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

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

a. Download the latest stable version of Wireshark from www.wireshark.org. Choose the software version you need based on your PC's architecture and operating system.

b. 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.

Step 2: Capture DNS traffic.

a. Start Wireshark. Select an active interface with traffic for packet capture.

b. 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.

(i) 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**

(ii) 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**

3) 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.

c. At a command prompt or terminal, type **nslookup** enter the interactive mode.

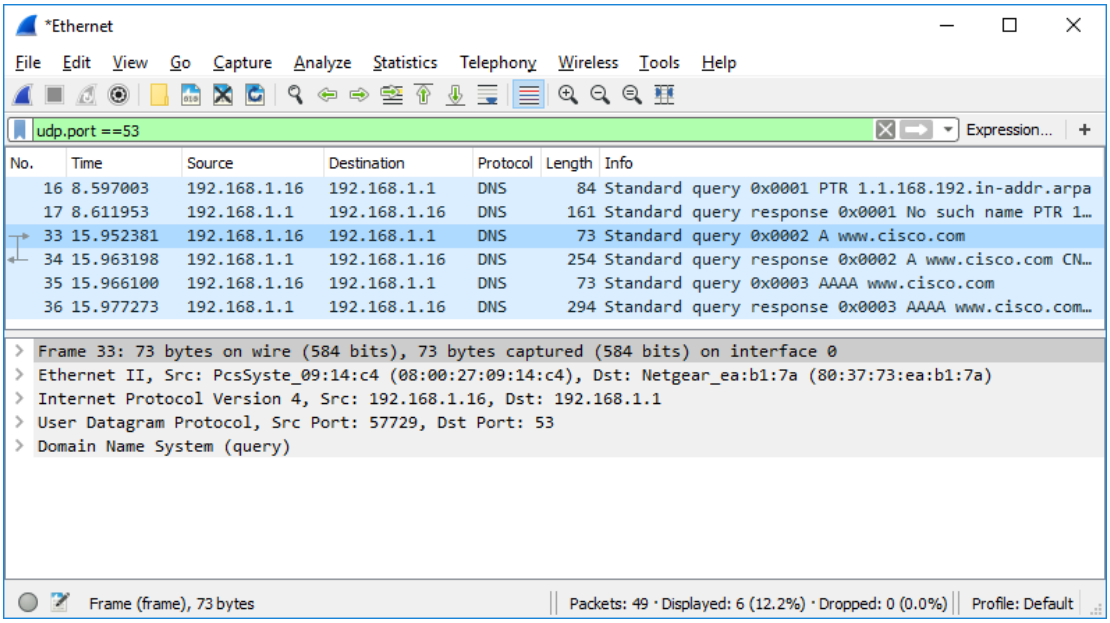
d. Enter the domain name of a website. The domain name www.cisco.com is used in this example.

e. Type **exit** when finished. Close the command prompt.

f. Click **Stop capturing packets** to stop the Wireshark capture.

