

## 3.8.8 Lab – Explore DNS Traffic (Answers)

---

 [itexamanswers.net/3-8-8-lab-explore-dns-traffic-answers.html](https://itexamanswers.net/3-8-8-lab-explore-dns-traffic-answers.html)

October 2, 2020

### Lab – Explore DNS Traffic (Instructor Version)

---

#### 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

**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

---

##### Step 1: Capture DNS traffic.

---

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



b. At the Command Prompt, enter `ipconfig /flushdns` clear the DNS cache.

```
C:\Users\Student> ipconfig /flushdns
```

```
Windows IP Configuration
```

```
Successfully flushed the DNS Resolver Cache.
```

c. Enter `nslookup` at the prompt to enter the nslookup interactive mode.

d. 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** at the > prompt.

```

C:\Users\Student> nslookup
Default Server:  UnKnown
Address:  68.105.28.16

> www.cisco.com
Server:  UnKnown
Address:  68.105.28.16

Non-authoritative answer:
Name:      e2867.dsca.akamaiedge.net
Addresses: 2001:578:28:68d::b33
           2001:578:28:685::b33
           96.7.79.147
Aliases:   www.cisco.com
           www.cisco.com.akadns.net
           wwwds.cisco.com.edgekey.net
           wwwds.cisco.com.edgekey.net.globalredir.akadns.net

```

e. Enter **exit** when finished to exit the nslookup interactive mode. Close the command prompt.

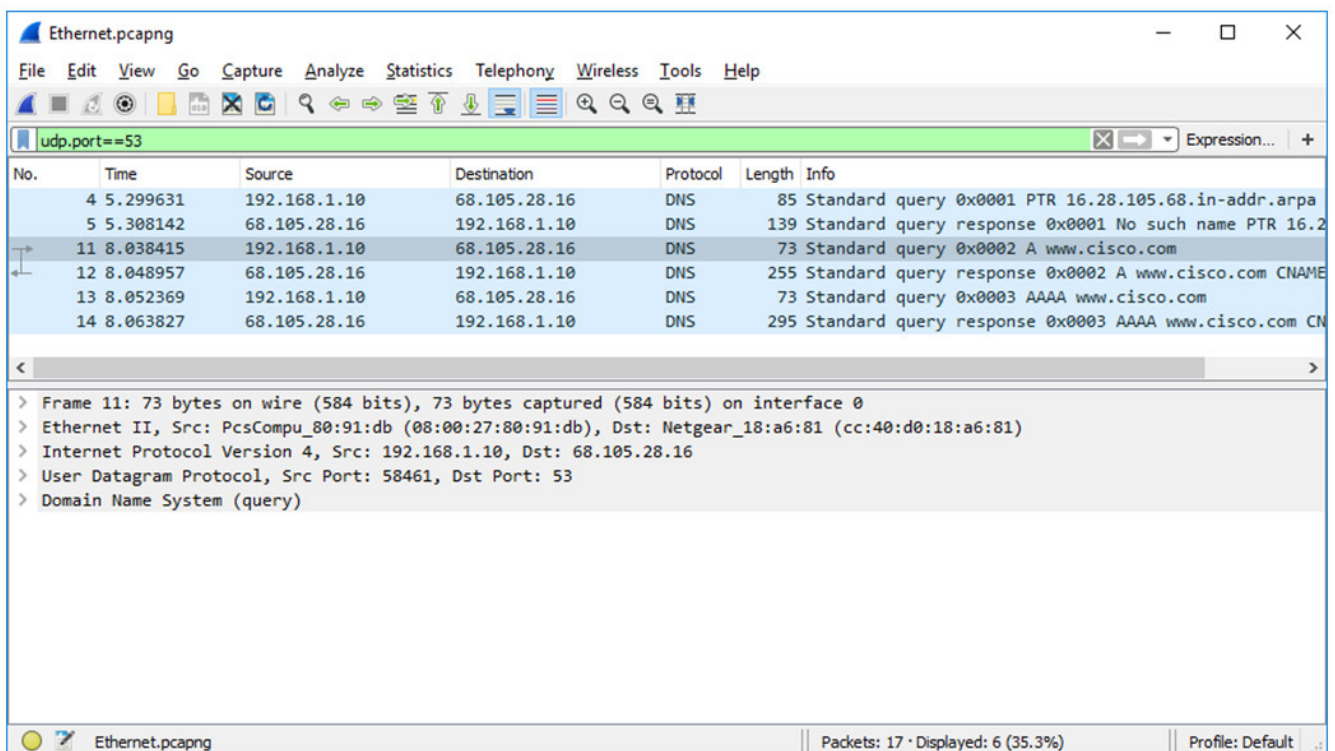
f. Click **Stop capturing packets** to stop the Wireshark capture.

