

## Lab - Explore DNS Traffic

**Nombre:** Luis Enrique Pérez Señalín

### 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.

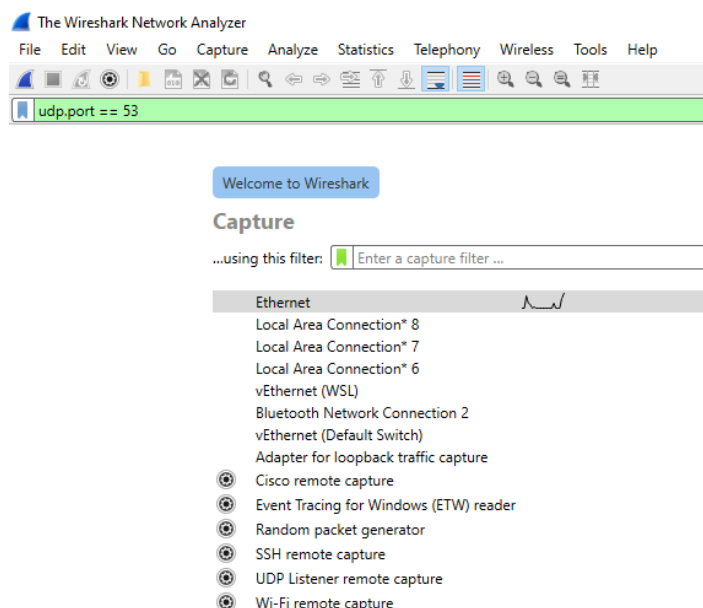
### Required Resources

- 1 Windows PC with internet access and Wireshark installed

### Instructions

#### Part 1: Capture DNS traffic.

- 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** 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
```

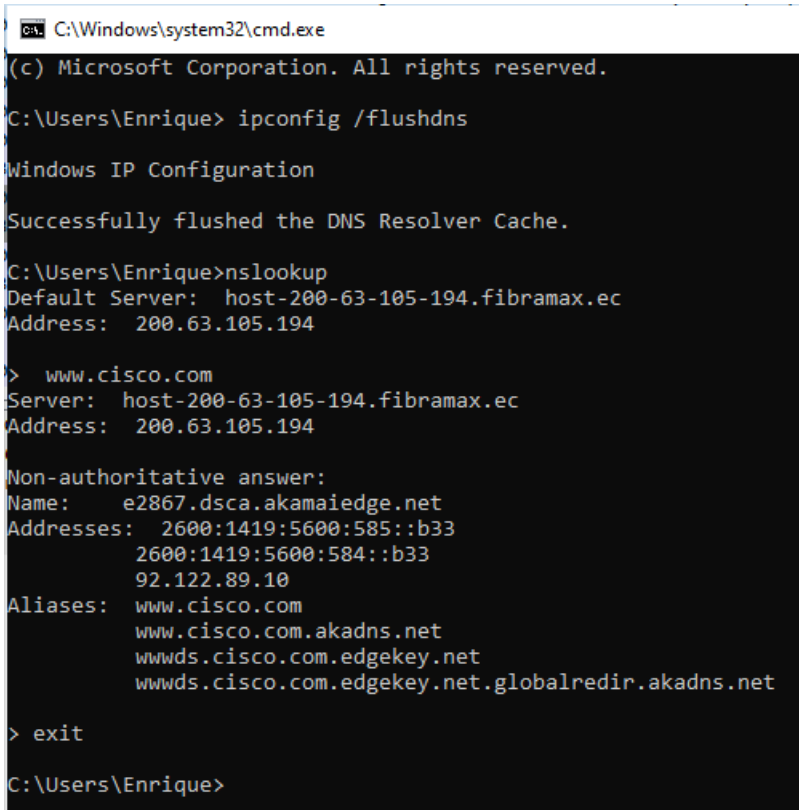
```
Aliases: www.cisco.com
```

```
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:\Windows\system32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

C:\Users\Enrique> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Enrique> nslookup
Default Server: host-200-63-105-194.fibramax.ec
Address: 200.63.105.194

