

Lab - Explore 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 on a Windows system and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

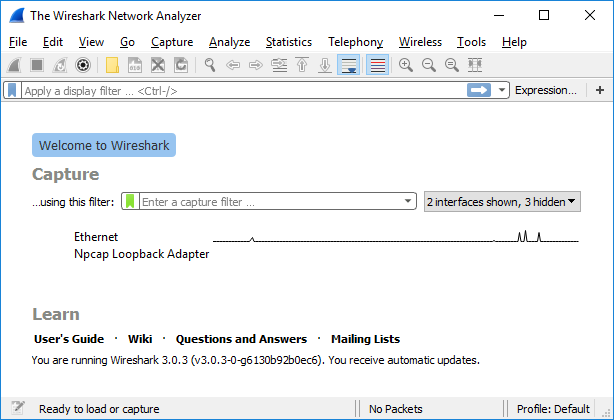
# Required Resources

* 1 Windows PC with internet access and Wireshark installed

# Instructions

**Part 1: Capture DNS traffic.**

1. Open **Wireshark** and start a Wireshark capture by double clicking a network interface with traffic.



1. At the Command Prompt, enter **ipconfig /flushdns** clear the DNS cache.

PS C:\Users\HP> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

1. Enter **nslookup** at the prompt to enter the nslookup 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. Enter

[**www.cisco.com**](http://www.cisco.com/)at the > prompt.

PS C:\Users\HP> nslookup

Default Server: UnKnown

Address: 10.0.1.50

> www.cisco.com

Server: UnKnown

Address: 10.0.1.50

Non-authoritative answer:

Name: e2867.dsca.akamaiedge.net

Addresses: 2600:1413:b000:39a::b33

2600:1413:b000:380::b33

23.54.57.29

Aliases: www.cisco.com

www.cisco.com.akadns.net

wwwds.cisco.com.edgekey.net

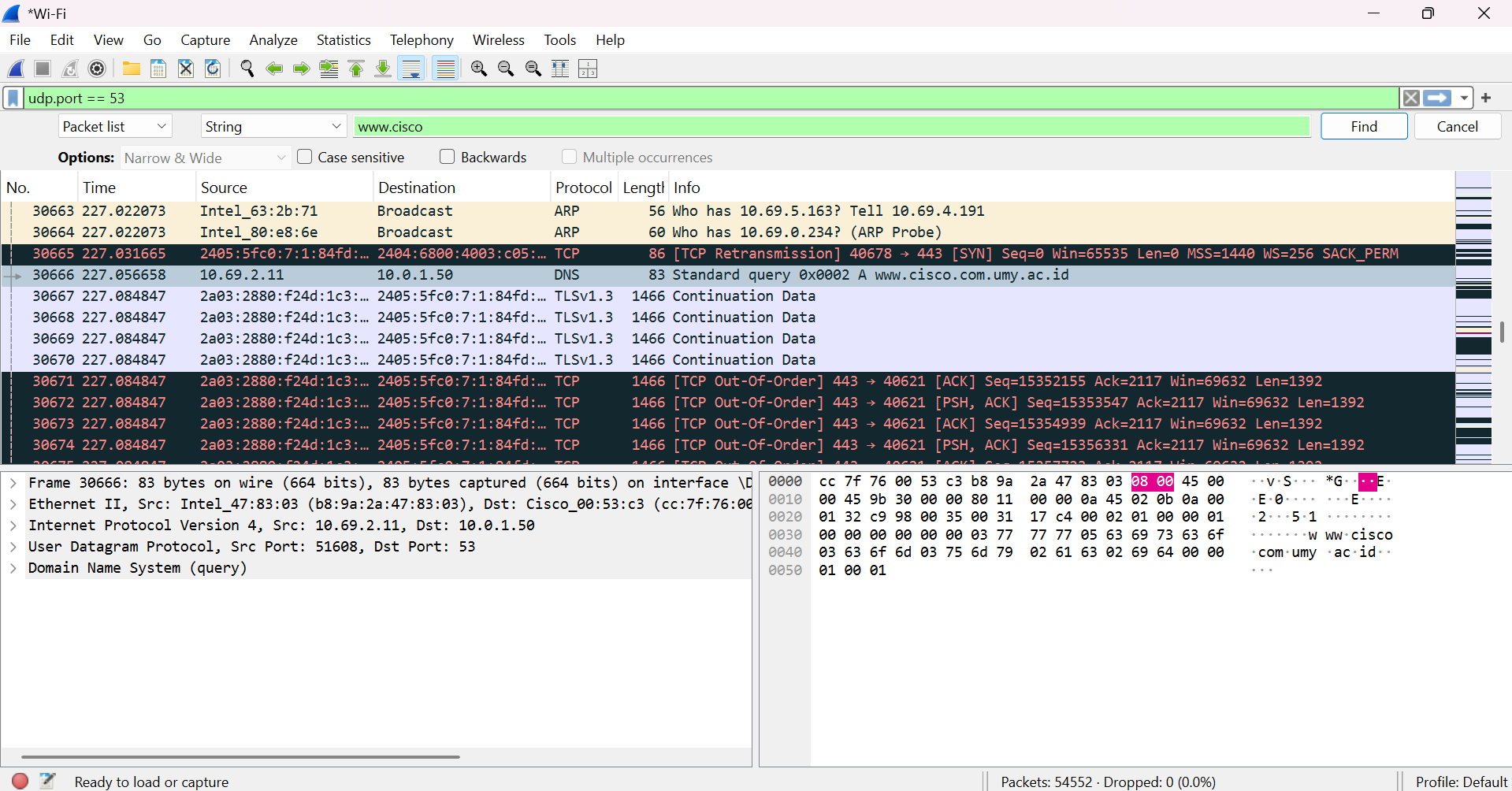
wwwds.cisco.com.edgekey.net.globalredir.akadns.net

