



LAB 2 - EXPLORE DNS TRAFFIC

Mohamad Saiful Nizam Bin Abd Aziz (Apol)
A179830

Lab 2 - 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.

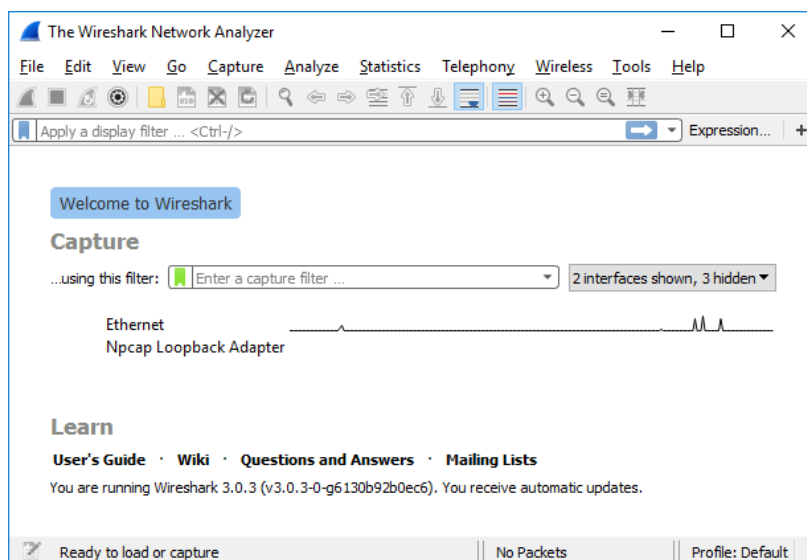
Required Resources

- 1 Windows PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS traffic.

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



- 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** 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.

```
C:\Users\HP-PC>ipconfig/flushdns

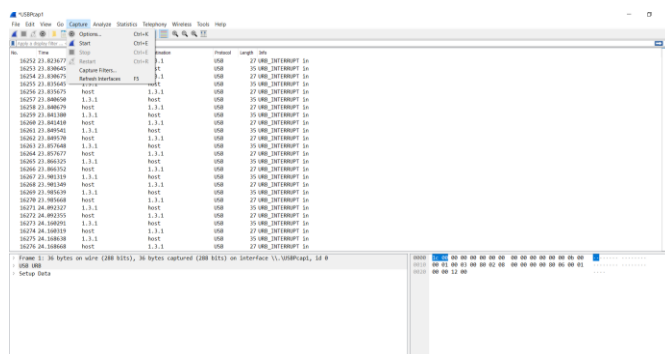
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\HP-PC>nslookup