## Step 2: Explore DNS Query Traffic

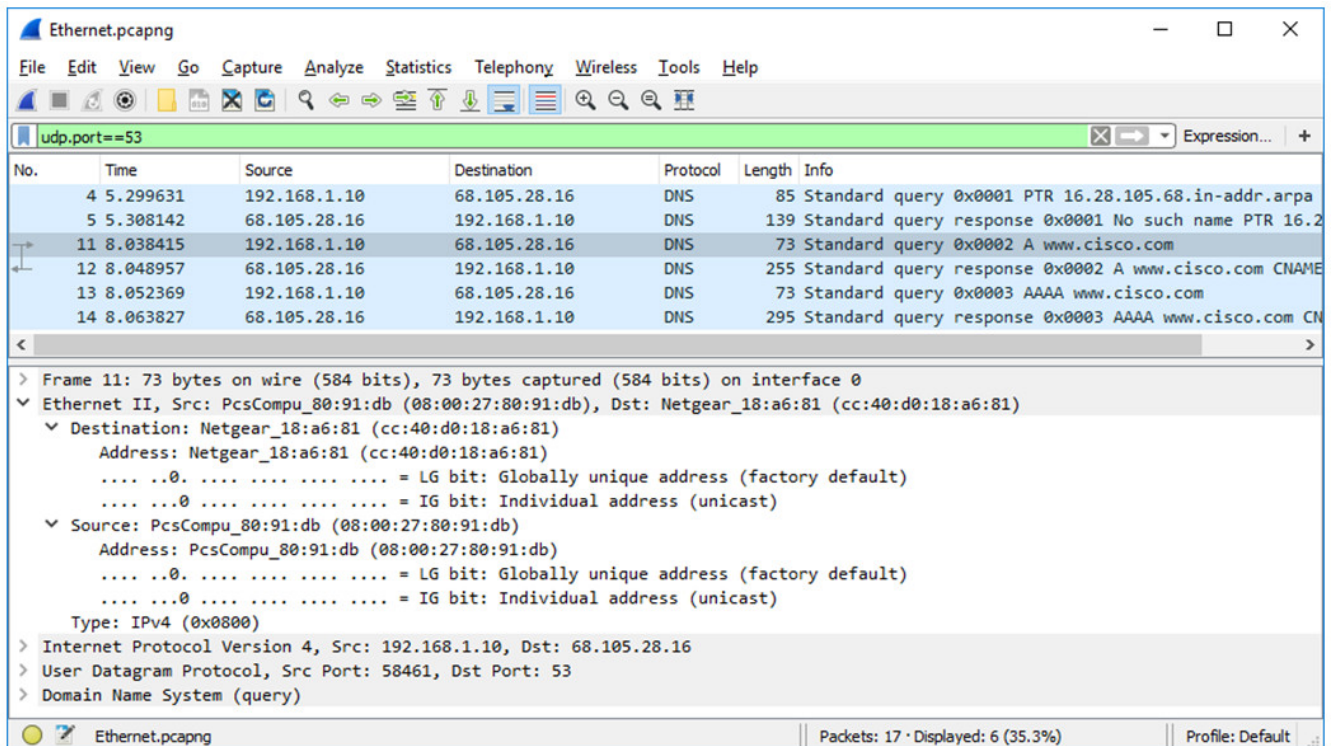
a. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets.

b. Select the DNS packet labeled **Standard query 0x0002 A 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).



