Lab 7.3.1.6 – Exploring DNS Traffic

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

Part 1: Explore DNS Query Traffic

Part 2: 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, use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Part 1: Explore DNS Query Traffic

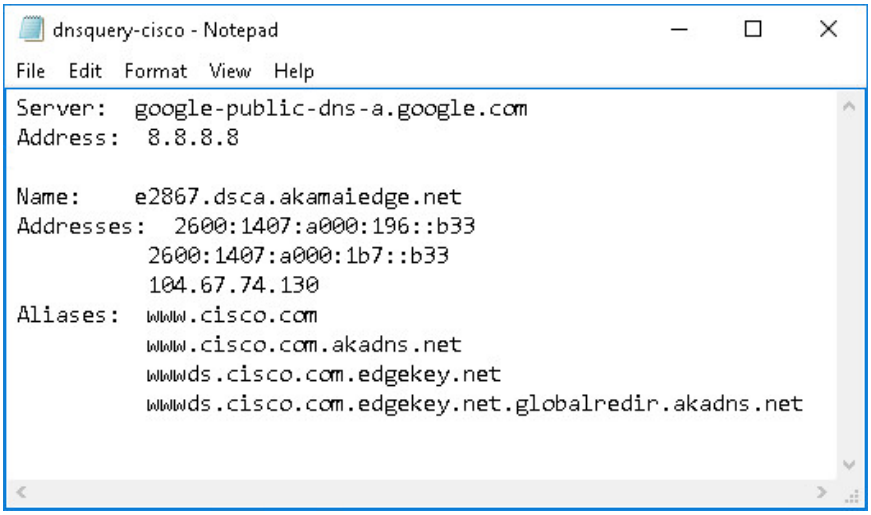
a. Access the **WinClient** machine. Unlock the machine by clicking on the drop-down arrow for that specific machine's tab and select **Send CTRL+ALT+DEL**.

b. Login as the `CyberOpsUser` using `cyberops` as the password.

c. On the *Desktop*, navigate to the **Toolbox** folder and open the **dns_query_files** folder.

d. Open the **dnsquery-cisco.txt** file.

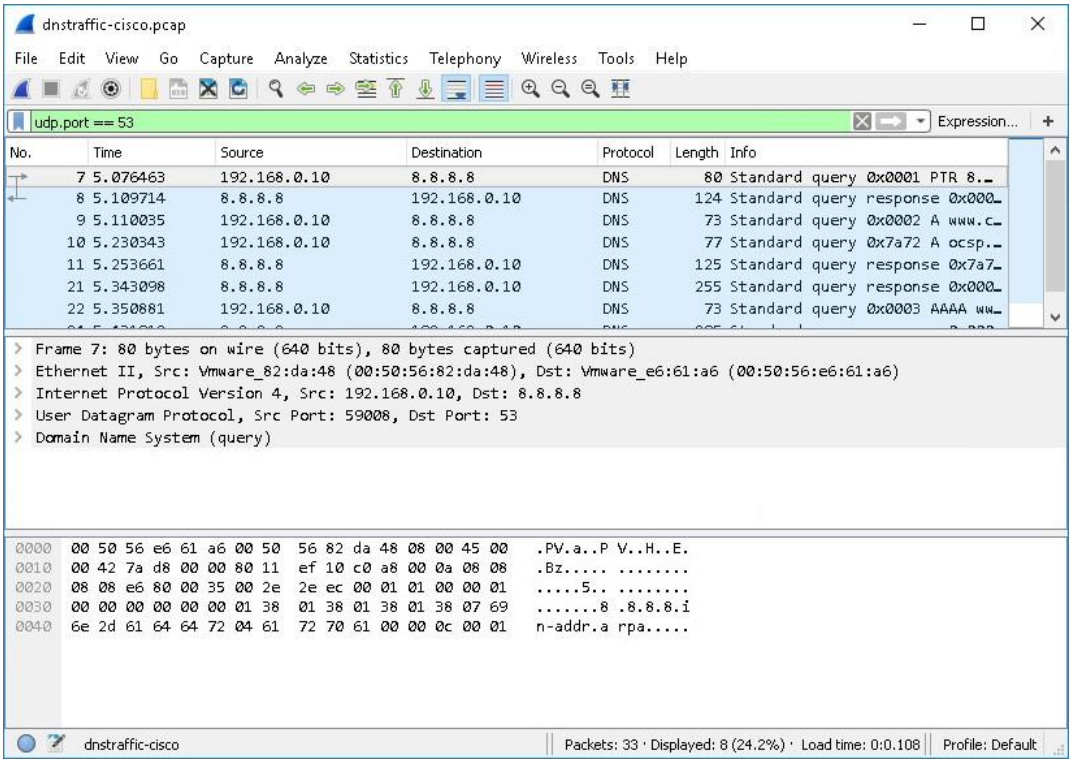
e. Notice the *DNS* query information from the www.cisco.com domain.



