

Lab - Exploring 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 and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Required Resources

- 1 PC with internet access and Wireshark installed

Instructions

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

- a. Download the latest stable version of Wireshark from www.wireshark.org. Choose the software version you need based on your PC's architecture and operating system.
- b. Follow the on-screen instructions to install Wireshark. If you are prompted to install USBPcap, **do NOT** install USBPcap for normal traffic capture. USBPcap is experimental, and it could cause USB problems on your PC.

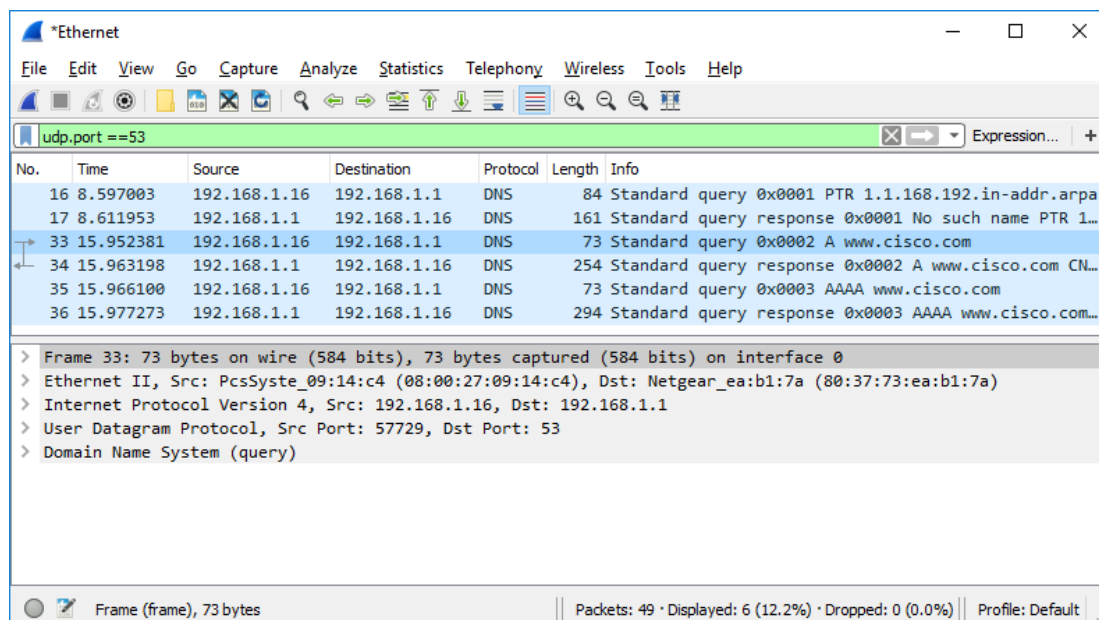
Step 2: Capture DNS traffic.

- a. Start Wireshark. Select an active interface with traffic for packet capture.
- b. Clear the DNS cache.
 - 1) In Windows, enter **ipconfig /flushdns** in Command Prompt.
 - 2) For the majority of Linux distributions, one of the following utilities is used for DNS caching: Systemd - Resolved, DNSMasq, and NSCD. If your Linux distribution does not use one of the listed utilities, please perform an internet search for the DNS caching utility for your Linux distribution.
 - (i) Identify the utility used in your Linux distribution by checking the status:
Systemd-Resolved: **systemctl status systemd-resolved.service**
DNSMasq: **systemctl status dnsmasq.service**
NSCD: **systemctl status nscd.service**

- (ii) If you are using system-resolved, enter **systemd-resolve --flush-caches** to flush the cache for Systemd-Resolved before restarting the service. The following commands restart the associated service using elevated privileges:
 - Systemd-Resolved: **sudo systemctl restart systemd-resolved.service**
 - DNSMasq: **sudo systemctl restart dnsmasq.service**
 - NSCD: **sudo systemctl restart nscd.service**
- 3) For the macOS, enter **sudo killall -HUP mDNSResponder** to clear the DNS cache in the Terminal. Perform an internet search for the commands to clear the DNS cache for an older OS.
- c. At a command prompt or terminal, type **nslookup** enter the interactive mode.
- d. Enter the domain name of a website. The domain name www.cisco.com is used in this example.
- e. Type **exit** when finished. 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. **Note:** The provided screenshots are just examples. Your output may be slightly different.



