Lab - Exploring DNS Traffic

# Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

# Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

# Required Resources

* 1 PC with internet access and Wireshark installed

# Instructions

## Capture DNS Traffic

### Download and install Wireshark.

* + - 1. Download the latest stable version of Wireshark from [www.wireshark.org](http://www.wireshark.org). Choose the software version you need based on your PC’s architecture and operating system.
      2. Follow the on-screen instructions to install Wireshark. If you are prompted to install USBPcap, **do NOT** install USBPcap for normal traffic capture. USBPcap is experimental, and it could cause USB problems on your PC.

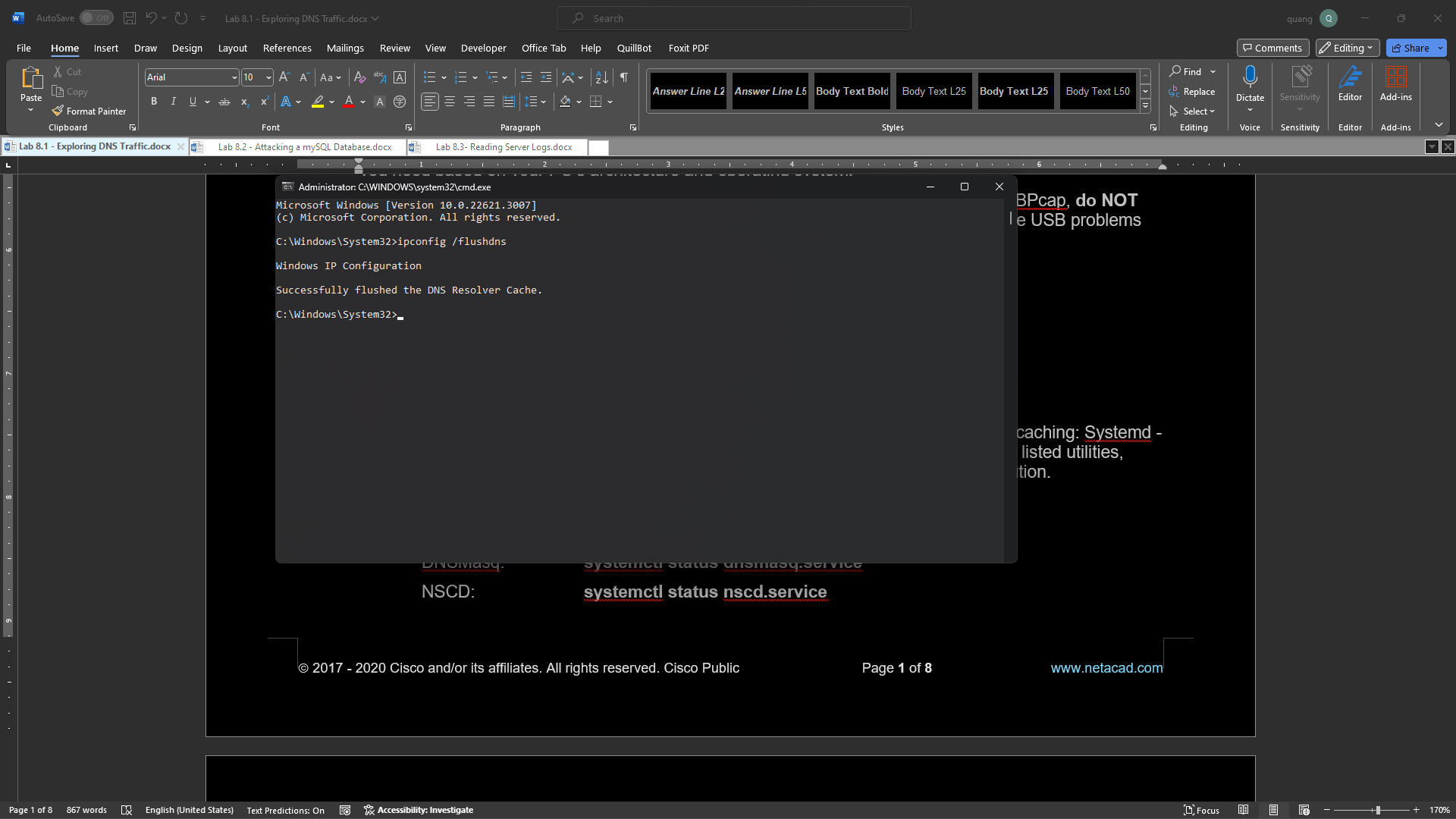
### Capture DNS traffic.