1. Enter **exit** when finished to exit the nslookup interactive mode. Close the command prompt.
2. Click **Stop capturing packets** to stop the Wireshark capture.

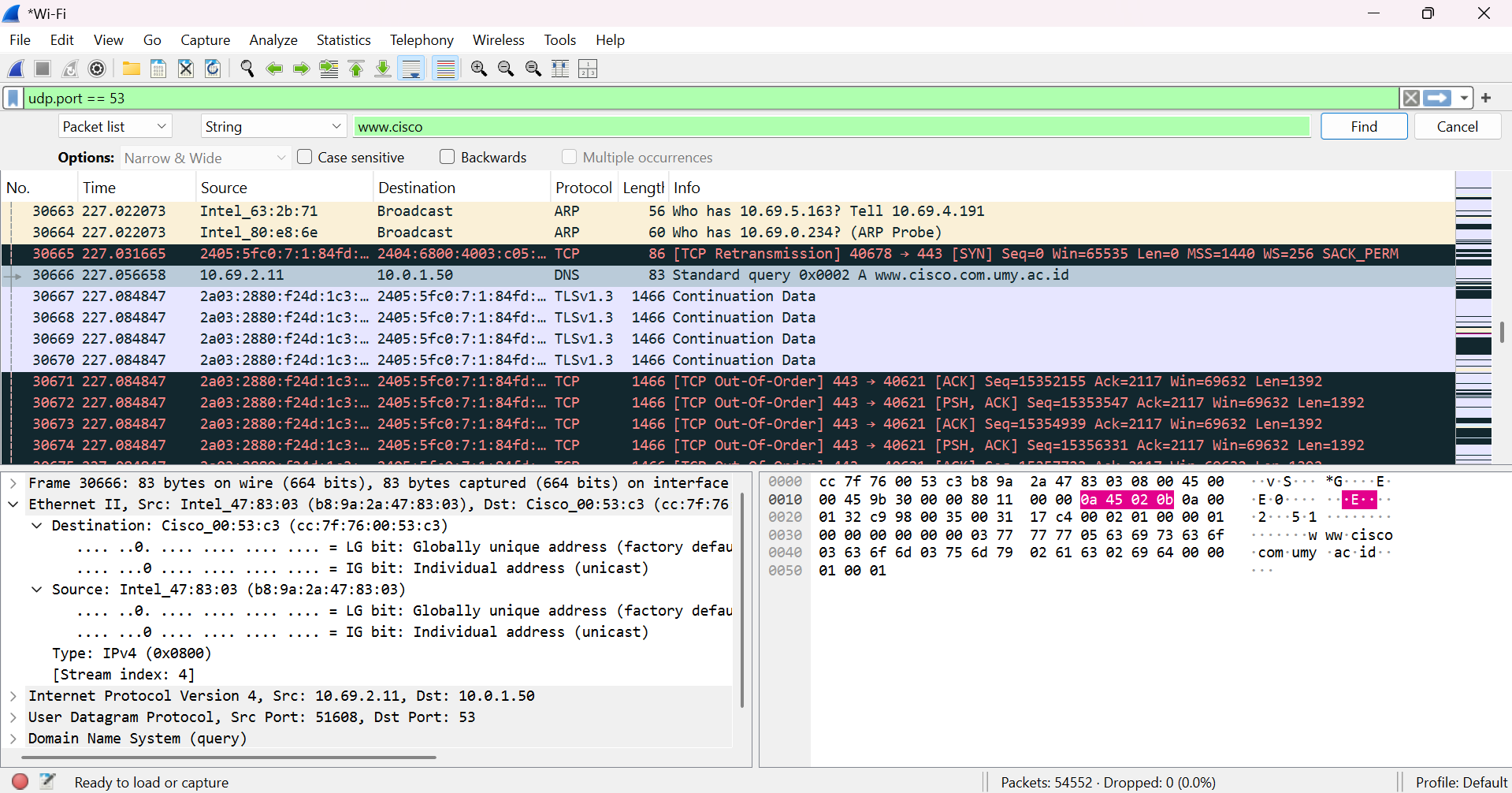
# Part 2: Explore DNS Query Traffic

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.
2. Select the DNS packet labeled **Standard query 0x0002 A** [**www.cisco.com**.](http://www.cisco.com/)