Default Server: cdns01v6.tm.net.my
Address: 2001:e68:b:68

>
>
> www.cisco.com
Server: cdns01v6.tm.net.my
Address: 2001:e68:b:68

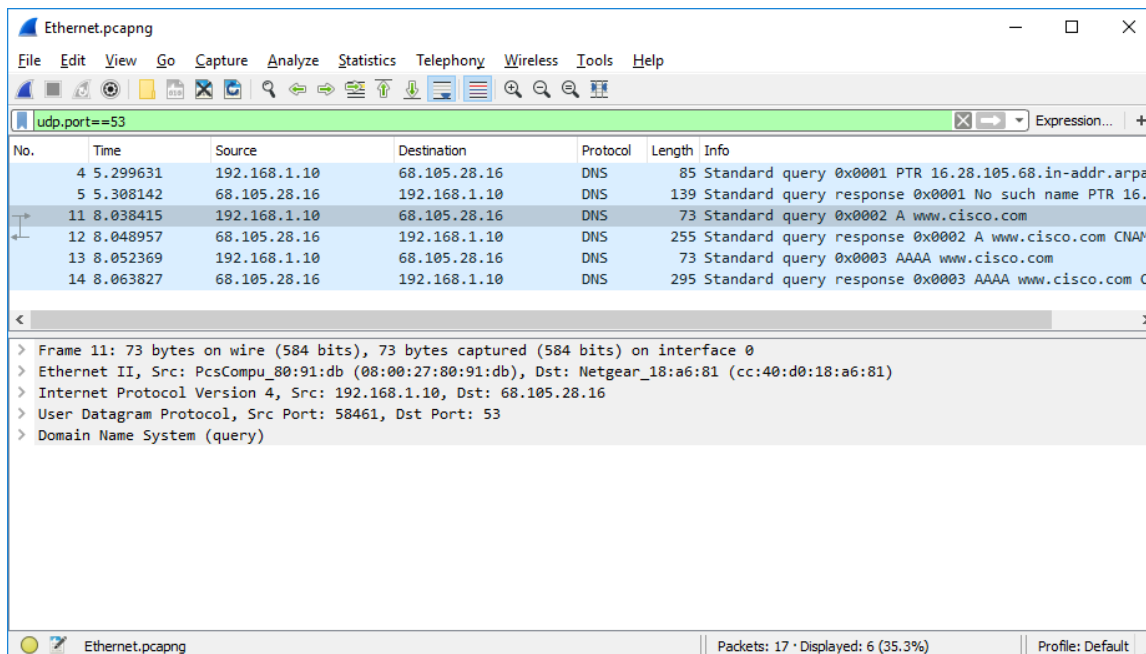
Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2001:e68:5:82::b33
2001:e68:5:8d::b33
118.214.84.167
Aliases: www.cisco.com
www.cisco.com.akadns.net
wwwds.cisco.com.edgekey.net
wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```



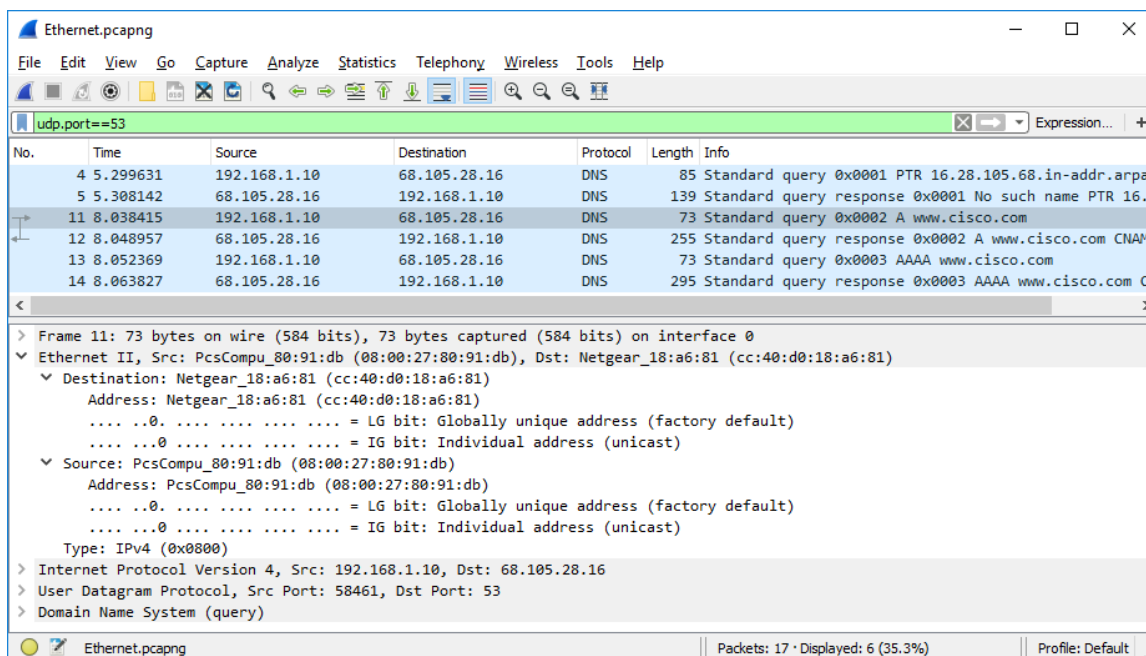
Part 2: Explore DNS Query Traffic

- 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.