* + - 1. Start Wireshark. Select an active interface with traffic for packet capture.

A screenshot of a computer

Description automatically generated

* + - 1. Clear the DNS cache.
         1. In Windows, enter **ipconfig /flushdns** in Command Prompt.



* + - * 1. For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd -Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.

Identify the utility used in your Linux distribution by checking the status:

Systemd-Resolved: **systemctl status systemd-resolved.service**

DNSMasq: **systemctl status dnsmasq.service**

NSCD: **systemctl status nscd.service**

If you are using system-resolved, enter **systemd-resolve --flush-caches** to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:

Systemd-Resolved: **sudo systemctl restart systemd-resolved.service**

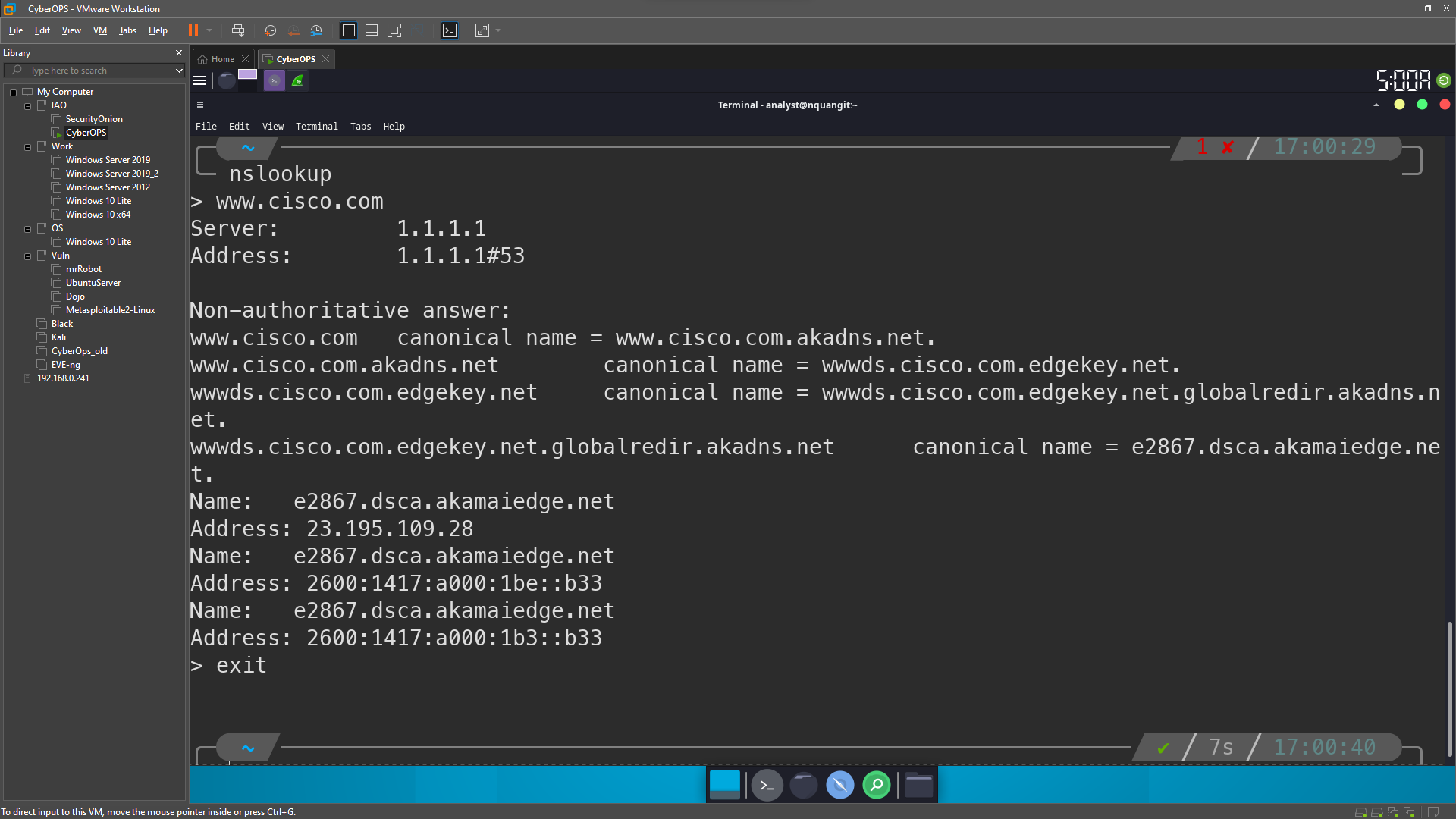
DNSMasq: **sudo systemctl restart dnsmasq.service**