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

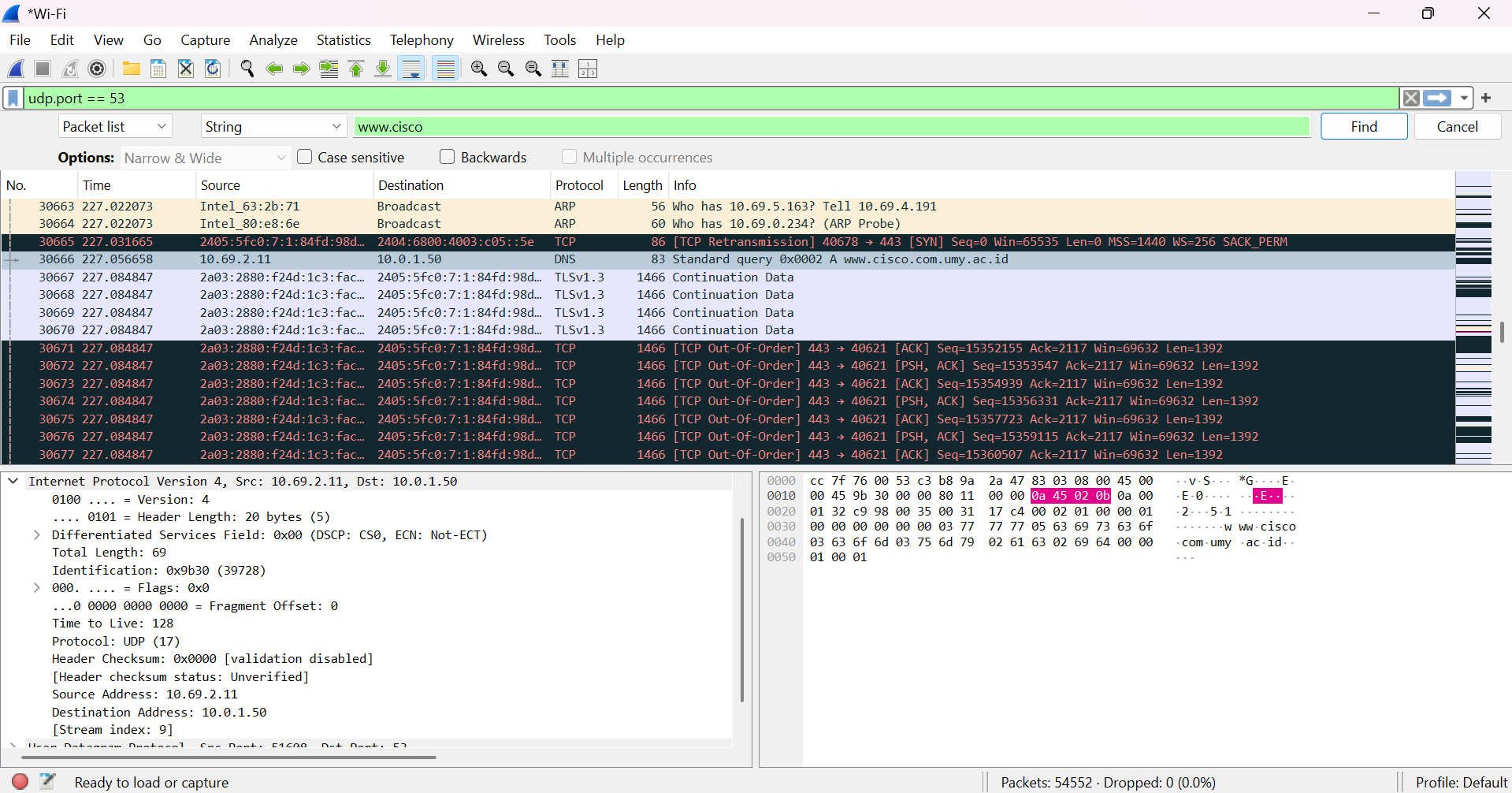


1. Expand **Ethernet II** to view the details. Observe the source and destination fields.



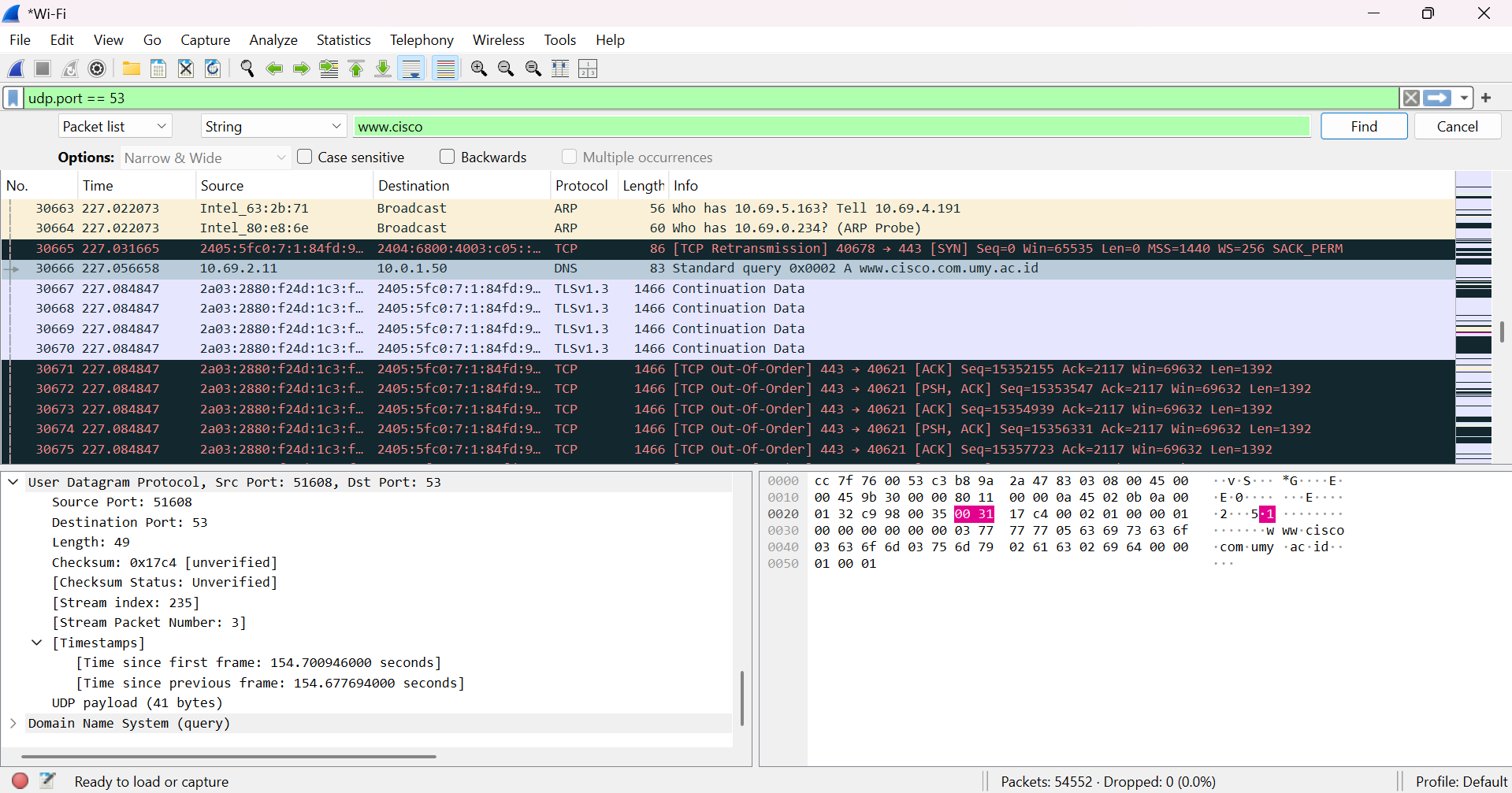
What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