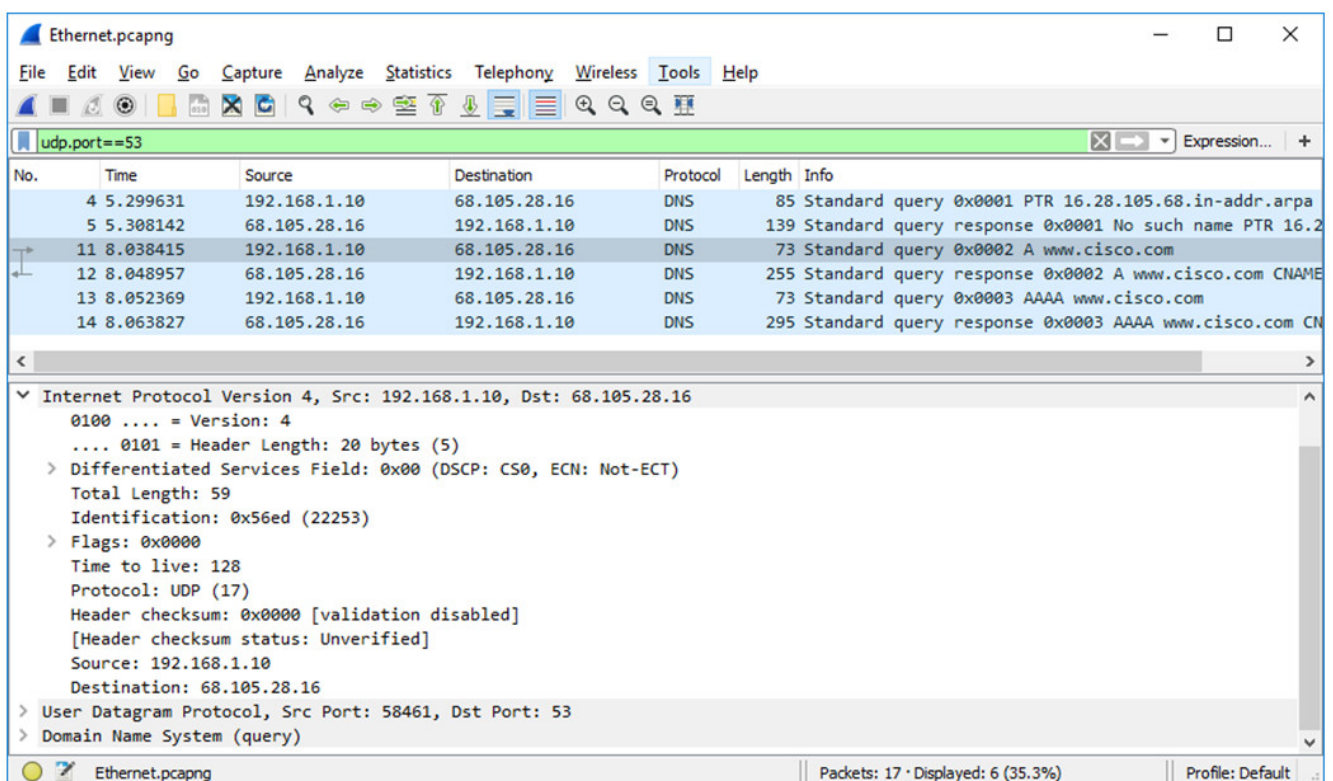
c. Expand **Ethernet II** to view the details. Observe the source and destination fields.



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

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.