NSCD: **sudo systemctl restart nscd.service**

A screenshot of a computer

Description automatically generated

* + - * 1. For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.
      1. At a command prompt or terminal, type **nslookup** enter the interactive mode.
      2. Enter the domain name of a website. The domain name [www.cisco.com](http://www.cisco.com) is used in this example.
      3. Type **exit** when finished. Close the command prompt.



* + - 1. Click **Stop capturing packets** to stop the Wireshark capture.

## Explore DNS Query Traffic

* + - 1. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets. **Note**: The provided screenshots are just examples. Your output maybe slightly different.

A computer screen shot of a computer

Description automatically generated

* + - 1. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.
      2. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).
      3. Expand **Ethernet II** to view the details. Observe the source and destination fields.

A computer screen shot of a computer

Description automatically generated

What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

Source MAC: 00:0c:29:a2:3a:c9

Dest MAC: 00:50:56:e5:36:07

Source MAC is current device NIC

Dest MAC is the default gateway NIC

* + - 1. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.

A screenshot of a computer

Description automatically generated

#### Question:

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

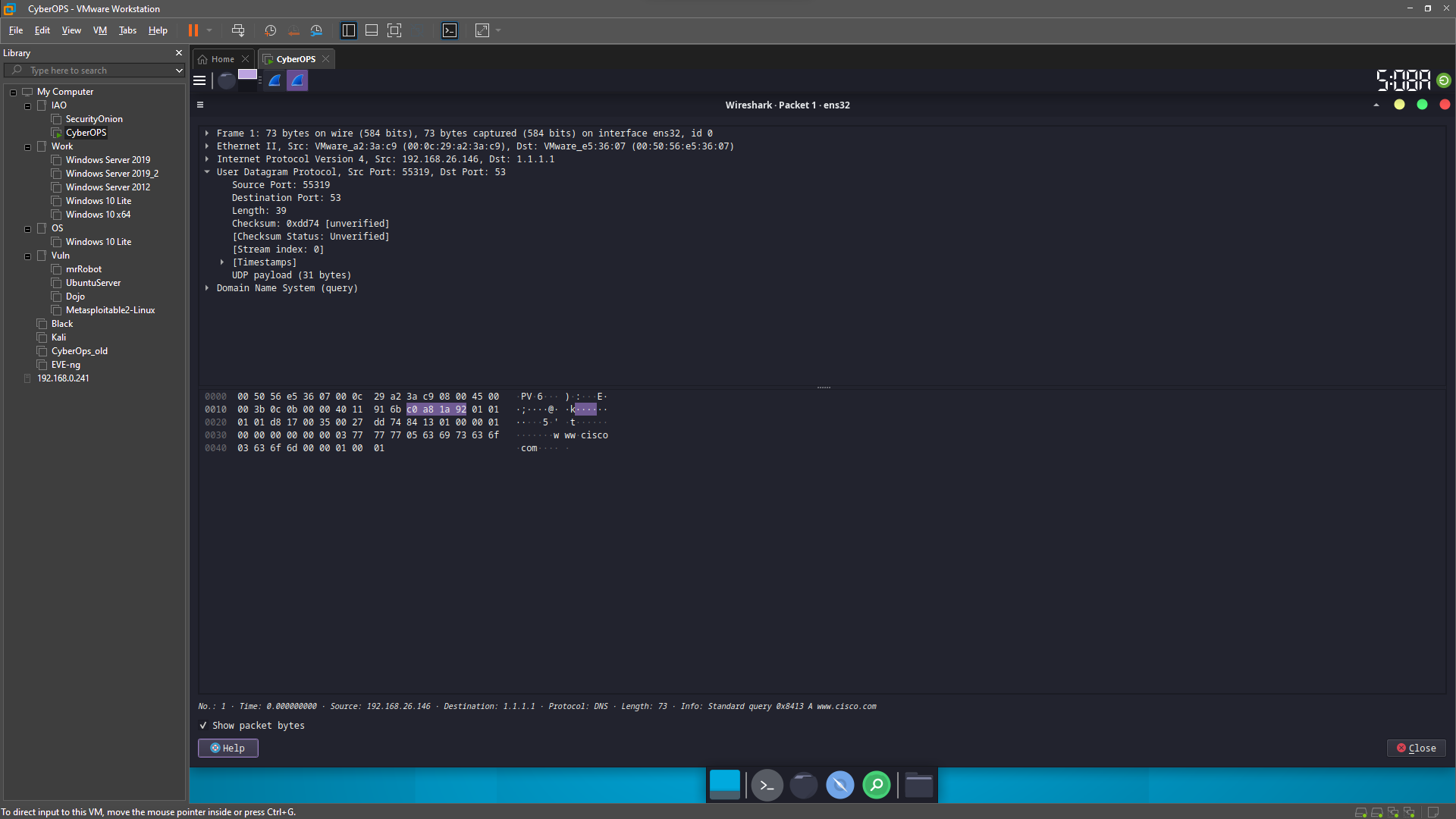
Source IP: 192.168.26.146

Dest IP: 1.1.1.1

Source IP is the current device’s IP.

Dest IP is the DNS server’s IP.

* + - 1. Expand the **User Datagram Protocol**. Observe the source and destination ports.



#### Question:

What are the source and destination ports? What is the default DNS port number?

Source port: 55319

Dest port: 53

Default DNS port number is 53

* + - 1. Determine the IP and MAC address of the PC.
         1. In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

A screen shot of a computer