f. Minimize the **Notepad** application and change focus to the **Toolbox** folder.

g. Launch the **Wireshark** application. Navigate to **File > Open** and choose to open the **dnstraffic-cisco.pcap** file from the **pcaps** folder in the *Toolbox* folder.

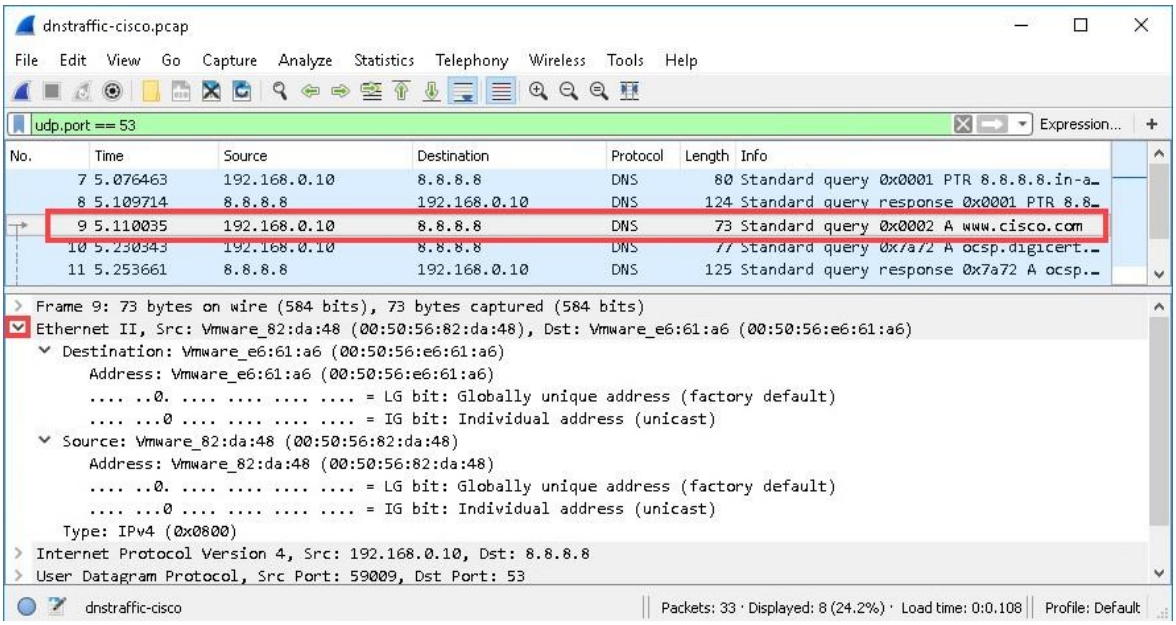
h. Observe the traffic captured in the *Wireshark Packet List* pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets.



i. Select the DNS packet labeled **Standard query 0x0002 A www.cisco.com**.

