

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.

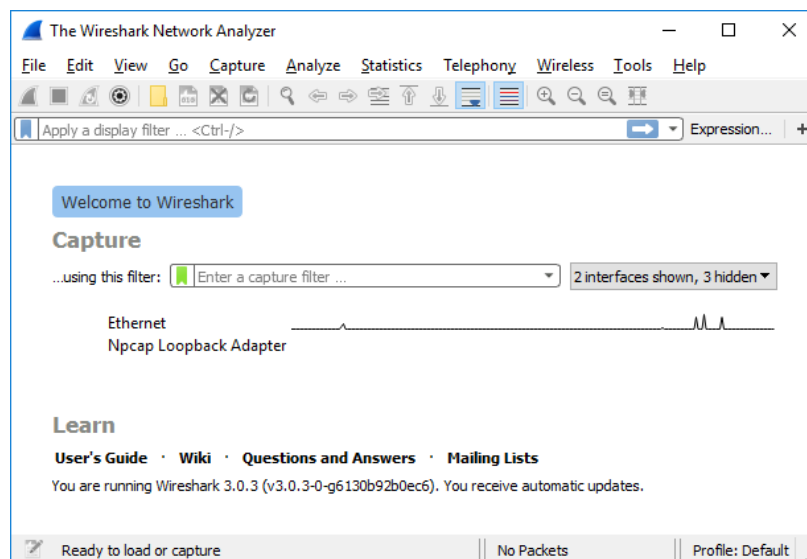
Required Resources

- 1 Windows PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS traffic.

- 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.

```
PS C:\Users\shafa> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Lab - Explore DNS Traffic

- 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.

```
PS C:\Users\shafa> 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:b000:380::b33
           2600:1413:b000:39a::b33
           184.27.28.118
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.

Part 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).

No.	Time	Source	Destination	Protocol	Length	Info
19169	136.467733	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x571b
19189	136.482228	10.0.1.50	10.69.4.163	DNS	99	Standard query response
19212	136.505183	10.0.1.50	10.69.4.163	DNS	111	Standard query response
19615	136.621969	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xd836
19616	136.622020	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xf4d9
19647	136.636781	10.0.1.50	10.69.4.163	DNS	94	Standard query response
19650	136.636781	10.0.1.50	10.69.4.163	DNS	106	Standard query response
22383	139.135737	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xcc16
22384	139.135820	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xa738
22469	139.169820	10.0.1.50	10.69.4.163	DNS	103	Standard query response
22471	139.169820	10.0.1.50	10.69.4.163	DNS	115	Standard query response
24695	146.111275	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0002
24698	146.160898	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24699	146.161571	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0003
24700	146.199842	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24701	146.200412	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0004
24702	146.233094	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24703	146.233815	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0005
24704	146.250500	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24705	146.251181	10.69.4.163	10.0.1.50	DNS	73	Standard query 0x0006
24708	146.298799	10.0.1.50	10.69.4.163	DNS	271	Standard query response

▶ Frame 24695: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{...}
 ▶ Ethernet II, Src: Intel_2d:9e:ca (f4:6d:3f:2d:9e:ca), Dst: Cisco_00:53:c3 (cc:7f:76:00:53:c3)
 ▶ Internet Protocol Version 4, Src: 10.69.4.163, Dst: 10.0.1.50
 ▶ User Datagram Protocol, Src Port: 50108, Dst Port: 53
 ▶ Domain Name System (query)

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

No.	Time	Source	Destination	Protocol	Length	Info
19169	136.467733	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x571b
19189	136.482228	10.0.1.50	10.69.4.163	DNS	99	Standard query response
19212	136.505183	10.0.1.50	10.69.4.163	DNS	111	Standard query response
19615	136.621969	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xd836
19616	136.622020	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xf4d9
19647	136.636781	10.0.1.50	10.69.4.163	DNS	94	Standard query response
19650	136.636781	10.0.1.50	10.69.4.163	DNS	106	Standard query response
22383	139.135737	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xcc16
22384	139.135820	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xa738
22469	139.169820	10.0.1.50	10.69.4.163	DNS	103	Standard query response
22471	139.169820	10.0.1.50	10.69.4.163	DNS	115	Standard query response
24695	146.111275	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0002
24698	146.160898	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24699	146.161571	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0003
24700	146.199842	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24701	146.200412	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0004
24702	146.233094	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24703	146.233815	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0005
24704	146.250500	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24705	146.251181	10.69.4.163	10.0.1.50	DNS	73	Standard query 0x0006
24708	146.298799	10.0.1.50	10.69.4.163	DNS	271	Standard query response