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



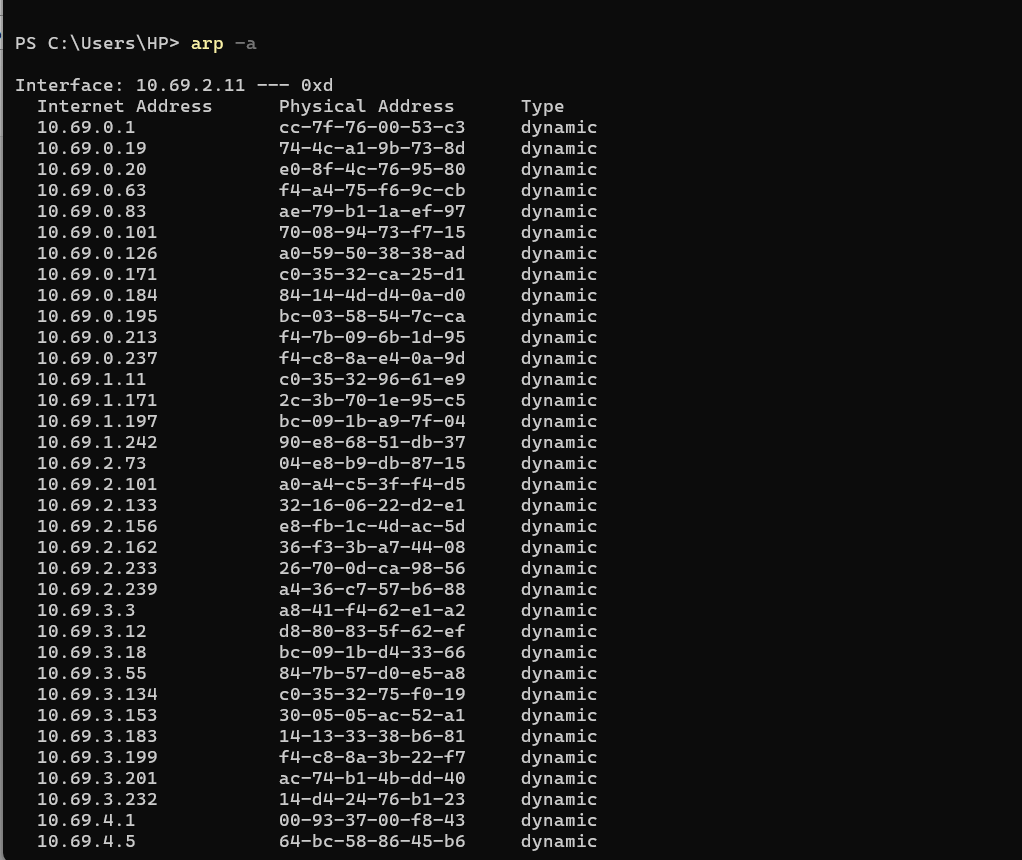
What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

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

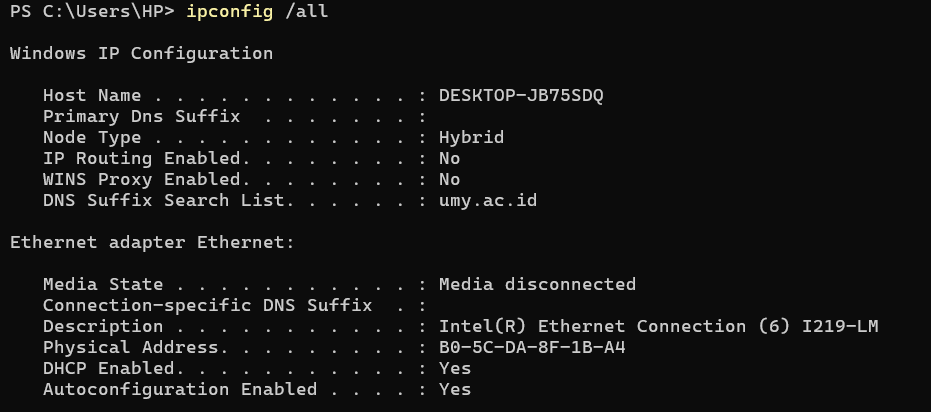


What are the source and destination ports? What is the default DNS port number?

* 1. Open a Command Prompt and enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.