Part 2: Explore DNS Query Traffic

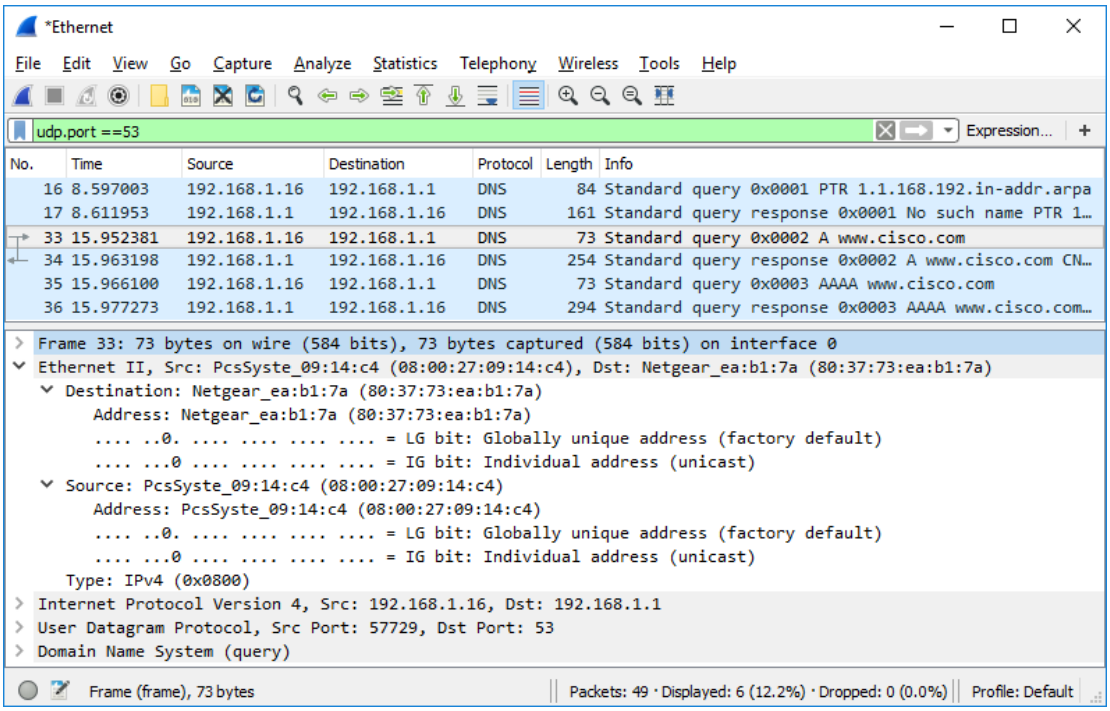
a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets. **Note**: The provided screenshots are just examples. Your output maybe slightly different.



b. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.

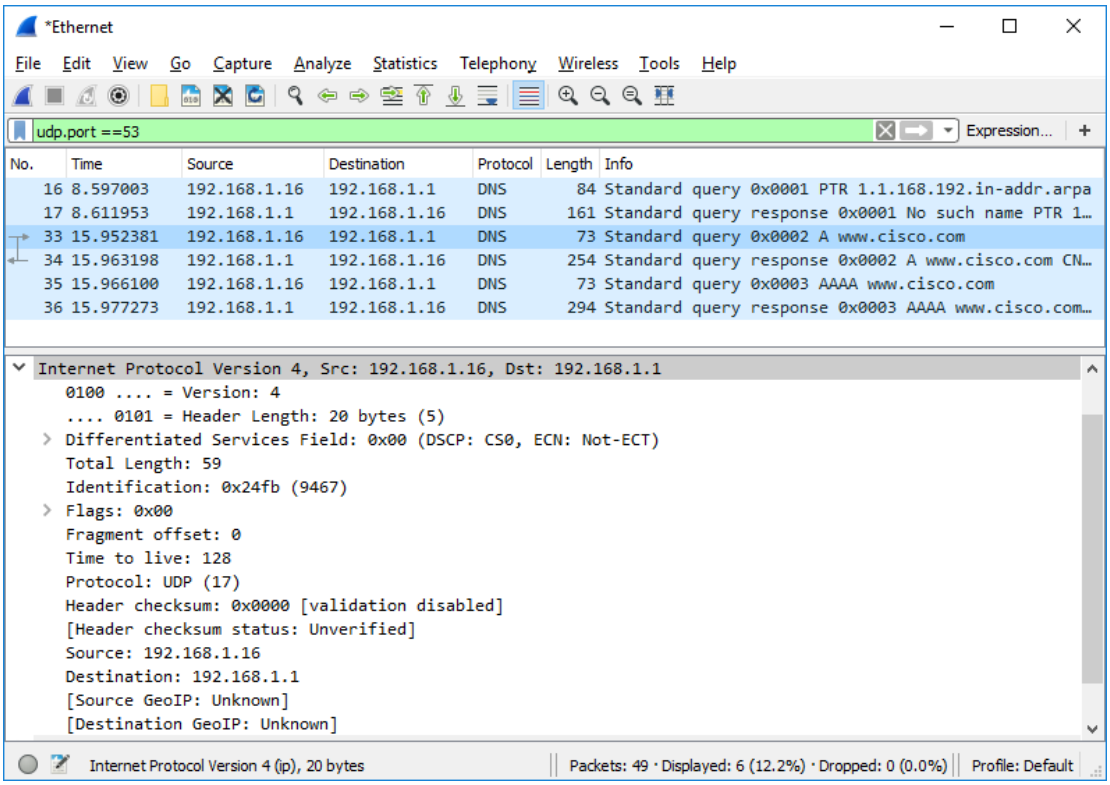
c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand **Ethernet II** to view the details. Observe the source and destination fields.