▶ Frame 24695: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{...}
 ▶ Ethernet II, Src: Intel_2d:9e:ca (f4:6d:3f:2d:9e:ca), Dst: Cisco_00:53:c3 (cc:7f:76:00:53:c3)
 ▶ Destination: Cisco_00:53:c3 (cc:7f:76:00:53:c3)
 ▶ Source: Intel_2d:9e:ca (f4:6d:3f:2d:9e:ca)
 Type: IPv4 (0x0800)
 [Stream index: 22]
 ▶ Internet Protocol Version 4, Src: 10.69.4.163, Dst: 10.0.1.50
 ▶ User Datagram Protocol, Src Port: 50108, Dst Port: 53
 ▶ Domain Name System (query)

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

- Source MAC Address: 08-00-27-80-91-DB (dari ipconfig /all)
- Destination MAC Address: cc-40-d0-18-a6-81 (dari arp -a untuk 192.168.1.1)
- Interface: Keduanya terkait dengan koneksi Ethernet. Source adalah MAC address dari PC (interface Ethernet), sedangkan destination adalah gateway (router).

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

No.	Time	Source	Destination	Protocol	Length	Info
19169	136.467733	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x571b A
19189	136.482228	10.0.1.50	10.69.4.163	DNS	99	Standard query response
19212	136.505183	10.0.1.50	10.69.4.163	DNS	111	Standard query response
19615	136.621969	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xd836 A
19616	136.622020	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xf4d9 A
19647	136.636781	10.0.1.50	10.69.4.163	DNS	94	Standard query response
19650	136.636781	10.0.1.50	10.69.4.163	DNS	106	Standard query response
22383	139.135737	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xcc16 A
22384	139.135820	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xa738 A
22469	139.169820	10.0.1.50	10.69.4.163	DNS	103	Standard query response
22471	139.169820	10.0.1.50	10.69.4.163	DNS	115	Standard query response
24695	146.111275	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x002 A
24698	146.160898	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24699	146.161571	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0003 A
24700	146.199842	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24701	146.200412	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0004 A
24702	146.233094	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24703	146.233815	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0005 A
24704	146.250500	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24705	146.251181	10.69.4.163	10.0.1.50	DNS	73	Standard query 0x0006 A
24708	146.298799	10.0.1.50	10.69.4.163	DNS	271	Standard query response

```

> Frame 24695: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: Intel_2d:9e:ca (f4:6d:3f:2d:9e:ca), Dst: Cisco_00:53:c3 (cc:7f:76:00:53:c3)
> Internet Protocol Version 4, Src: 10.69.4.163, Dst: 10.0.1.50
  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 69
    Identification: 0xed81 (60801)
  > 0000 .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.69.4.163
    Destination Address: 10.0.1.50
    [Stream index: 30]
  > User Datagram Protocol, Src Port: 50108, Dst Port: 53
  > Domain Name System (query)
  
```

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

- Source IP Address: 192.168.1.10
- Destination IP Address: 192.168.1.1
- Interface: Source IP adalah dari PC lokal

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

No.	Time	Source	Destination	Protocol	Length	Info
19169	136.467733	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x571b A
19189	136.482228	10.0.1.50	10.69.4.163	DNS	99	Standard query response
19212	136.505183	10.0.1.50	10.69.4.163	DNS	111	Standard query response
19615	136.621969	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xd836 A
19616	136.622020	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xf4d9 A
19647	136.636781	10.0.1.50	10.69.4.163	DNS	94	Standard query response
19650	136.636781	10.0.1.50	10.69.4.163	DNS	106	Standard query response
22383	139.135737	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xcc16 A
22384	139.135820	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xa738 A
22469	139.169820	10.0.1.50	10.69.4.163	DNS	103	Standard query response
22471	139.169820	10.0.1.50	10.69.4.163	DNS	115	Standard query response
24695	146.111275	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x002 A
24698	146.160898	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24699	146.161571	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0003 A
24700	146.199842	10.0.1.50	10.69.4.163	DNS	136	Standard query response
24701	146.200412	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0004 A
24702	146.233094	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24703	146.233815	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0005 A
24704	146.250500	10.0.1.50	10.69.4.163	DNS	147	Standard query response
24705	146.251181	10.69.4.163	10.0.1.50	DNS	73	Standard query 0x0006 A
24708	146.298799	10.0.1.50	10.69.4.163	DNS	271	Standard query response

```

> Frame 24695: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: Intel_2d:9e:ca (f4:6d:3f:2d:9e:ca), Dst: Cisco_00:53:c3 (cc:7f:76:00:53:c3)
> Internet Protocol Version 4, Src: 10.69.4.163, Dst: 10.0.1.50
> User Datagram Protocol, Src Port: 50108, Dst Port: 53
  Source Port: 50108
  Destination Port: 53
  Length: 49
  Checksum: 0x1a5c [unverified]
  [Checksum Status: Unverified]
  [Stream index: 476]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (41 bytes)
  > Domain Name System (query)
  
