Lab - Exploring DNS Traffic (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# 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

**Instructor Note**: Using a packet sniffer such as Wireshark may be considered a breach of the security policy of the school. It is recommended that permission is obtained before running Wireshark for this lab. If using a packet sniffer such as Wireshark is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

# 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.
      2. Clear the DNS cache.
         1. In Windows, enter **ipconfig /flushdns** in Command Prompt.
         2. 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**

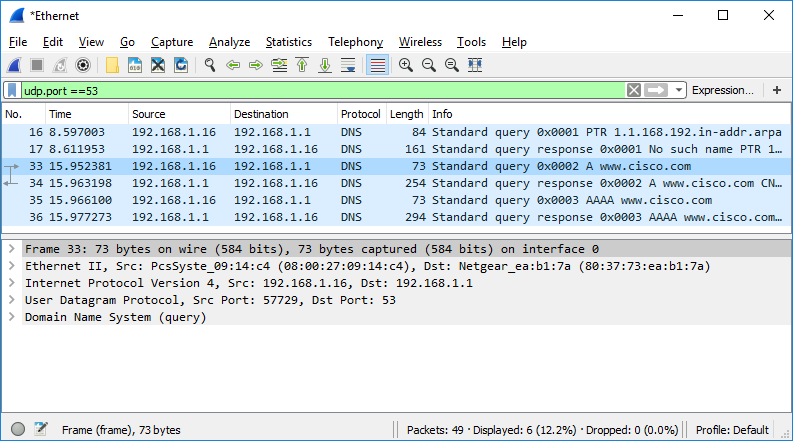
DNSMasq: **sudo systemctl restart dnsmasq.service**

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

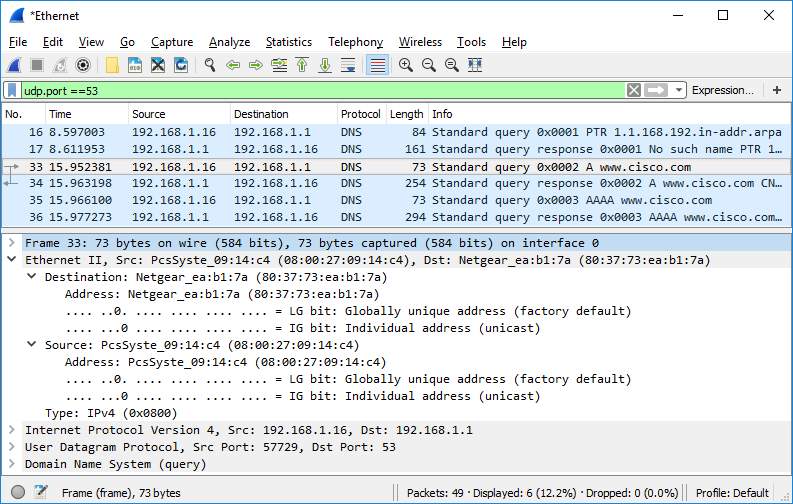
* + - * 1. For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.
      1. At a command prompt or terminal, type **nslookup** enter the interactive mode.
      2. Enter the domain 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.
      4. 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.



* + - 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.

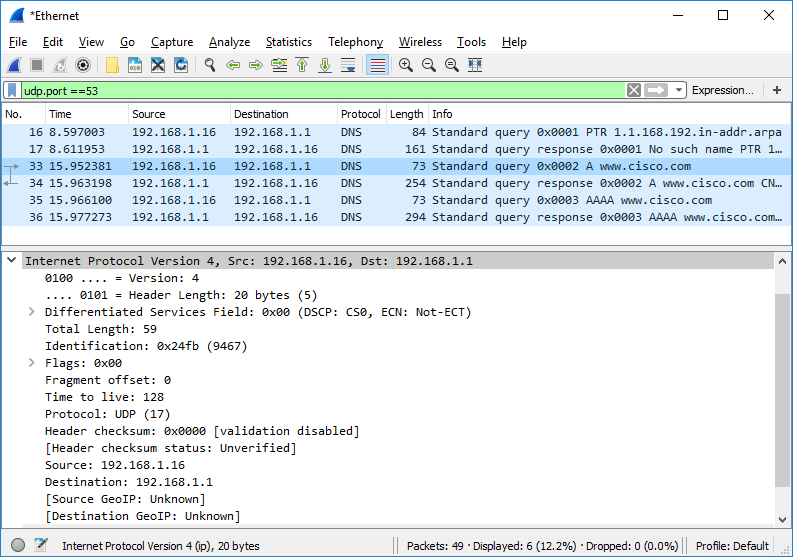


What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

Type your answers here.