Description automatically generated

* + - * 1. For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

A screenshot of a computer

Description automatically generated

#### Question:

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

The MAC and IP addresses in the Wireshark result are the same as the addresses in ip address command result

* + - 1. Expand **Domain Name System (query**) in the Packet Details pane. Then expand the **Flags** and **Queries**.
      2. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.

A computer screen shot of a computer

Description automatically generated

## Explore DNS Response Traffic

* + - 1. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.

A screenshot of a computer

Description automatically generated

#### Question:

What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

The source IP, MAC address, and port number in the query packet are now destination addresses. The destination IP, MAC address, and port number in the query packet are now source addresses.

* + - 1. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.

A computer screen shot of a computer screen

Description automatically generated

* + - 1. Observe the results.

#### Question:

Can the DNS server do recursive queries?

Yes

A screenshot of a computer

Description automatically generated

* + - 1. Observe the CNAME and A records in the Answers details.

#### Question:

How do the results compare to nslookup results?

The result in Wireshark are the same with the nslookup results.

# Reflection

* 1. From the Wireshark results, what else can you learn about the network when you remove the filter?

If we remove the filter, other package will be display such as ARP, DHCP, HTTP, … From these package and its information, we can learn how the network work, encapsulate packages, and many other protocol.

* 1. How can an attacker use Wireshark to compromise your network security?

Attacker can use Wireshark to capture all traffic on LAN and can get some sensitive information if it is not encrypted.

End of document