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

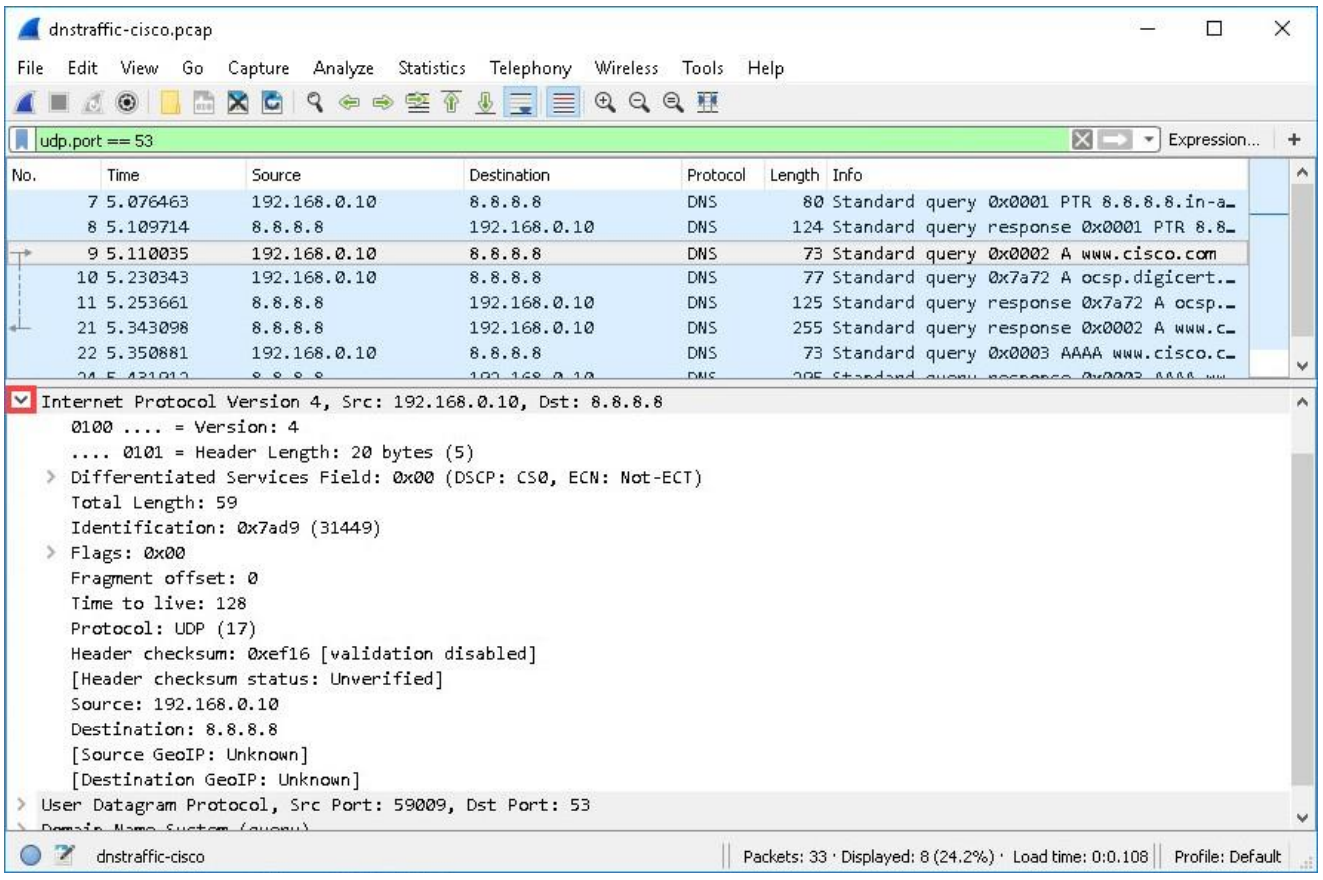
k. Expand **Ethernet II** to view the details. Observe the source and destination fields.



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

The Source MAC address is 192.168.0.10. It is associated with NIC and Destination MAC address is 8.8.8.8. It is associated with default gateway. This is associated DNS protocol.

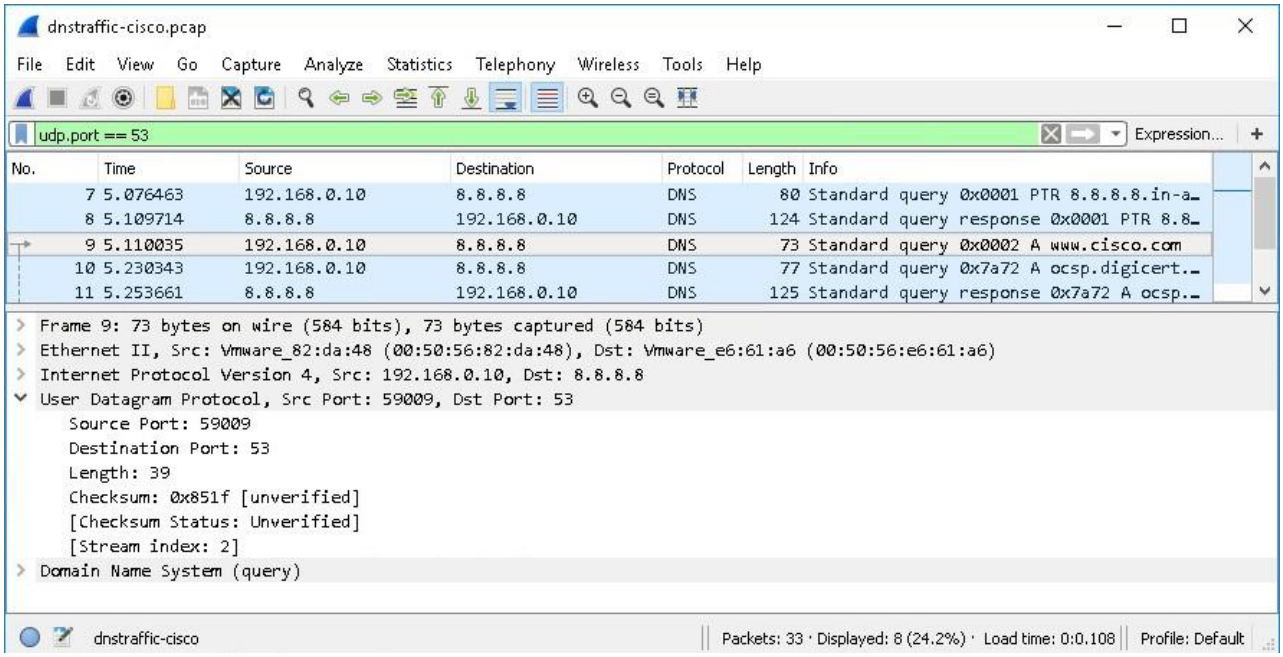
l. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.