```

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

- Source Port: 50108
- Destination Port: 53
- Default DNS Port: 53

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

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

Interface: 10.69.4.163 --- 0xb
Internet Address      Physical Address      Type
10.69.0.1             cc-7f-76-00-53-c3    dynamic
10.69.0.19            74-4c-a1-9b-73-8d    dynamic
10.69.0.63            f4-a4-75-f6-9c-cb    dynamic
10.69.0.126           a0-59-50-38-38-ad    dynamic
10.69.0.184           84-14-4d-d4-0a-d0    dynamic
10.69.1.116           f4-c8-8a-3a-e1-fc    dynamic
10.69.1.160           28-d0-43-09-f0-b8    dynamic
10.69.2.11            b8-9a-2a-47-83-03    dynamic
10.69.2.239           a4-36-c7-57-b6-88    dynamic
10.69.3.3             a8-41-f4-62-e1-a2    dynamic
10.69.3.12            d8-80-83-5f-62-ef    dynamic
10.69.3.134           c0-35-32-75-f0-19    dynamic
10.69.3.153           30-05-05-ac-52-a1    dynamic
10.69.3.183           14-13-33-38-b6-81    dynamic
10.69.3.199           f4-c8-8a-3b-22-f7    dynamic
10.69.4.5             64-bc-58-86-45-b6    dynamic
10.69.4.50            10-68-38-ad-85-bb    dynamic
10.69.4.74            a6-7e-c6-70-4a-be    dynamic
10.69.4.114           84-7b-57-c0-e9-b4    dynamic
10.69.4.130           94-bb-43-de-8b-02    dynamic
10.69.4.198           8c-b8-7e-6f-b2-56    dynamic
10.69.4.252           f4-c8-8a-53-b1-8c    dynamic
10.69.5.7             28-d0-43-5e-88-84    dynamic
10.69.5.164           04-ec-d8-85-14-a7    dynamic
10.69.5.166           50-84-92-82-c5-ee    dynamic
10.69.6.161           c0-a5-e8-3b-1b-cc    dynamic
10.69.7.77            80-32-53-a5-77-8d    dynamic
10.69.7.179           2c-3b-70-dc-61-09    dynamic
10.69.7.216           1c-ce-51-c7-6a-1f    dynamic
10.69.7.255           ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    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
```

Lab - Explore DNS Traffic

```
Command Prompt
DNS Suffix Search List. . . . . : umy.ac.id

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : F4-6D-3F-2D-9E-CB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : F6-6D-3F-2D-9E-CA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