> www.cisco.com
Server: host-200-63-105-194.fibramax.ec
Address: 200.63.105.194

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2600:1419:5600:585::b33
2600:1419:5600:584::b33
92.122.89.10
Aliases: www.cisco.com
www.cisco.com.akadns.net
wwwds.cisco.com.edgekey.net
wwwds.cisco.com.edgekey.net.globalredir.akadns.net

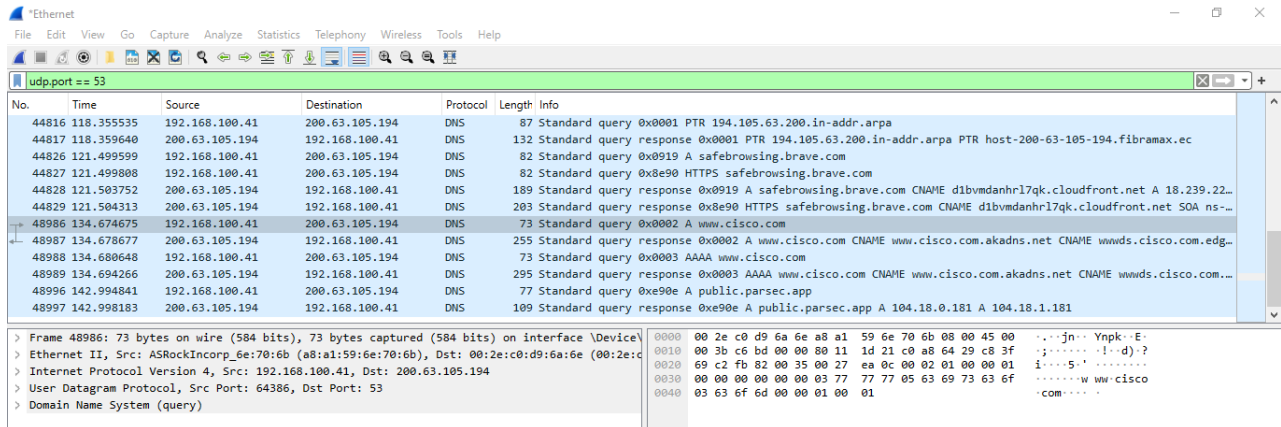
> exit

C:\Users\Enrique>
```

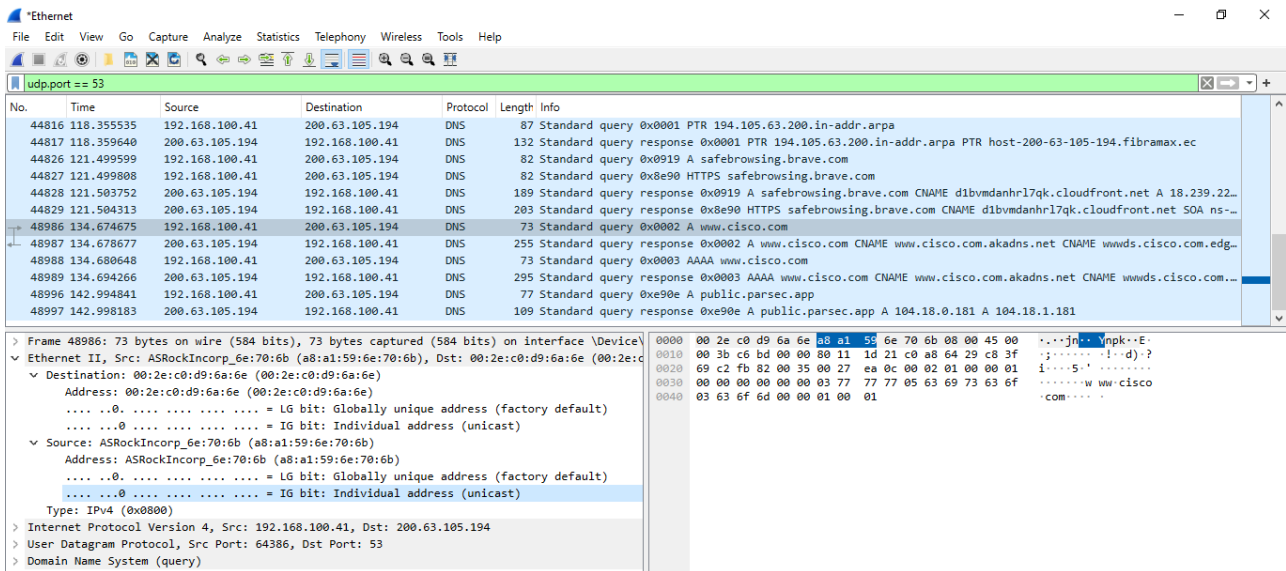
## Part 2: Explore DNS Query Traffic

- 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.



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

**R:** Destination MAC addresses: 00:2e:c0:d9:6a:6e Source MAC addresses: a8:a1:59:6e:70:6b.

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

The screenshot shows a Wireshark packet capture of DNS traffic. The packet list pane displays a list of packets, with packet 48986 selected. The packet details pane shows the expanded Internet Protocol Version 4 header, displaying the source address as 192.168.100.41 and the destination address as 200.63.105.194. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
44816	118.355535	192.168.100.41	200.63.105.194	DNS	87	Standard query 0x0001 PTR 194.105.63.200.in-addr.arpa
44817	118.359640	200.63.105.194	192.168.100.41	DNS	132	Standard query response 0x0001 PTR 194.105.63.200.in-addr.arpa PTR host-200-63-105-194.fibramax.ec
44826	121.499599	192.168.100.41	200.63.105.194	DNS	82	Standard query 0x0919 A safebrowsing.brave.com
44827	121.499808	192.168.100.41	200.63.105.194	DNS	82	Standard query 0x8e90 HTTPS safebrowsing.brave.com
44828	121.503752	200.63.105.194	192.168.100.41	DNS	189	Standard query response 0x0919 A safebrowsing.brave.com CNAME d1bvmndanhr17qk.cloudfront.net A 18.239.22...
44829	121.504313	200.63.105.194	192.168.100.41	DNS	203	Standard query response 0x8e90 HTTPS safebrowsing.brave.com CNAME d1bvmndanhr17qk.cloudfront.net SOA ns-...
48986	134.674675	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0002 A www.cisco.com
48987	134.678677	200.63.105.194	192.168.100.41	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edg...
48988	134.680648	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0003 AAAA www.cisco.com
48989	134.694266	200.63.105.194	192.168.100.41	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com...
48996	142.994841	192.168.100.41	200.63.105.194	DNS	77	Standard query 0xe90e A public.parsec.app
48997	142.998183	200.63.105.194	192.168.100.41	DNS	109	Standard query response 0xe90e A public.parsec.app A 104.18.0.181 A 104.18.1.181

Packet 48986 details:

- Frame 48986: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF...
- Ethernet II, Src: ASRockIncorp\_6e:70:6b (a8:a1:59:6e:70:6b), Dst: 00:2e:c0:d9:6a:6e (00:2e:c0:d9:6a:6e)
- Internet Protocol Version 4, Src: 192.168.100.41, Dst: 200.63.105.194
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 59
  - Identification: 0xc6bd (50877)
  - 0000 .... = Flags: 0x0
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 128