- 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).



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

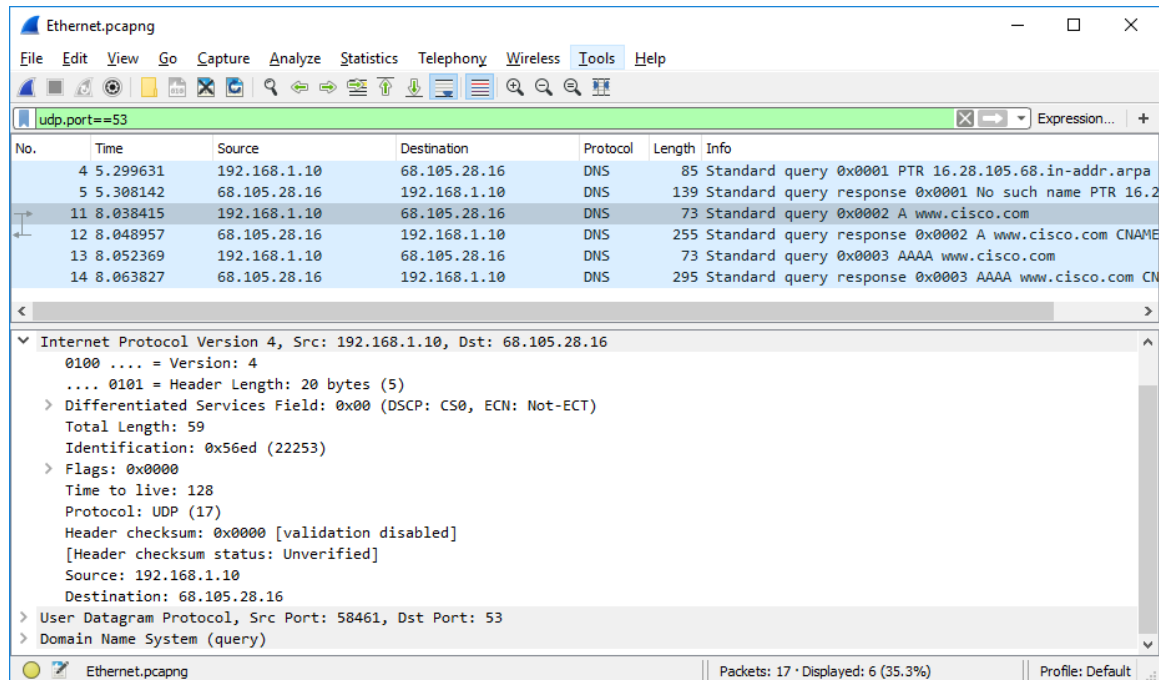


Lab 2 - Explore DNS Traffic

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

The default gateway is connected to the destination MAC address and the PC's NIC to the source MAC address. If a local DNS server is operating, its MAC address would function as the destination MAC address.