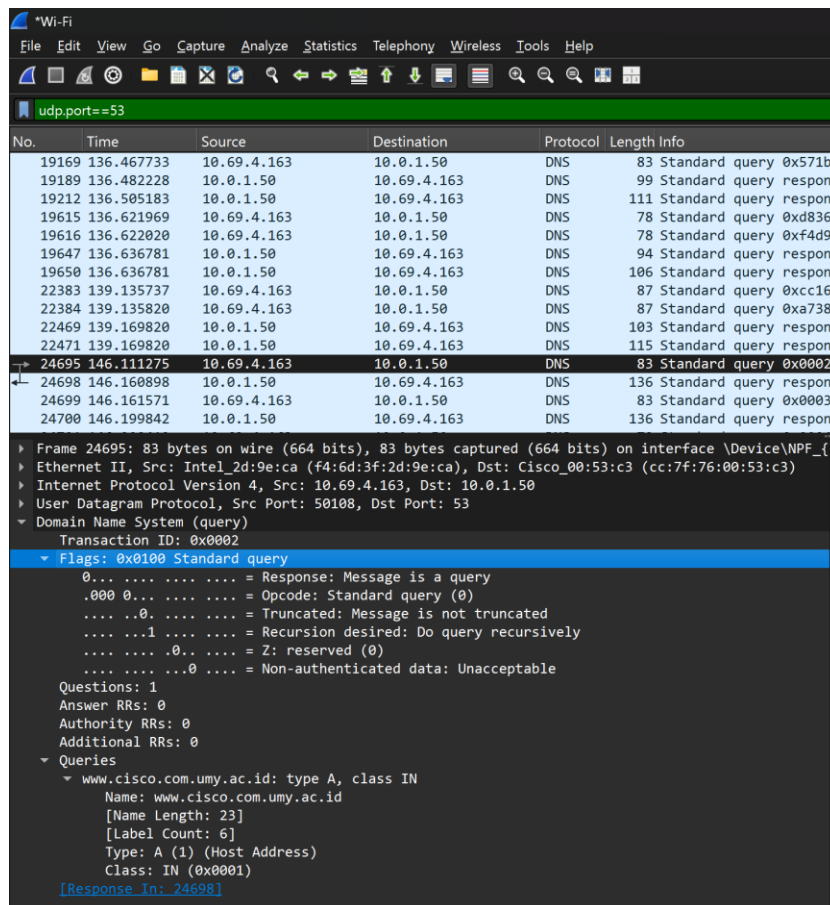
Connection-specific DNS Suffix . : umy.ac.id
Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . : F4-6D-3F-2D-9E-CA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2405:5fc0:7:1:370e:5a19:3fa9:24e6(Preferred)
Temporary IPv6 Address. . . . . : 2405:5fc0:7:1:bdca:60f5:7d11:bdf1(Preferred)
Link-local IPv6 Address . . . . : fe80::471d:7711:142:1aae%11(Preferred)
IPv4 Address. . . . . : 10.69.4.163(Preferred)
Subnet Mask . . . . . : 255.255.248.0
Lease Obtained. . . . . : Wednesday, April 23, 2025 1:24:07 PM
Lease Expires . . . . . : Wednesday, April 23, 2025 2:35:50 PM
Default Gateway . . . . . : fe80::ce7f:76ff:fe00:53c3%11
                          10.69.0.1
DHCP Server . . . . . : 10.0.1.51
DHCPv6 IAID . . . . . : 99904831
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-BA-2D-19-F4-6D-3F-2D-9E-CA
DNS Servers . . . . . : 10.0.1.50
                          10.0.4.50
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?

MAC dan IP address yang terlihat di Wireshark konsisten dengan informasi dari ipconfig /all dan arp - a, yang menunjukkan bahwa paket DNS query berasal dari PC lokal dan dikirim ke router sebagai DNS resolver.

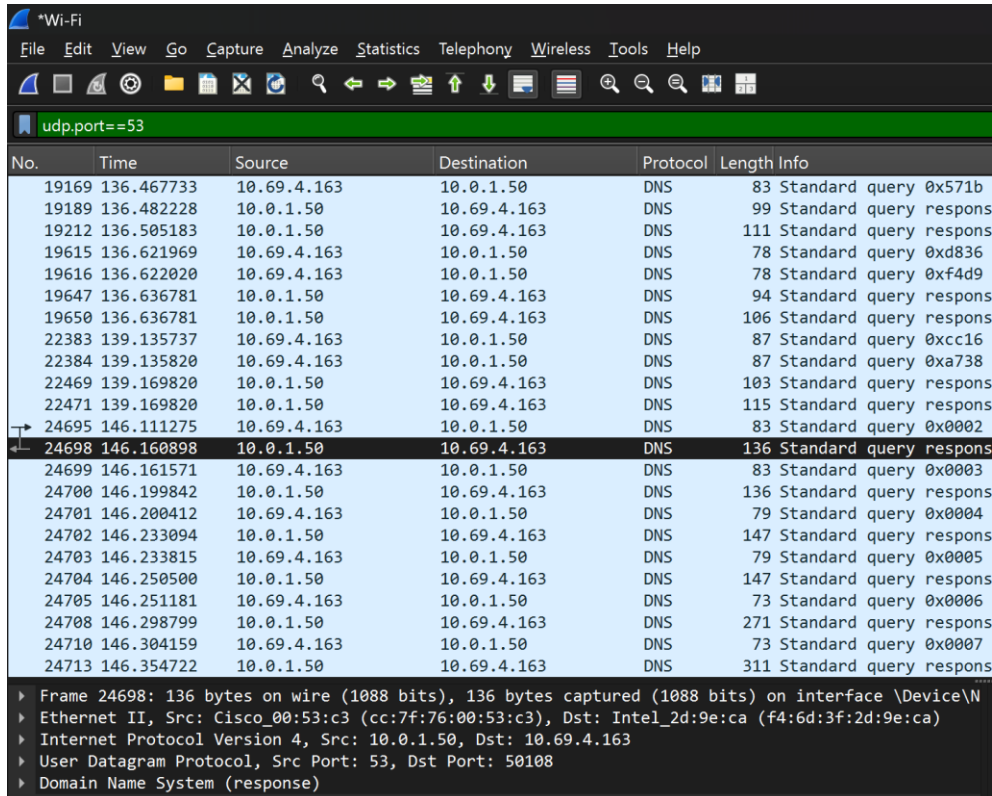
- 3) Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.