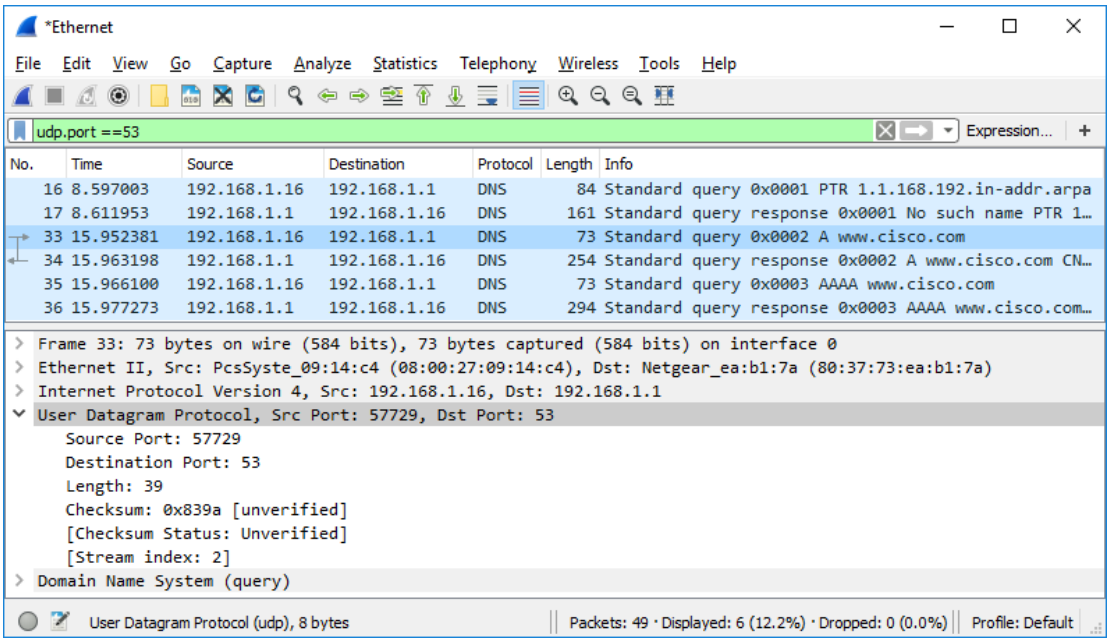
What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

e. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.



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

f. Expand the **User Datagram Protocol**. Observe the source and destination ports.



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

g. Determine the IP and MAC address of the PC.