|  |
| --- |
|  |



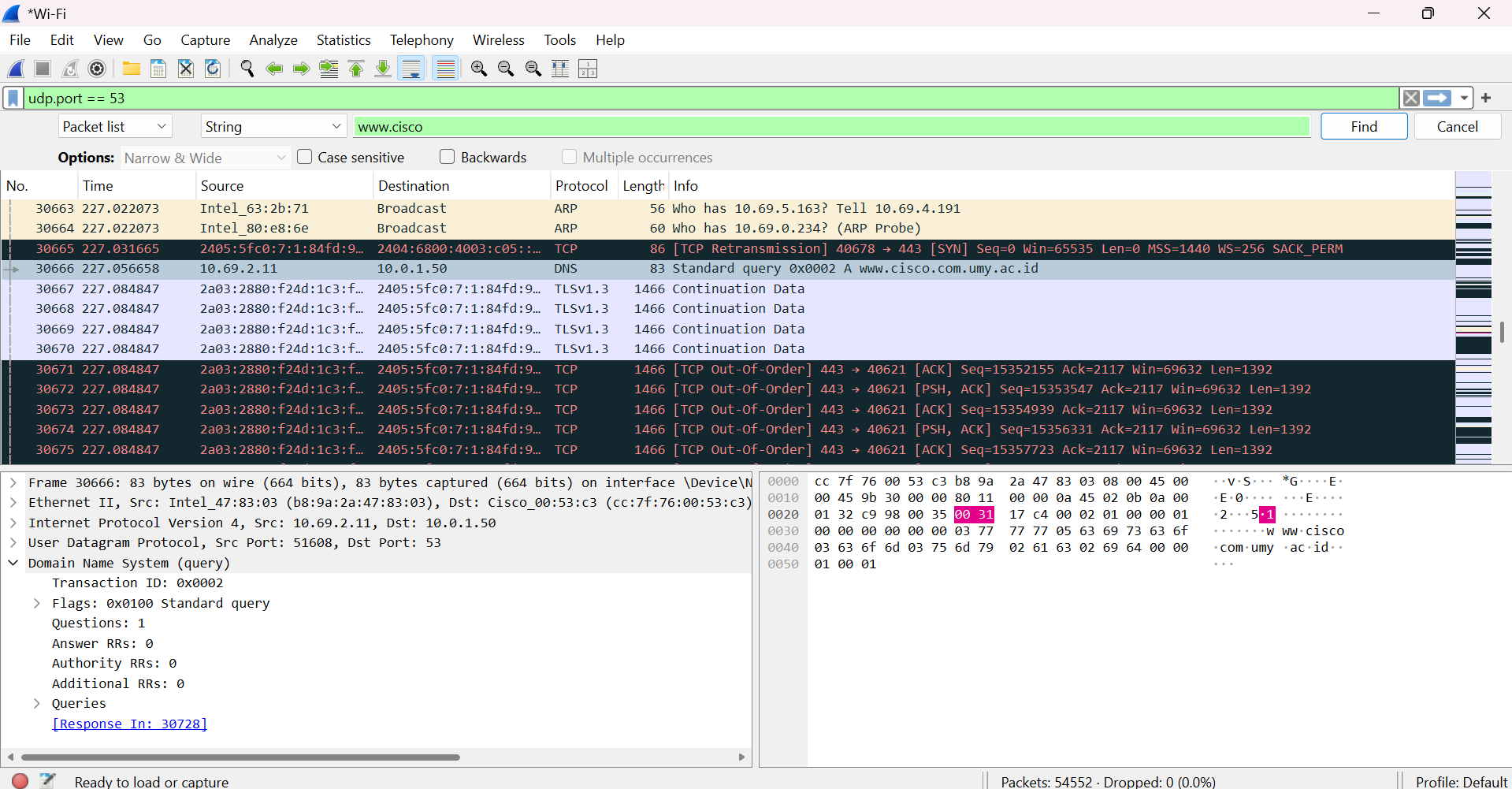
Compare the MAC and IP addresses in the Wireshark results to the results from the **ipconfig /all**