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



Part 3: Explore DNS Response Traffic

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



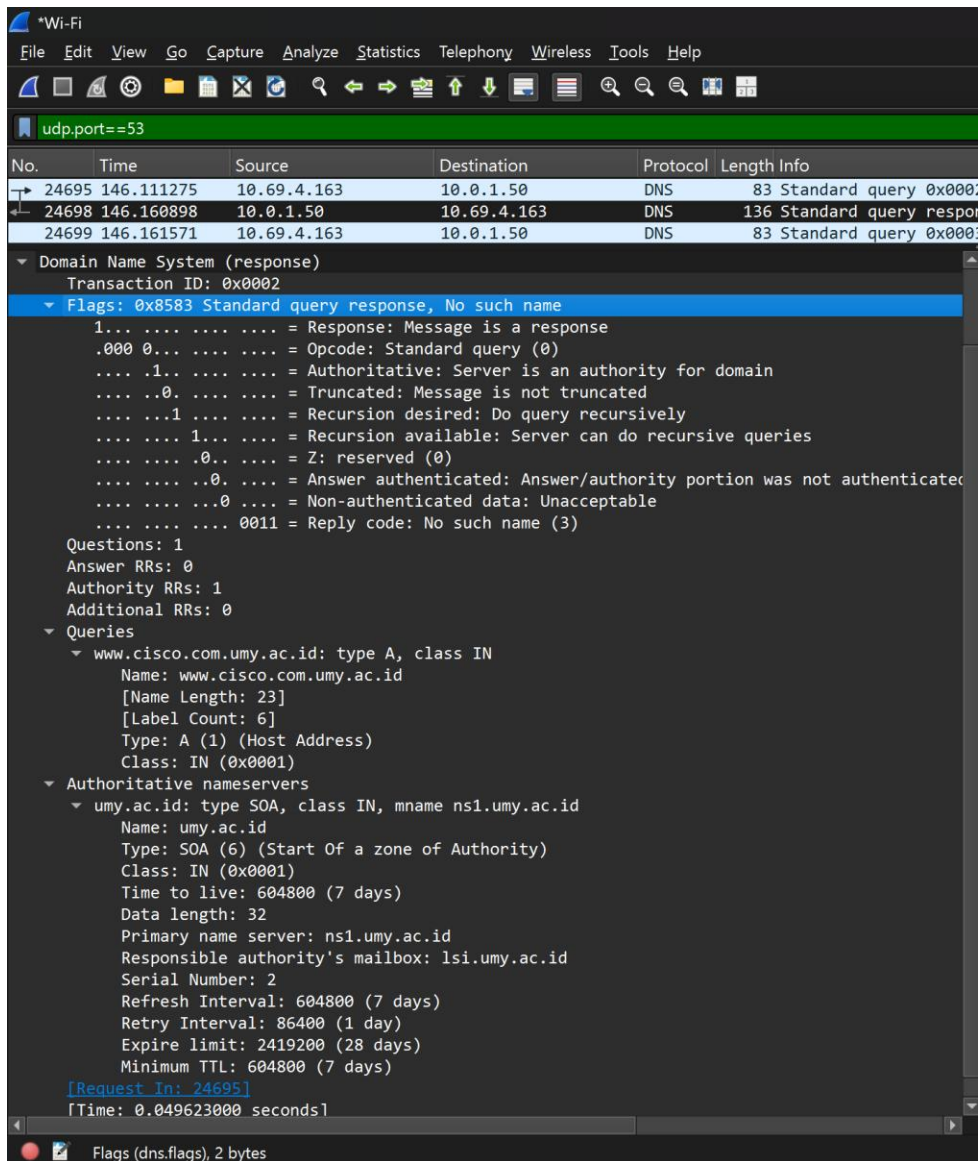
No.	Time	Source	Destination	Protocol	Length	Info
19169	136.467733	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x571b
19189	136.482228	10.0.1.50	10.69.4.163	DNS	99	Standard query respons
19212	136.505183	10.0.1.50	10.69.4.163	DNS	111	Standard query respons
19615	136.621969	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xd836
19616	136.622020	10.69.4.163	10.0.1.50	DNS	78	Standard query 0xf4d9
19647	136.636781	10.0.1.50	10.69.4.163	DNS	94	Standard query respons
19650	136.636781	10.0.1.50	10.69.4.163	DNS	106	Standard query respons
22383	139.135737	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xcc16
22384	139.135820	10.69.4.163	10.0.1.50	DNS	87	Standard query 0xa738
22469	139.169820	10.0.1.50	10.69.4.163	DNS	103	Standard query respons
22471	139.169820	10.0.1.50	10.69.4.163	DNS	115	Standard query respons
24695	146.111275	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0002
24698	146.160898	10.0.1.50	10.69.4.163	DNS	136	Standard query respons
24699	146.161571	10.69.4.163	10.0.1.50	DNS	83	Standard query 0x0003
24700	146.199842	10.0.1.50	10.69.4.163	DNS	136	Standard query respons
24701	146.200412	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0004
24702	146.233094	10.0.1.50	10.69.4.163	DNS	147	Standard query respons
24703	146.233815	10.69.4.163	10.0.1.50	DNS	79	Standard query 0x0005
24704	146.250500	10.0.1.50	10.69.4.163	DNS	147	Standard query respons
24705	146.251181	10.69.4.163	10.0.1.50	DNS	73	Standard query 0x0006
24708	146.298799	10.0.1.50	10.69.4.163	DNS	271	Standard query respons
24710	146.304159	10.69.4.163	10.0.1.50	DNS	73	Standard query 0x0007
24713	146.354722	10.0.1.50	10.69.4.163	DNS	311	Standard query respons