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

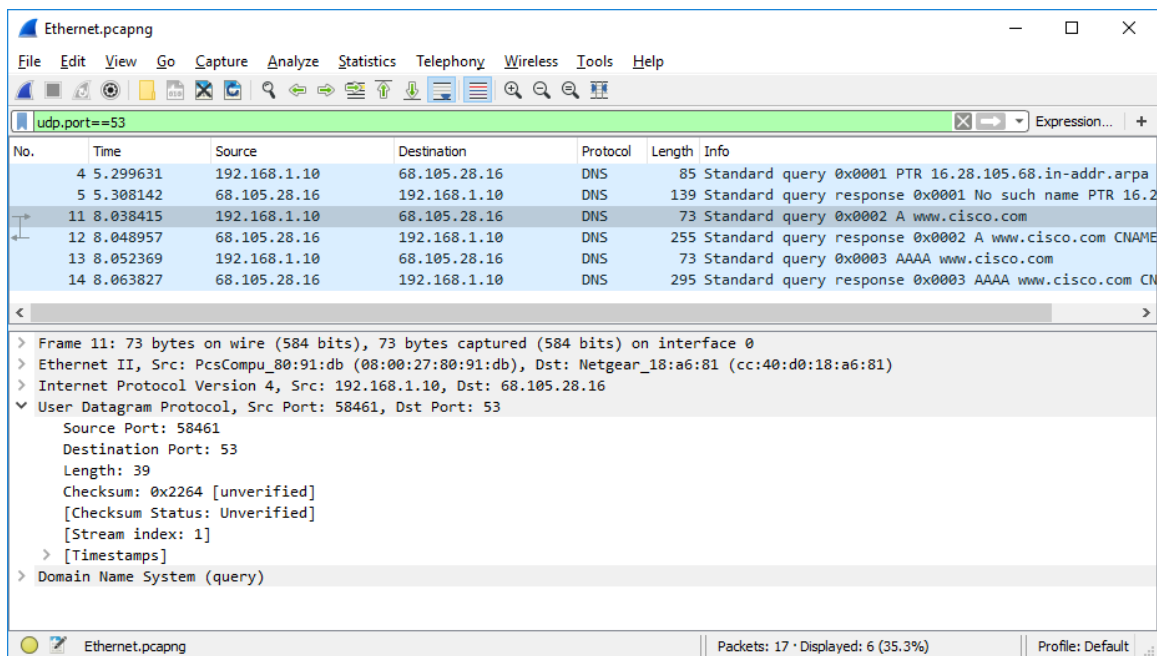


What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

The DNS server is connected to the destination IP address, while the source IP address is connected to the PC's NIC.

Lab 2 - Explore DNS Traffic

- 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?

The destination port is 53(default DNS port number) and the source port is 58461.

- 2) 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 arp - a and ipconfig /all commands both list the same IP and MAC addresses as those recorded by Wireshark.

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

Lab 2 - Explore DNS Traffic

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_00:91: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)
- = 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

Part 3: Explore DNS Response Traffic

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

The screenshot shows a Wireshark packet capture window titled "Ethernet.pcapng". The filter bar at the top shows "udp.port==53". The packet list contains six entries, with packet 12 selected. The details pane for packet 12 shows the following structure:

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

The details pane for packet 12 shows the following structure:

- 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)

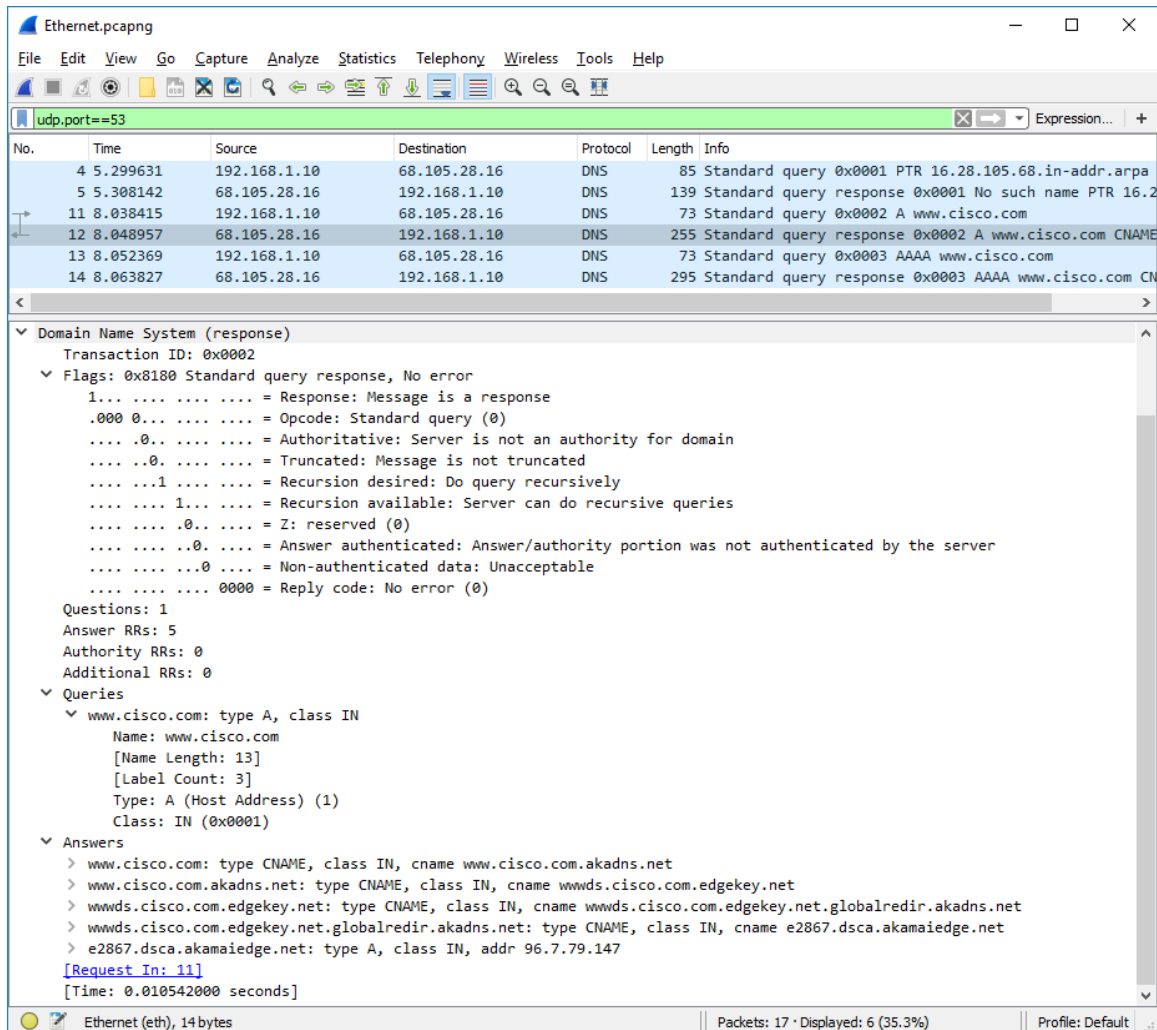
The status bar at the bottom shows "Number of answers in packet (dns.count.answers), 2 bytes" and "Packets: 17 · Displayed: 6 (35.3%)".

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 query packet's source IP, MAC address, and port number are now the destination addresses. The source addresses in the inquiry packet are now the destination IP, MAC address, and port number.

Lab 2 - Explore DNS Traffic

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



