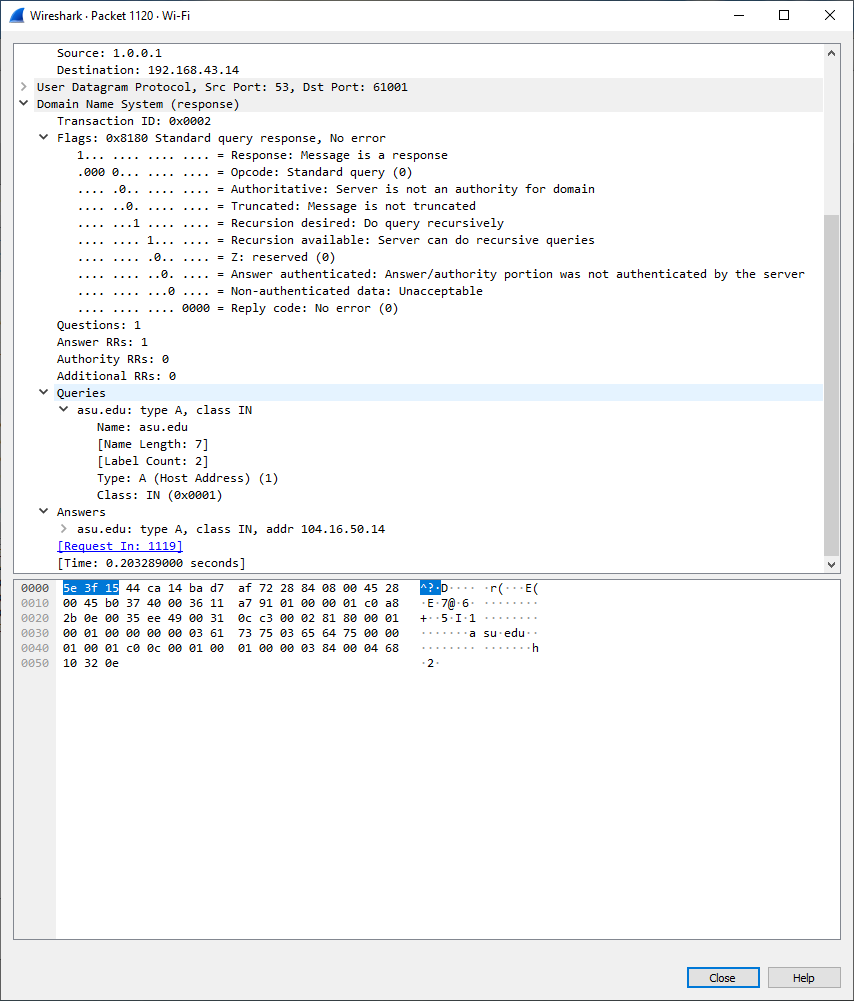
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How do the addresses compare to those in the DNS query packets?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Expand Domain Name System (response). Next expand the Flags, Queries, and Answers. Look at the results. What type of host address is the domain asu.edu?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



1. Look at the A record in the section titled **Answers.** How do the results compare to the results obtained from nslookup?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_