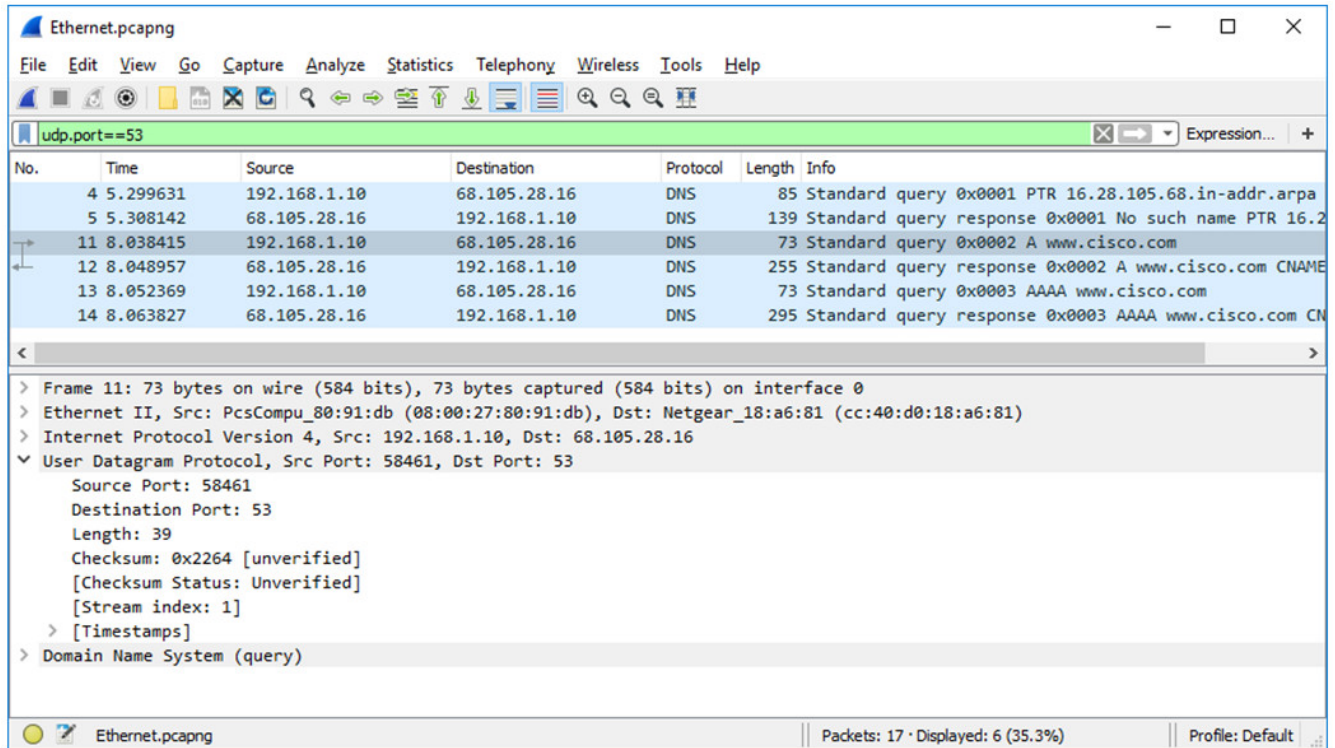
a. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.



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

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

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



No.	Time	Source	Destination	Protocol	Length	Info
4	5.299631	192.168.1.10	68.105.28.16	DNS	85	Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
5	5.308142	68.105.28.16	192.168.1.10	DNS	139	Standard query response 0x0001 No such name PTR 16.2
11	8.038415	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0002 A www.cisco.com
12	8.048957	68.105.28.16	192.168.1.10	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME
13	8.052369	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0003 AAAA www.cisco.com
14	8.063827	68.105.28.16	192.168.1.10	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CN

Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0	
Ethernet II, Src: PcsCompu_80:91:db (08:00:27:80:91:db), Dst: Netgear_18:a6:81 (cc:40:d0:18:a6:81)	
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16	
User Datagram Protocol, Src Port: 58461, Dst Port: 53	
Source Port: 58461	
Destination Port: 53	
Length: 39	
Checksum: 0x2264 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 1]	
[Timestamps]	
Domain Name System (query)	

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

The source port number is 58461 and the destination port is 53, which is the default DNS port number.