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

The Source IP address is 192.168.0.10. It is associated with NIC and Destination IP address is 8.8.8.8. It is associated with default gateway. This is associated with DNS network.

m. 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?

The source port number is 59009 then the destination port number is 53 and it is associated with the default DNS protocol.

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

```
C:\Windows\system32>arp -a

Interface: 192.168.0.10 --- 0x8
  Internet Address      Physical Address      Type
  192.168.0.1           08-00-27-8c-29-85     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 169.254.12.163 --- 0xa
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

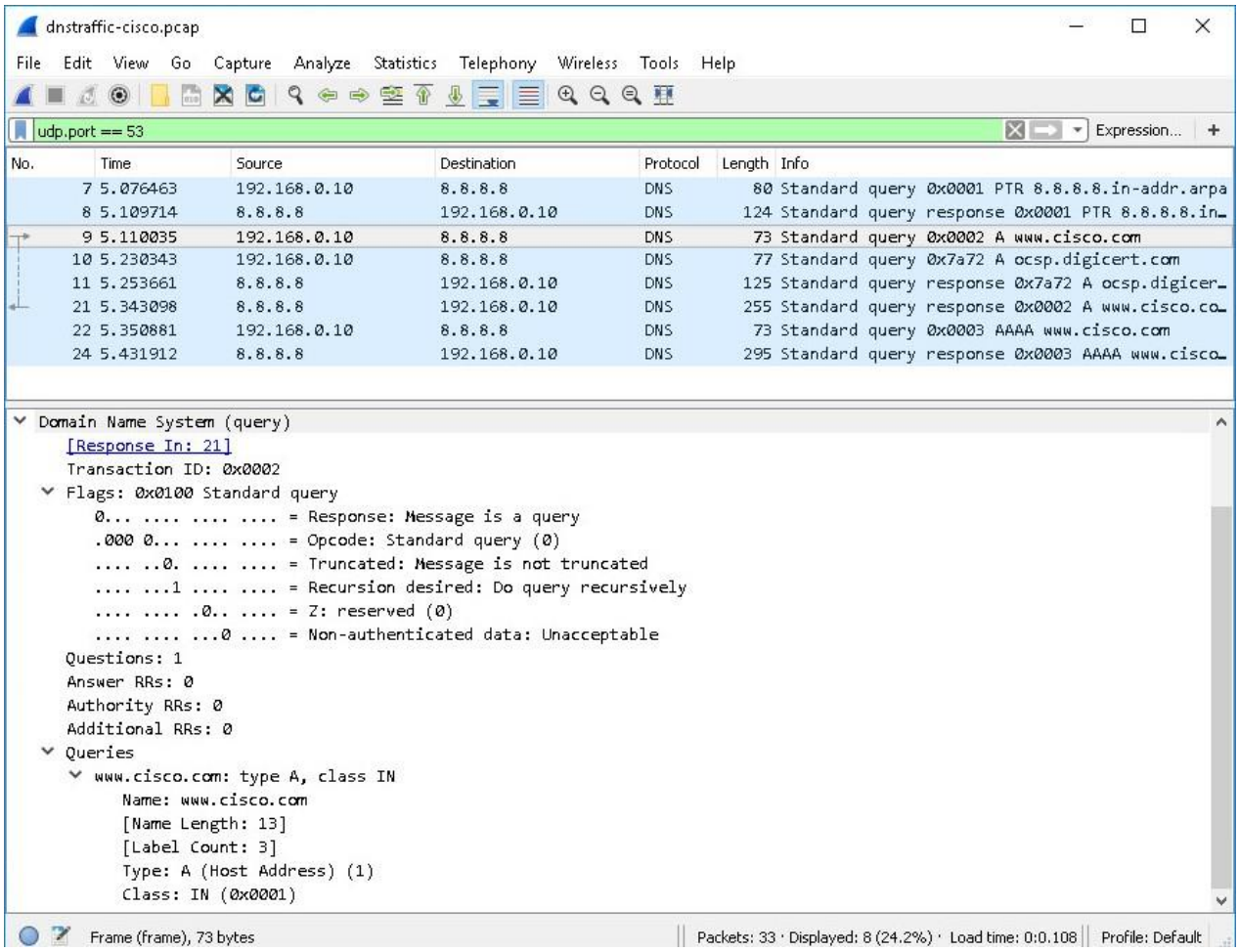
```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-8H4SOVG3LCL
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-82-DA-48
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a5b9:4eb7:1d5:818a%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 50352214
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-22-3B-17-9B-00-50-56-82-DA-48
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Compare the MAC and IP addresses in the Wireshark results to the results from the **ipconfig /all** results. What is your observation?