results. What is your observation?

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

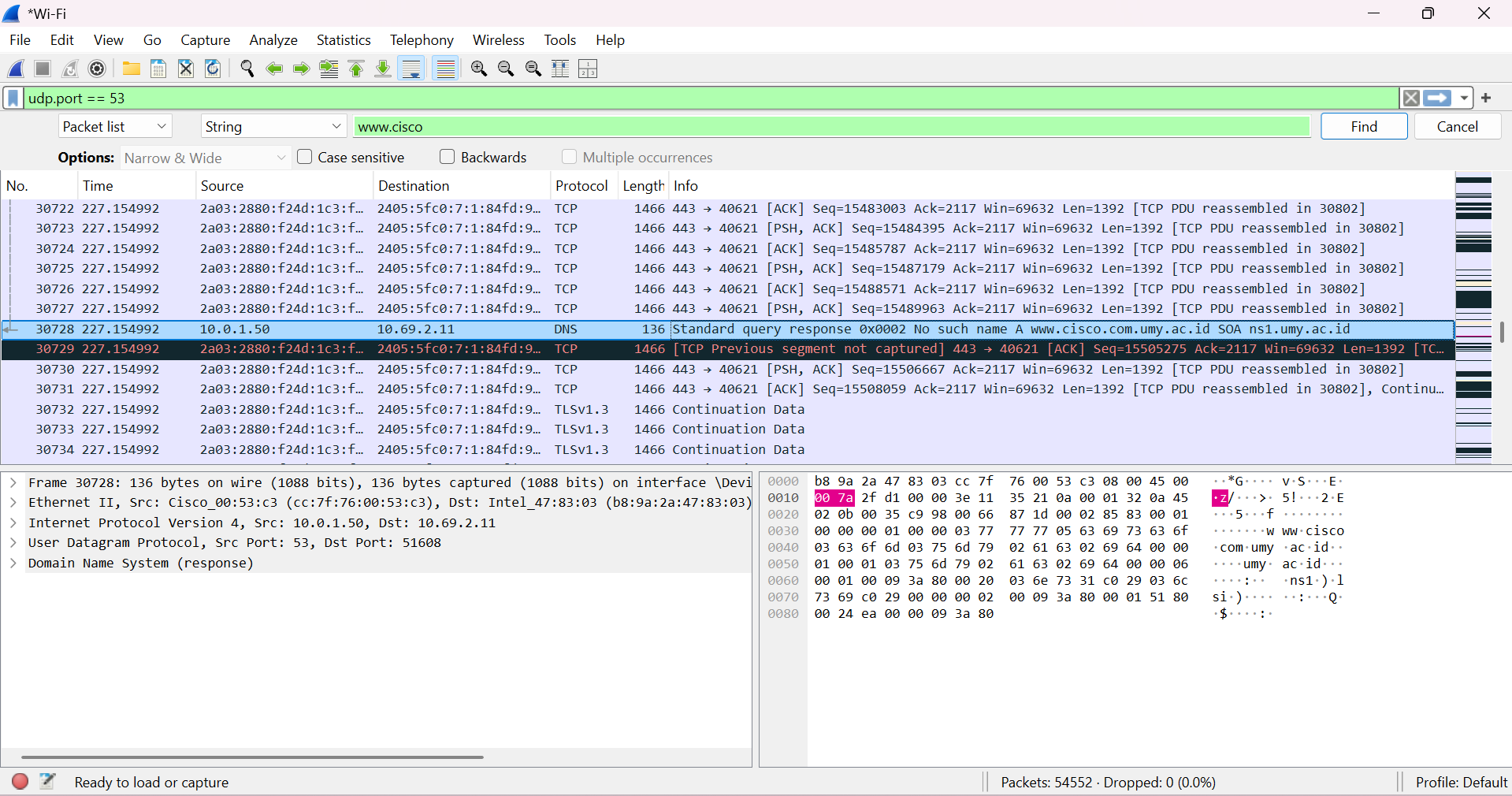
**Queries**.