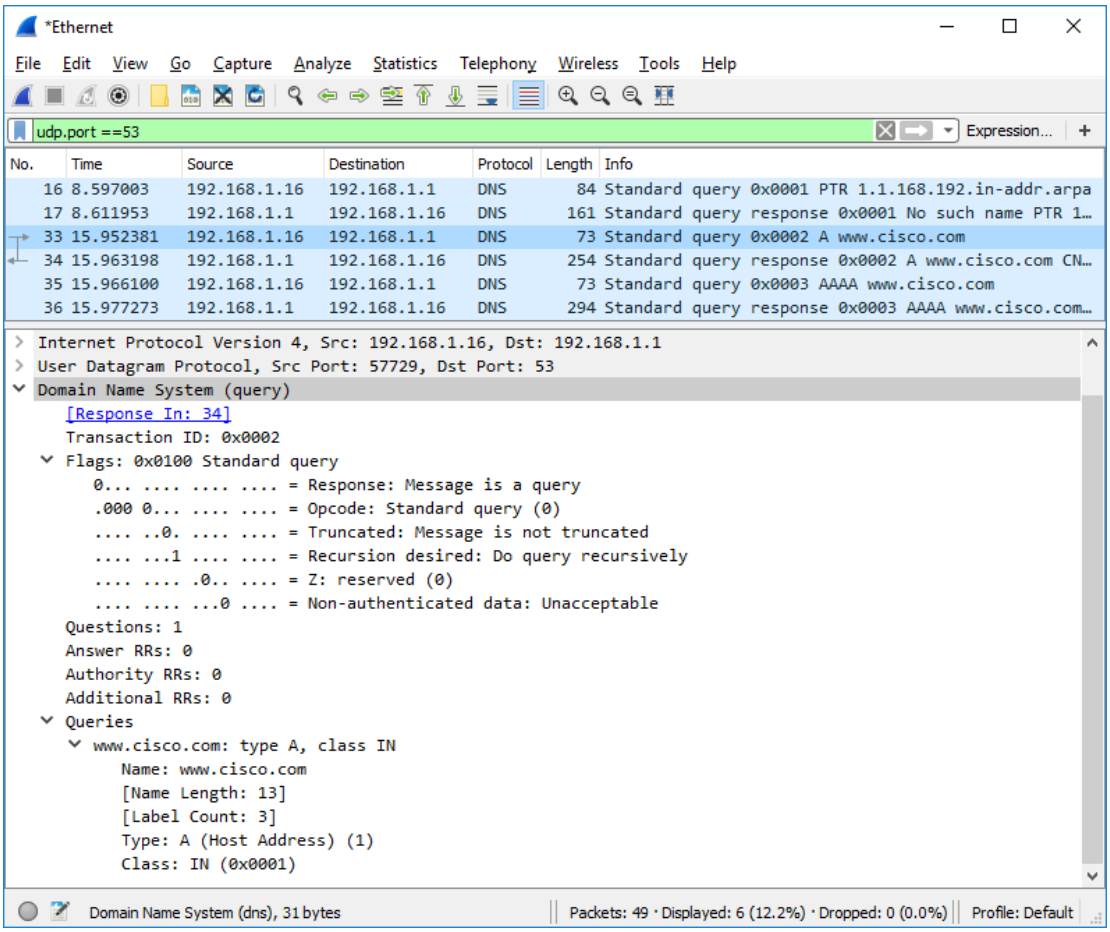
1) In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.

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

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

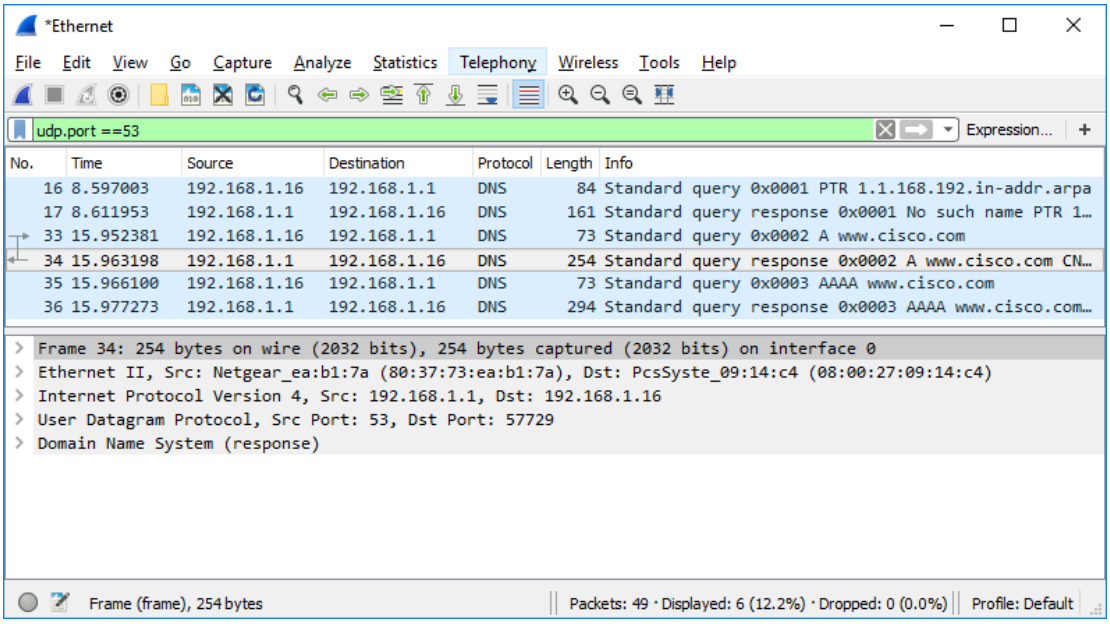
h. Expand **Domain Name System (query**) in the Packet Details pane. Then expand the **Flags** and **Queries**.

i. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.