In this example, the source MAC address is associated with the NIC on the PC and the destination MAC address is associated with the default gateway. If there is a local DNS server, the destination MAC address would be the MAC address of the local DNS server.

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



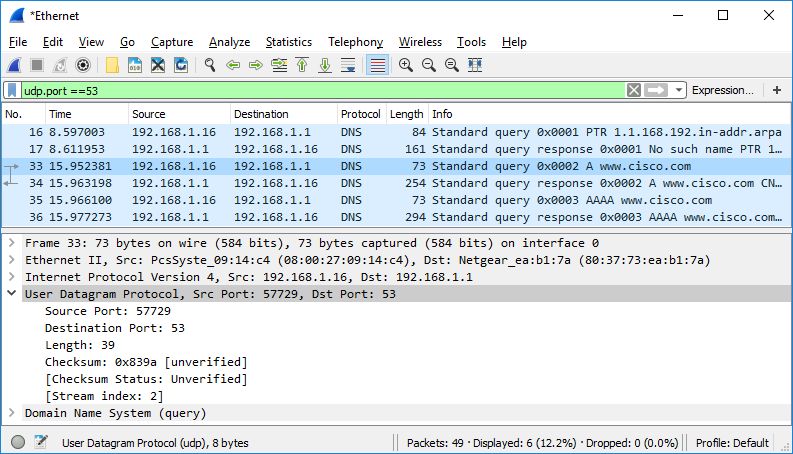
#### Question:

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

Type your answers here.

In this example, the source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

* + - 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?

Type your answers here.

The source port number is 577729 and the destination port is 53, which is the default DNS port number.

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

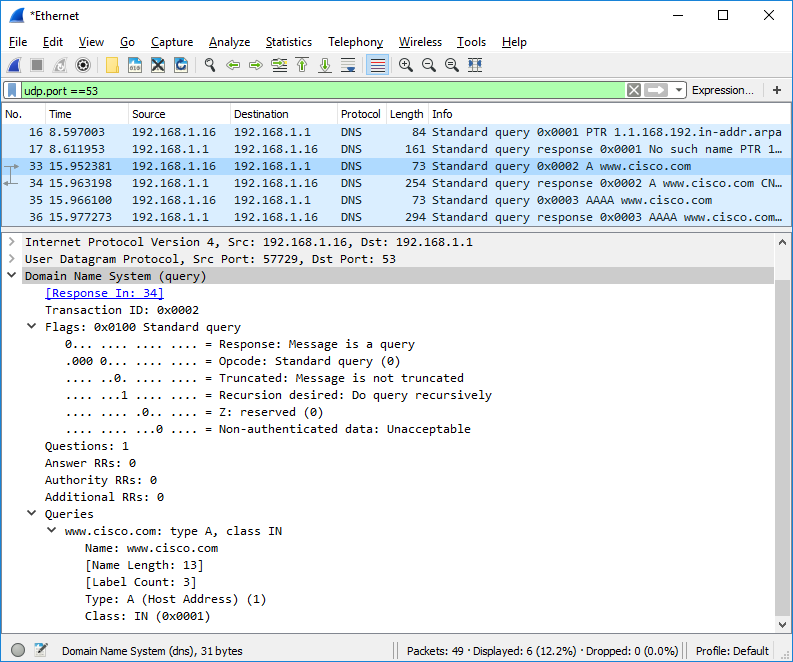
#### Question:

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

Type your answers here.