Observe the results. The flag is set to do the query recursively to query for the IP address to [www.cisco.com.](http://www.cisco.com/)



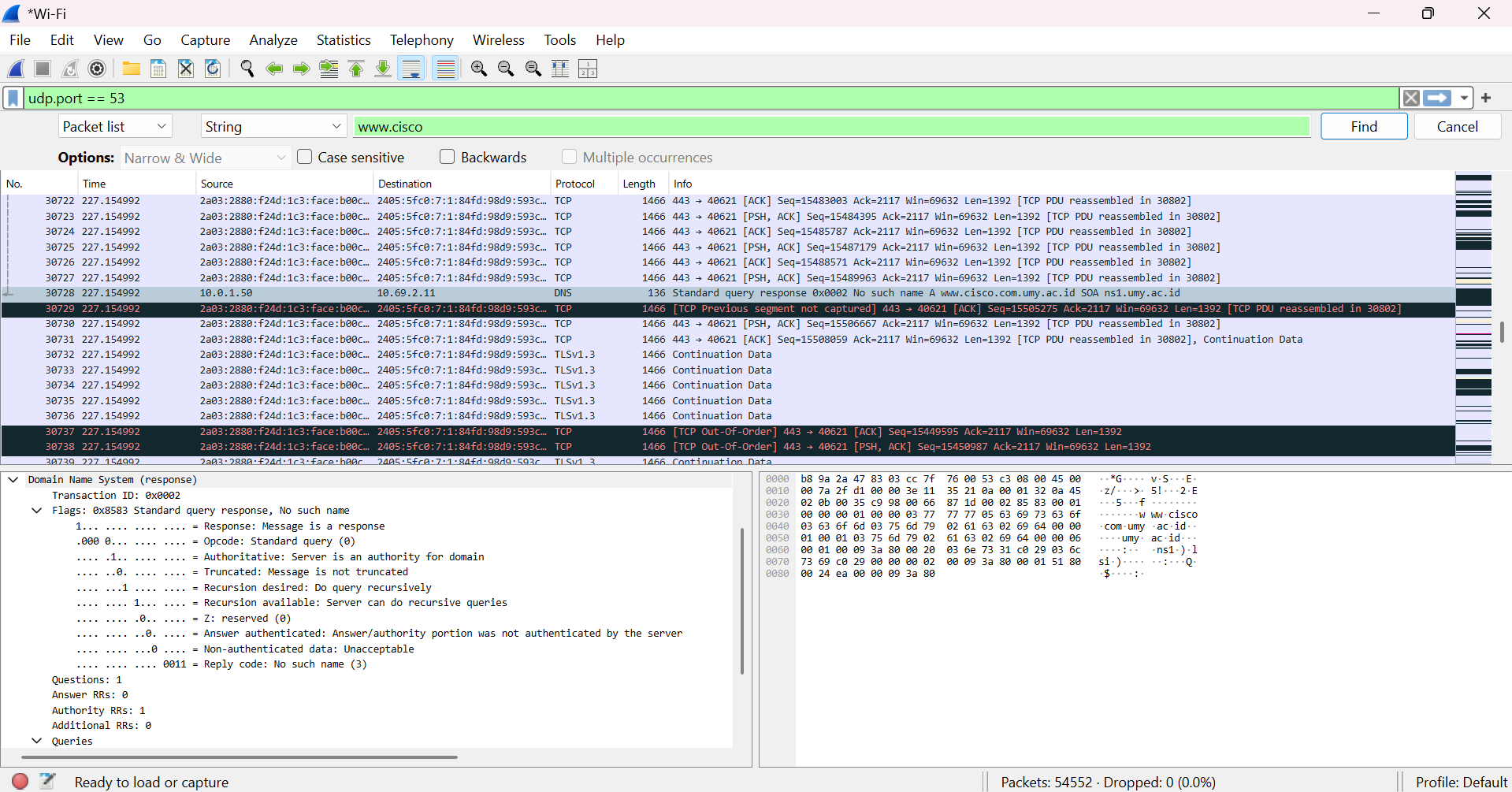
# Part 3: Explore DNS Response Traffic

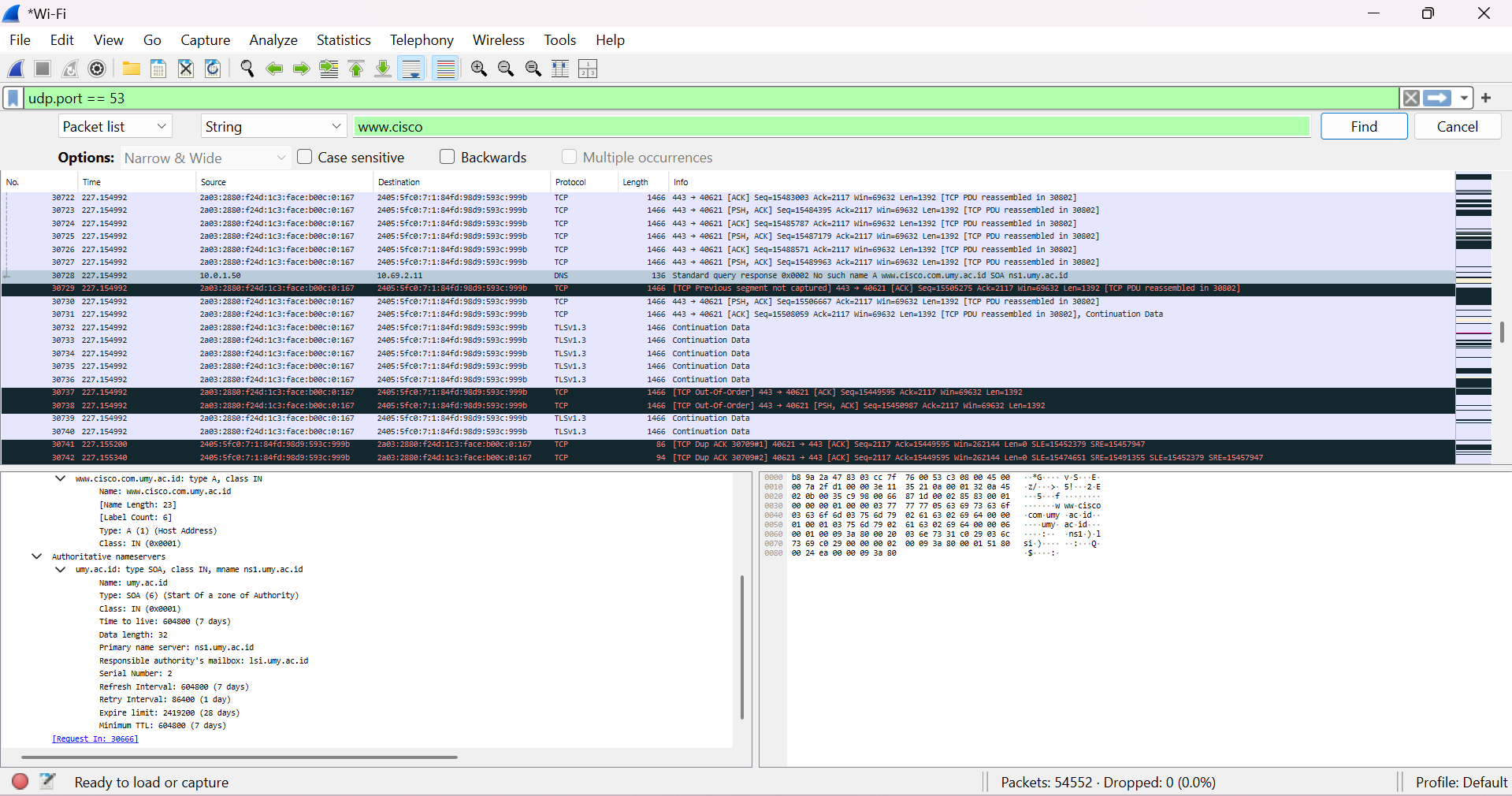
1. Select the corresponding response DNS packet labeled **Standard query response 0x0002 A** [**www.cisco.com**.](http://www.cisco.com/)



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?

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





Can the DNS server do recursive queries?

1. Observe the CNAME and A records in the answers details. How do the results compare to nslookup results?

# Reflection Question

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?