The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list at the top shows several DNS packets. The packet details pane is expanded to show the 'Domain Name System (response)' section for a specific packet. The flags section shows the response code as 'No error (0)'. The queries section shows a query for 'www.cisco.com' of type A, class IN. The answers section shows several CNAME and A records, including 'www.cisco.com.akadns.net' and 'www.cisco.com.akadns.net.edgekey.net'.

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

Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... 0... .. = Authoritative: Server is not an authority for domain
... ..0. = Truncated: Message is not truncated
... ..1 = Recursion desired: Do query recursively
... ..1 = Recursion available: Server can do recursive queries
... ..0... .. = Z: reserved (0)
... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
... ..0... .. = Non-authenticated data: Unacceptable
... ..0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 5
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)
Answers
www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
e2867.dsca.akamaiedge.net: type A, class IN, addr 96.7.79.147
[Request In: 11]
[Time: 0.010542000 seconds]

Can the DNS server do recursive queries?

Yes, recursive queries are handled by the DNS.

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

How do the results compare to nslookup results?

The results from nslookup in the Command Prompt are same with the result in Wireshark.

Reflection Question

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

Without the filters, other packets, such as DHCP and ARP will appear in the results. We can discover information about other devices and their roles inside the LAN from these packets and the data they include.

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

If the network traffic is not encrypted, an attacker on the LAN can use Wireshark to monitor it and obtain sensitive data in the packet details.