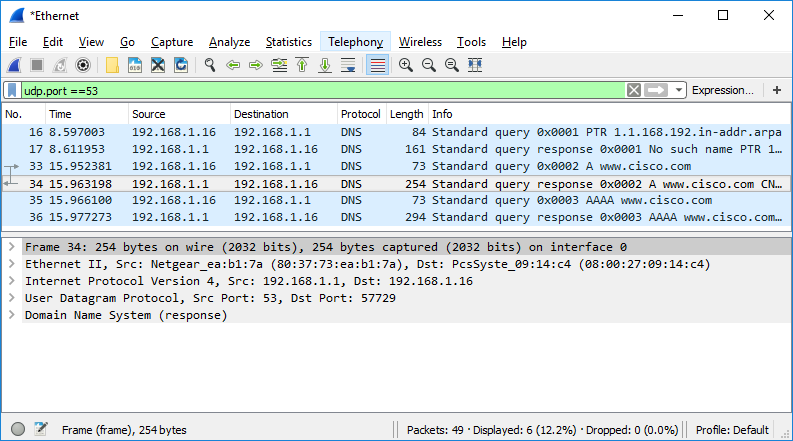
The IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in ipconfig /all command.

* + - 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.



## Explore DNS Response Traffic

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



#### 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?

Type your answers here.

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.

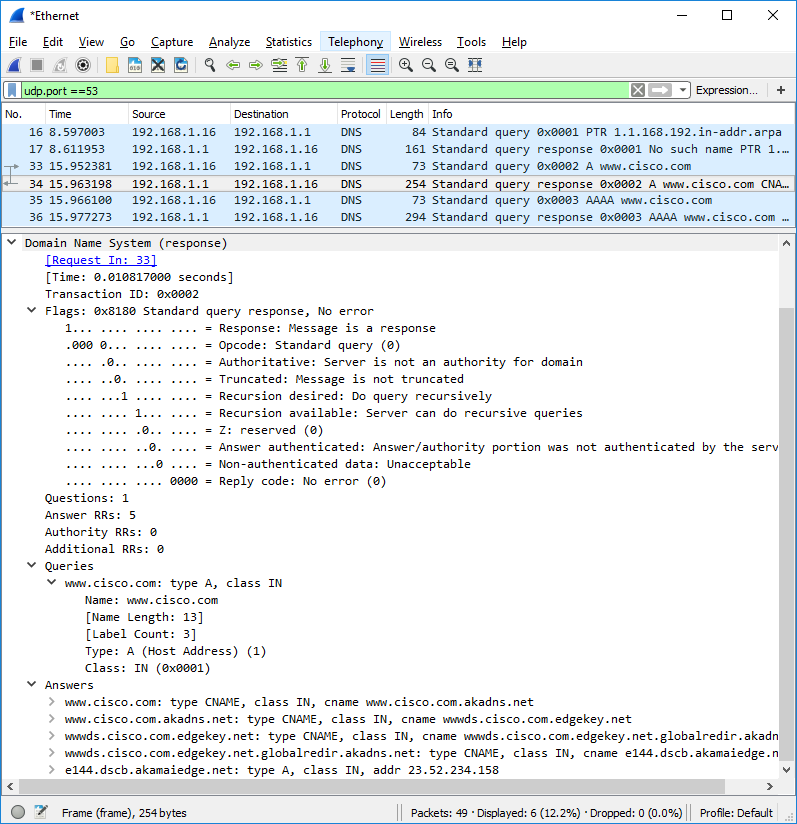
* + - 1. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.
      2. Observe the results.

#### Question:

Can the DNS server do recursive queries?

Type your answers here.

Yes, the DNS can handle recursive queries.



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

#### Question:

How do the results compare to nslookup results?

Type your answers here.

The results in the Wireshark should be the same as the results from nslookup in the Command Prompt or terminal.

# Reflection

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

Type your answers here.

Without the filters, the results display other packets, such as DHCP and ARP. From these packets and the information contained within these packets, you can learn about other devices and their functions within the LAN.

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

Type your answers here.

An attacker on the LAN can use Wireshark to observe the network traffic and can get sensitive information in the packet details if the traffic is not encrypted.

End of document