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

```
C:\Users\Student> arp -a
```

```
Interface: 192.168.1.10 --- 0x4
```

Internet Address	Physical Address	Type
192.168.1.1	cc-40-d0-18-a6-81	dynamic
192.168.1.122	b0-a7-37-46-70-bb	dynamic
192.168.1.255	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:\Users\Student> ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : DESKTOP
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-80-91-DB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, August 20, 2019 5:39:51 PM
Lease Expires . . . . . : Wednesday, August 21, 2019 5:39:50 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 50855975
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
DNS Servers . . . . . : 68.105.28.16
                        68.105.29.16
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 IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in `arp -a` and `ipconfig /all` command.

d. 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`.



Ethernet.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
4	5.299631	192.168.1.10	68.105.28.16	DNS	85	Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
5	5.308142	68.105.28.16	192.168.1.10	DNS	139	Standard query response 0x0001 No such name PTR 16.2
11	8.038415	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0002 A www.cisco.com
12	8.048957	68.105.28.16	192.168.1.10	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME
13	8.052369	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0003 AAAA www.cisco.com
14	8.063827	68.105.28.16	192.168.1.10	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CN

> Frame 11: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

> Ethernet II, Src: PcsCompu\_80:91:db (08:00:27:80:91:db), Dst: Netgear\_18:a6:81 (cc:40:d0:18:a6:81)

> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 68.105.28.16

> User Datagram Protocol, Src Port: 58461, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

▼ Flags: 0x0100 Standard query

- 0... .. = Response: Message is a query
- .000 0... .. = Opcode: Standard query (0)
- .... 0... .. = Truncated: Message is not truncated
- .... ..1... .. = Recursion desired: Do query recursively
- .... ..0... .. = Z: reserved (0)
- .... ..0... .. = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ www.cisco.com: type A, class IN

- Name: www.cisco.com
- [Name Length: 13]
- [Label Count: 3]
- Type: A (Host Address) (1)
- Class: IN (0x0001)

[Response In: 12]

Do query recursively? (dns.flags.recdesired), 2 bytes

Packets: 17 · Displayed: 6 (35.3%)

Profile: Default

### Step 3: Explore DNS Response Traffic

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

Ethernet.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==53

No.	Time	Source	Destination	Protocol	Length	Info
4	5.299631	192.168.1.10	68.105.28.16	DNS	85	Standard query 0x0001 PTR 16.28.105.68.in-addr.arpa
5	5.308142	68.105.28.16	192.168.1.10	DNS	139	Standard query response 0x0001 No such name PTR 16.2
11	8.038415	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0002 A www.cisco.com
12	8.048957	68.105.28.16	192.168.1.10	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME
13	8.052369	192.168.1.10	68.105.28.16	DNS	73	Standard query 0x0003 AAAA www.cisco.com
14	8.063827	68.105.28.16	192.168.1.10	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CN

< >

> Frame 12: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface 0  
 > Ethernet II, Src: Netgear\_18:a6:81 (cc:40:d0:18:a6:81), Dst: PcsCompu\_80:91:db (08:00:27:80:91:db)  
 > Internet Protocol Version 4, Src: 68.105.28.16, Dst: 192.168.1.10  
 > User Datagram Protocol, Src Port: 53, Dst Port: 58461  
 > Domain Name System (response)

Number of answers in packet (dns.count.answers), 2 bytes

Packets: 17 · Displayed: 6 (35.3%)