The MAC and IP address in the Wireshark results are same as the address from the above ipconfig/all command.

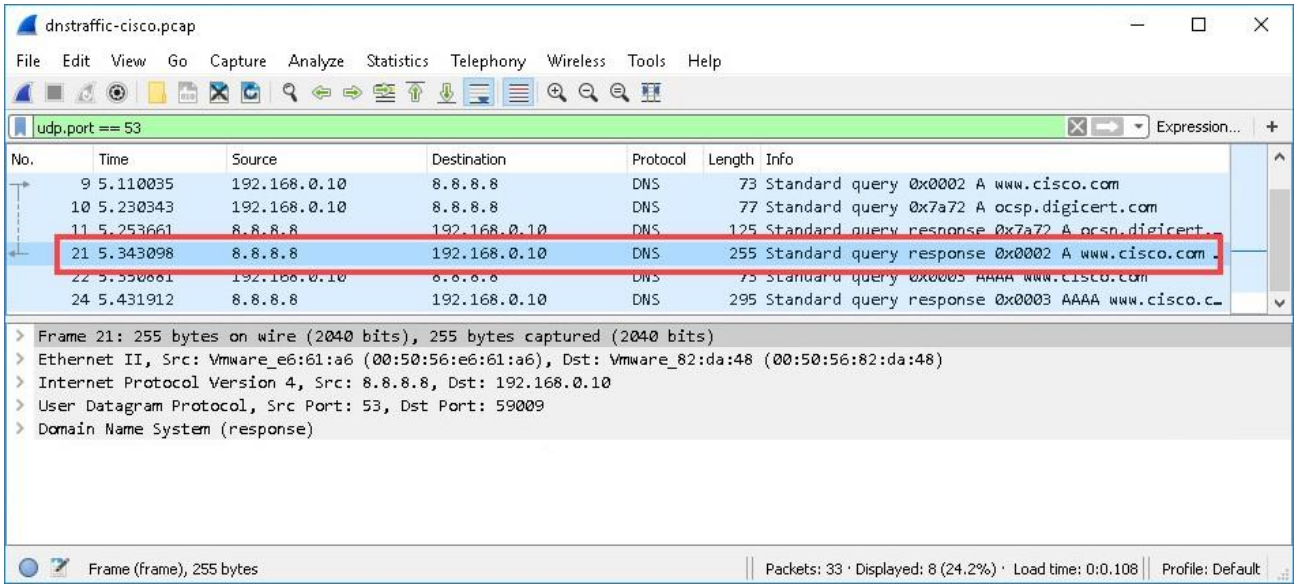
o. Change focus to the **Wireshark** application and expand **Domain Name System (query**) in the *Packet Details* pane followed by expanding **Flags** and **Queries**.

p. Observe the results. The flag is set to do the query recursively. The query is requesting the IP address to *www.cisco.com*.



Part 2: Explore DNS Response Traffic

a. Select the corresponding response DNS packet labeled **Standard query response 0x0002 A www.cisco.com**.