Part 3: Explore DNS Response Traffic

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

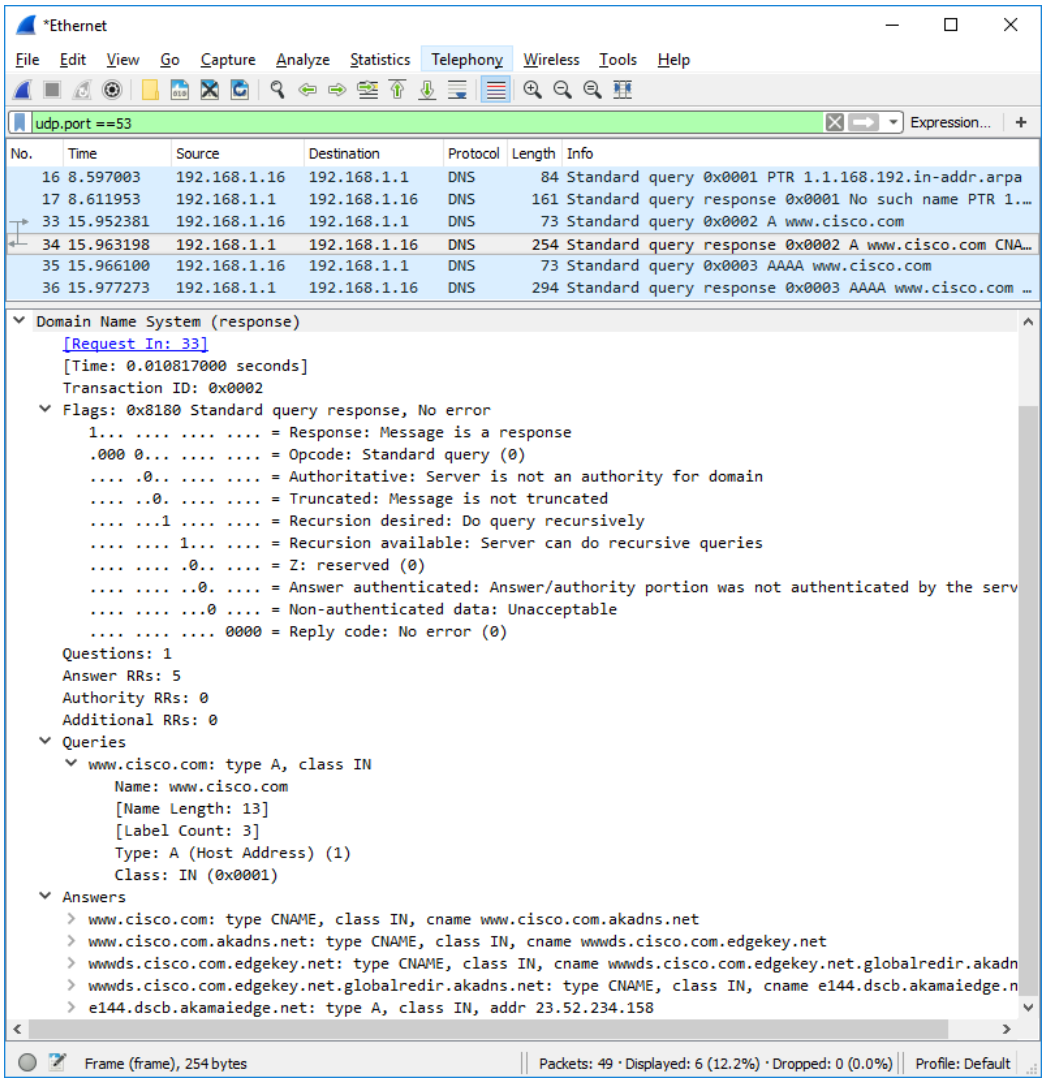


What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

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

c. Observe the results.

Can the DNS server do recursive queries?



d. Observe the CNAME and A records in the Answers details.

How do the results compare to nslookup results?

Reflection

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

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