  - Protocol: UDP (17)
  - Header Checksum: 0xd21 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 192.168.100.41
  - Destination Address: 200.63.105.194
- User Datagram Protocol, Src Port: 64386, Dst Port: 53
- Domain Name System (query)

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

**R:** Source IP addresses: 192.168.100.41, Destination IP addresses: 200.63.105.194

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

The screenshot shows a Wireshark packet capture of DNS traffic. The packet list pane displays a list of packets, with packet 48986 selected. The packet details pane shows the expanded User Datagram Protocol header, displaying the source port as 64386 and the destination port as 53. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
44816	118.355535	192.168.100.41	200.63.105.194	DNS	87	Standard query 0x0001 PTR 194.105.63.200.in-addr.arpa
44817	118.359640	200.63.105.194	192.168.100.41	DNS	132	Standard query response 0x0001 PTR 194.105.63.200.in-addr.arpa PTR host-200-63-105-194.fibramax.ec
44826	121.499599	192.168.100.41	200.63.105.194	DNS	82	Standard query 0x0919 A safebrowsing.brave.com
44827	121.499808	192.168.100.41	200.63.105.194	DNS	82	Standard query 0x8e90 HTTPS safebrowsing.brave.com
44828	121.503752	200.63.105.194	192.168.100.41	DNS	189	Standard query response 0x0919 A safebrowsing.brave.com CNAME d1bvmndanhr17qk.cloudfront.net A 18.239.22...
44829	121.504313	200.63.105.194	192.168.100.41	DNS	203	Standard query response 0x8e90 HTTPS safebrowsing.brave.com CNAME d1bvmndanhr17qk.cloudfront.net SOA ns-...
48986	134.674675	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0002 A www.cisco.com
48987	134.678677	200.63.105.194	192.168.100.41	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edg...
48988	134.680648	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0003 AAAA www.cisco.com
48989	134.694266	200.63.105.194	192.168.100.41	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com...
48996	142.994841	192.168.100.41	200.63.105.194	DNS	77	Standard query 0xe90e A public.parsec.app
48997	142.998183	200.63.105.194	192.168.100.41	DNS	109	Standard query response 0xe90e A public.parsec.app A 104.18.0.181 A 104.18.1.181

Packet 48986 details:

- Frame 48986: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF...
- Ethernet II, Src: ASRockIncorp\_6e:70:6b (a8:a1:59:6e:70:6b), Dst: 00:2e:c0:d9:6a:6e (00:2e:c0:d9:6a:6e)
- Internet Protocol Version 4, Src: 192.168.100.41, Dst: 200.63.105.194
- User Datagram Protocol, Src Port: 64386, Dst Port: 53
  - Source Port: 64386
  - Destination Port: 53
  - Length: 39
  - Checksum: 0xea0c [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 41]
  - [Timestamps]
  - UDP payload (31 bytes)
- Domain Name System (query)

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

**R:** Source port: 64386, Destination port: 53, Default DNS port number: 5

- 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
```