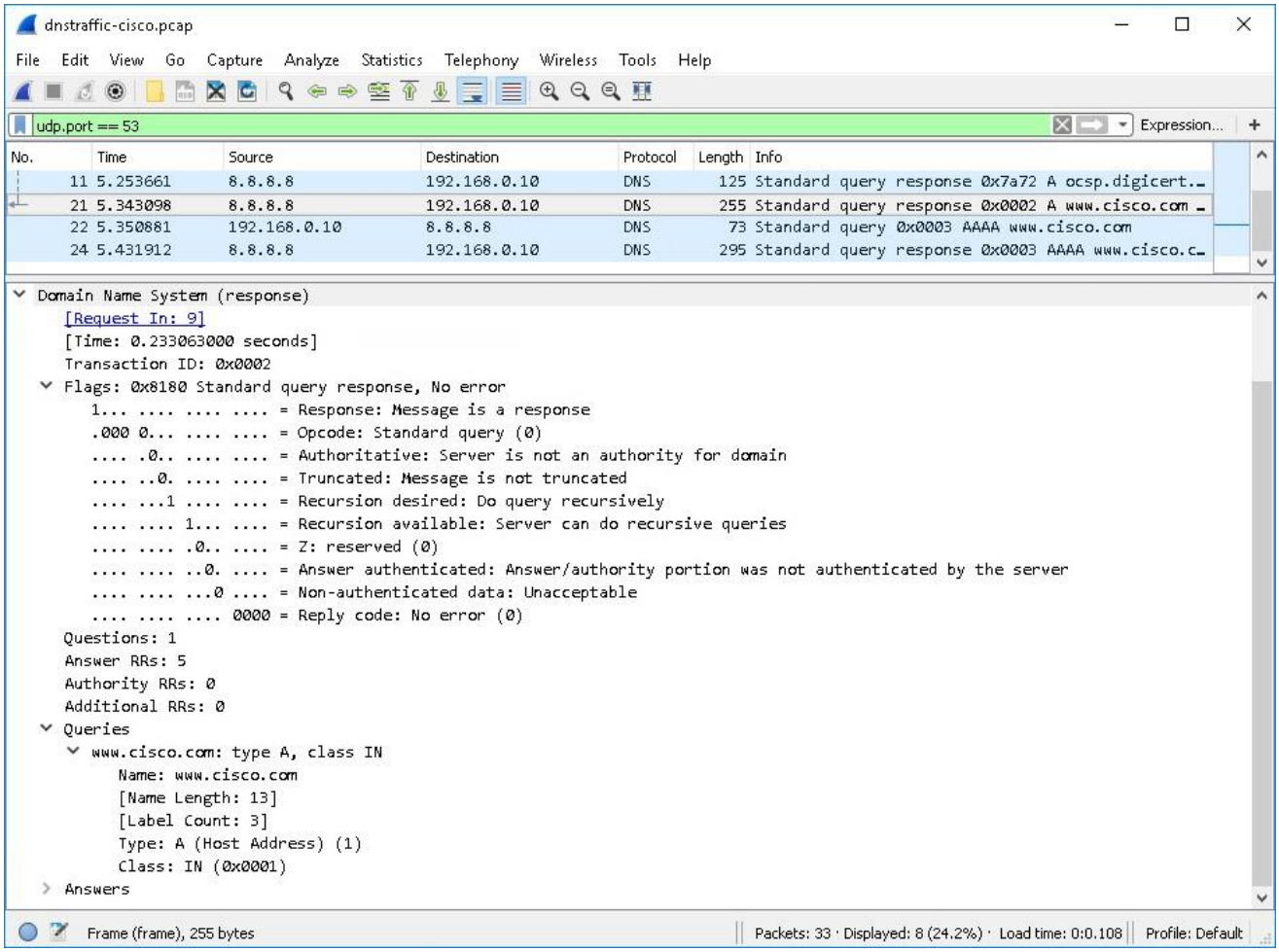


What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

The Source MAC address, IP address and port number in the query packets are known as Destination address. Destination MAC address, IP address and port number in the query packets are called as Source address.

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

c. Observe the results. Can the DNS server do recursive queries? YES



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

The result in nslookup is same as Wireshark in records.

Reflection

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

When you remove the filter in Wireshark, you can learn a lot more about the network traffic such as security risks,bandwidth usage and network protocols.

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

Wireshark is a network analysis mechanism that can be used to capture and inspect network traffic in real- time. Such as to gain sensitive information such as login credentials, credit card numbers and confidential data.