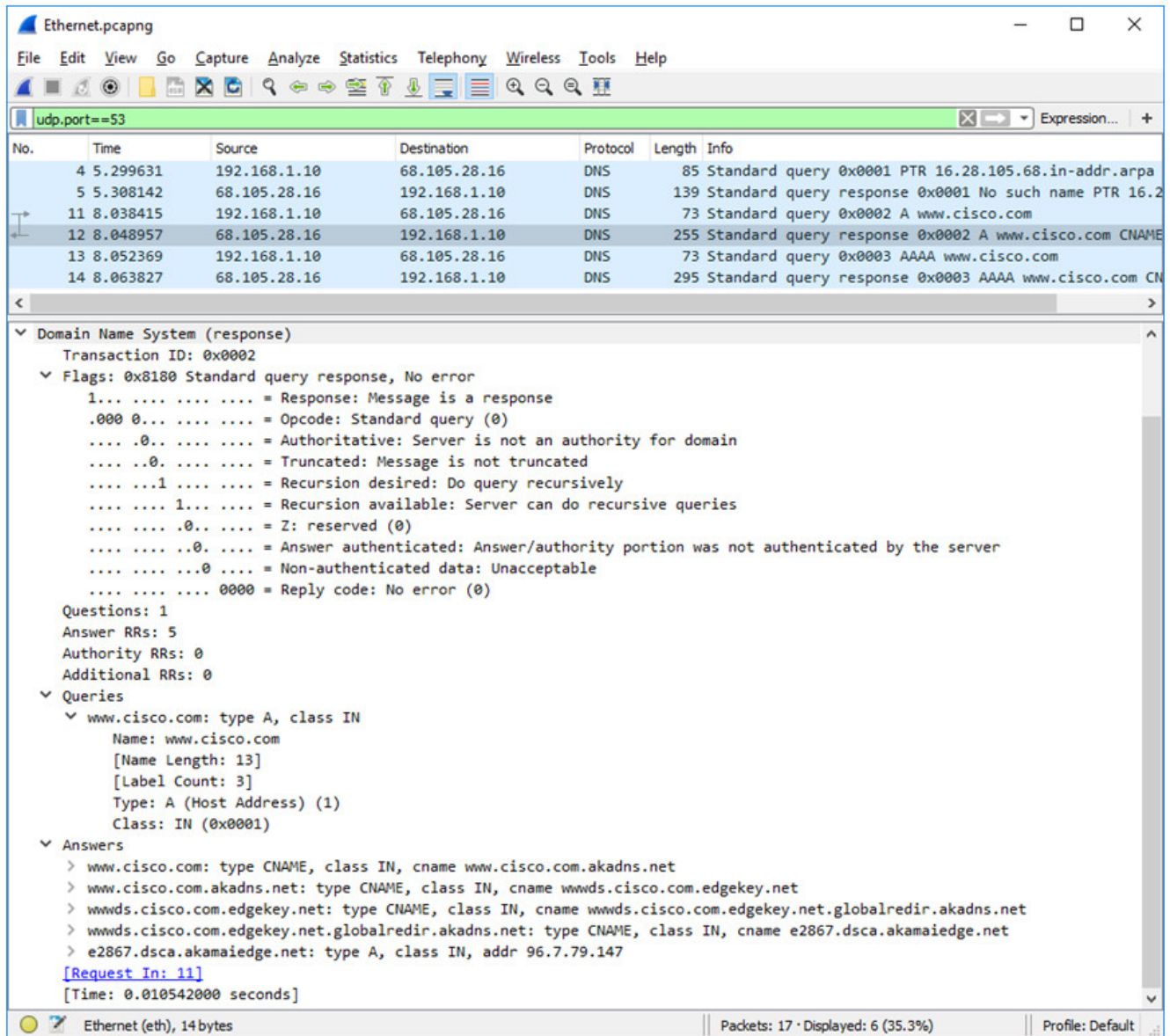
Profile: Default

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.

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





Can the DNS server do recursive queries?

Yes, the DNS can handle recursive queries.

c. Observe the CNAME and A records in the answers details.

How do the results compare to nslookup results?

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

## Reflection Question

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

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.

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

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.

**Download PDF & PKT file Completed 100% Score:**

---

[sociallocker id="54558"][/sociallocker]