Output:

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
Description . . . . . : Realtek PCIe 2.5GbE Family Controller
Physical Address. . . . . : A8-A1-59-6E-70-6B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::61fb:a772:f68f:f751%14(Preferred)
IPv4 Address. . . . . : 192.168.100.41(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, May 23, 2024 8:21:37 PM
Lease Expires . . . . . : Friday, May 24, 2024 8:21:36 PM
Default Gateway . . . . . : fe80::1%14
                             192.168.100.1

DHCP Server . . . . . : 192.168.100.1
DHCPv6 IAID . . . . . : 111714649
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-9A-6C-B2-A8-A1-59-6E-70-6B
DNS Servers . . . . . : 200.63.105.194
                             45.236.107.126

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?

**R:** The Physic Address is the same that the source MAC addresses, and the IPv4 Address is the same as the source IP address.

- 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`.

The screenshot shows the Wireshark interface with a packet capture of a DNS query. The packet list pane shows a packet from 192.168.100.41 to 200.63.105.194. The packet details pane is expanded to show the Domain Name System (query) section. The Flags field shows the query is recursive (bit 0x0001). The Queries field shows a query for www.cisco.com, type A, class IN.

No.	Time	Source	Destination	Protocol	Length	Info
44816	118.355535	192.168.100.41	200.63.105.194	DNS	87	Standard query 0x0001 PTR 194.105.63.200.in-addr.arpa
44817	118.359640	200.63.105.194	192.168.100.41	DNS	132	Standard query response 0x0001 PTR 194.105.63.200.in-addr.arpa PTR host-200-63-105-194.fibramax.ec
44826	121.499599	192.168.100.41	200.63.105.194	DNS	82	Standard query 0x0919 A safebrowsing.brave.com
44827	121.499808	192.168.100.41	200.63.105.194	DNS	82	Standard query 0x8e90 HTTPS safebrowsing.brave.com
44828	121.503752	200.63.105.194	192.168.100.41	DNS	189	Standard query response 0x0919 A safebrowsing.brave.com CNAME d1bvmadhanr17qk.cloudfront.net A 18.239.22...
44829	121.504313	200.63.105.194	192.168.100.41	DNS	203	Standard query response 0x8e90 HTTPS safebrowsing.brave.com CNAME d1bvmadhanr17qk.cloudfront.net SOA ns...
48986	134.674675	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0002 A www.cisco.com