▶ Frame 24698: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \Device\N
 ▶ Ethernet II, Src: Cisco_00:53:c3 (cc:7f:76:00:53:c3), Dst: Intel_2d:9e:ca (f4:6d:3f:2d:9e:ca)
 ▶ Internet Protocol Version 4, Src: 10.0.1.50, Dst: 10.69.4.163
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 50108
 ▶ 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?

- Source MAC Address: cc-40-d0-18-a6-81
- Destination MAC Address: 08-00-27-80-91-DB
- Source IP Address: 192.168.1.1
- Destination IP Address: 192.168.1.10
- Source Port: 53
- Destination Port: Port acak yang sama seperti digunakan pada query awal

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



Can the DNS server do recursive queries?

Ya. Hal ini dapat dilihat dari *Flags* dalam DNS response yang menunjukkan bahwa query dilakukan secara recursive dan berhasil mendapatkan jawaban akhir.

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

How do the results compare to nslookup results?

Hasil di Wireshark sama dengan hasil dari nslookup. Ada beberapa CNAME yang menunjukkan bahwa www.cisco.com merupakan alias dari beberapa nama domain lainnya, hingga akhirnya menghasilkan satu

Lab - Explore DNS Traffic

atau beberapa Alamat IP.

Reflection Question

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

Tanpa filter, dapat melihat seluruh lalu lintas jaringan, termasuk protocol lain seperti TCP, HTTP, ARP, DHCP, komunikasi antar perangkat di jaringan lokal, Alamat IP dan MAC dari perangkat lain, server DNS yang digunakan, serta potensi masalah seperti paket yang gagal dikirim atau duplikat

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

Seorang penyerang dapat menggunakan Wireshark untuk menangkap kredensial jika transmisi tidak dienkripsi, menganalisis struktur jaringan beserta IP, MAC, dan perangkat aktif, mengidentifikasi layanan yang berjalan untuk mengeksploitasi celah, Menyusun serangan man-in-the-middle (MITM), serta melakukan DNS spoofing dengan memanfaatkan informasi dari query asli.