Frame 48986: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF... Ethernet II, Src: ASRockIncorp\_6e:70:6b (a8:a1:59:6e:70:6b), Dst: 00:2e:c0:d9:6a:6e (00:2e:c0:d9:6a:6e) Internet Protocol Version 4, Src: 192.168.100.41, Dst: 200.63.105.194 User Datagram Protocol, Src Port: 64386, 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 (1) (Host Address)  
 Class: IN (0x0001)  
 [Response In: 48987]

## Part 3: Explore DNS Response Traffic

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

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane shows several packets, with packet 48987 selected. The packet details pane shows the structure of the DNS response, including the transaction ID, flags, queries, and answers.

No.	Time	Source	Destination	Protocol	Length	Info
44829	121.504313	200.63.105.194	192.168.100.41	DNS	203	Standard query response 0x8e90 HTTPS safebrowsing.brave.com CNAME d1bvmahnr17qk.cloudfront.net SOA ns-...
48986	134.674675	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0002 A www.cisco.com
48987	134.678677	200.63.105.194	192.168.100.41	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edg...
48988	134.680648	192.168.100.41	200.63.105.194	DNS	73	Standard query 0x0003 AAAA www.cisco.com
48989	134.694266	200.63.105.194	192.168.100.41	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com...
48996	142.994841	192.168.100.41	200.63.105.194	DNS	77	Standard query 0xe90e A public.parsec.app
48997	142.998183	200.63.105.194	192.168.100.41	DNS	109	Standard query response 0xe90e A public.parsec.app A 104.18.0.181 A 104.18.1.181

Frame 48987: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface \Dev...  
 Ethernet II, Src: 00:2e:c0:d9:6a:6e (00:2e:c0:d9:6a:6e), Dst: ASRockIncorp\_6e:70:6b (a8:a1:59:6e:70:6b)  
 Internet Protocol Version 4, Src: 200.63.105.194, Dst: 192.168.100.41  
 User Datagram Protocol, Src Port: 53, Dst Port: 64386  
 Domain Name System (response)

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?

**R:** Destination MAC addresses: a8:a1:59:6e:70:6b Source MAC addresses: 00:2e:c0:d9:6a:6e. Source IP addresses: 200.63.105.194, Destination IP addresses: 192.168.100.41. The difference between the query and the response DNS, is that the source and the destination was swapped because our computer recipe the response packet and not send the query packet.

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

The screenshot shows the Wireshark interface with the packet details pane expanded for packet 48987. The details pane shows the structure of the DNS response, including the transaction ID, flags, queries, and answers.

Domain Name System (response)  
 Transaction ID: 0x0002  
 Flags: 0x0180 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 authentic  
 .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 (1) (Host Address)  
 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  
 wwwds.cisco.com.edgekey.net: globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net: type A, class IN, addr 92.122.89.10  
 e2867.dsca.akamaiedge.net: type A, class IN, addr 92.122.89.10  
 [Request In: 48986]  
 [Time: 0.004002000 seconds]



Can the DNS server do recursive queries?

**R:** Yes, a response can contain multiple response, in this case 5 response.

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

How do the results compare to nslookup results?

**R:** I can't understand the question.

### Reflection Question

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

I can see the DNS request on the network, like what urls are querying on my network, and what is the source IP, and I can see what is my DNS server

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

A attacker can do a dns spoofing to redirection all the dns request to a fake portal pages and get the credentials of the users or invalid the network redirection all the urls to a failed page.

**Note:** All the images was extracted of my personal computer, including wireshark screenshots and prompt screenshots. The prompt screenshot included the username: Enrique