- b. Select the DNS packet contains **Standard query** and **A www.cisco.com** in the Info column.
- c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

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

The screenshot shows the Wireshark interface with a packet capture filter of `udp.port == 53`. The packet list displays several DNS packets. Packet 33 is selected, and its details are expanded, showing the Ethernet II header with source MAC `PcsSyste_09:14:c4` and destination MAC `Netgear_ea:b1:7a`.

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

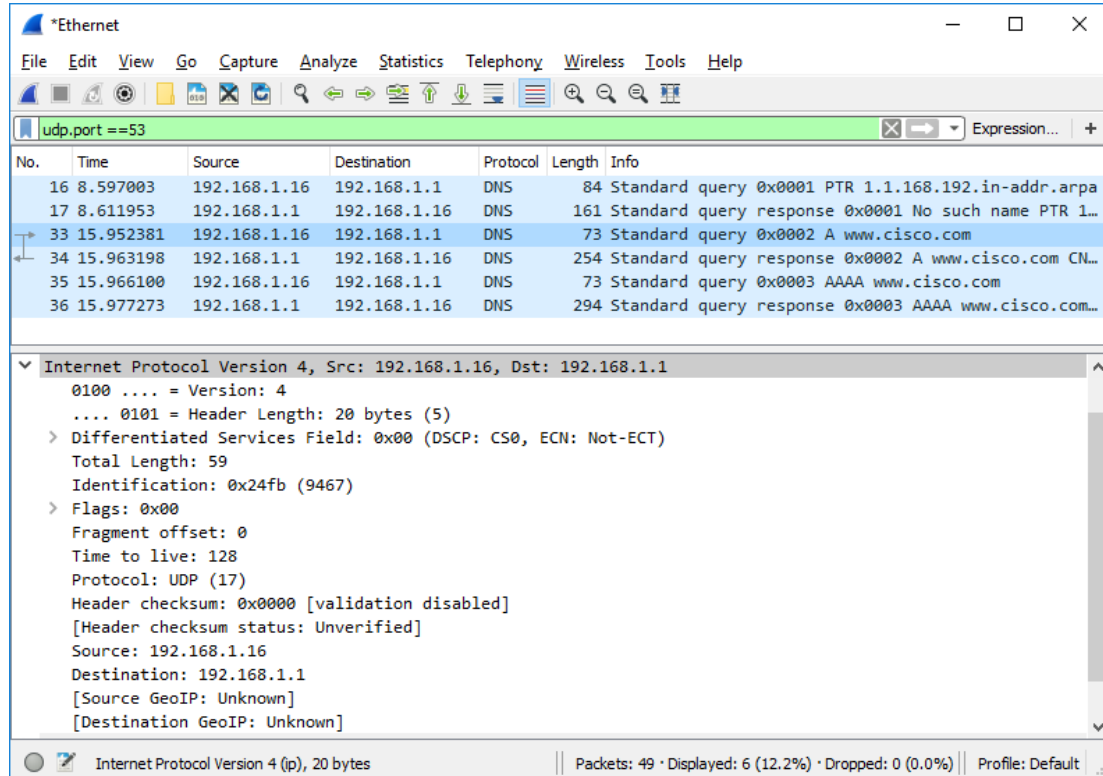
- Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Source: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
 - Address: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 57729, Dst Port: 53
- Domain Name System (query)

Frame (frame), 73 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

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

Answer: 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.

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



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane at the top shows a list of captured packets. The filter bar at the top of the packet list contains the expression 'udp.port == 53'. The packet list shows several DNS packets. The packet details pane for the selected packet (No. 33) is expanded, showing the Internet Protocol Version 4 header. The source IP address is 192.168.1.16 and the destination IP address is 192.168.1.1. The status bar at the bottom indicates that 49 packets are displayed, 6 (12.2%) are shown, and 0 (0.0%) are dropped.

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 59
- Identification: 0x24fb (9467)
- > Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: UDP (17)
- Header checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.16
- Destination: 192.168.1.1
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

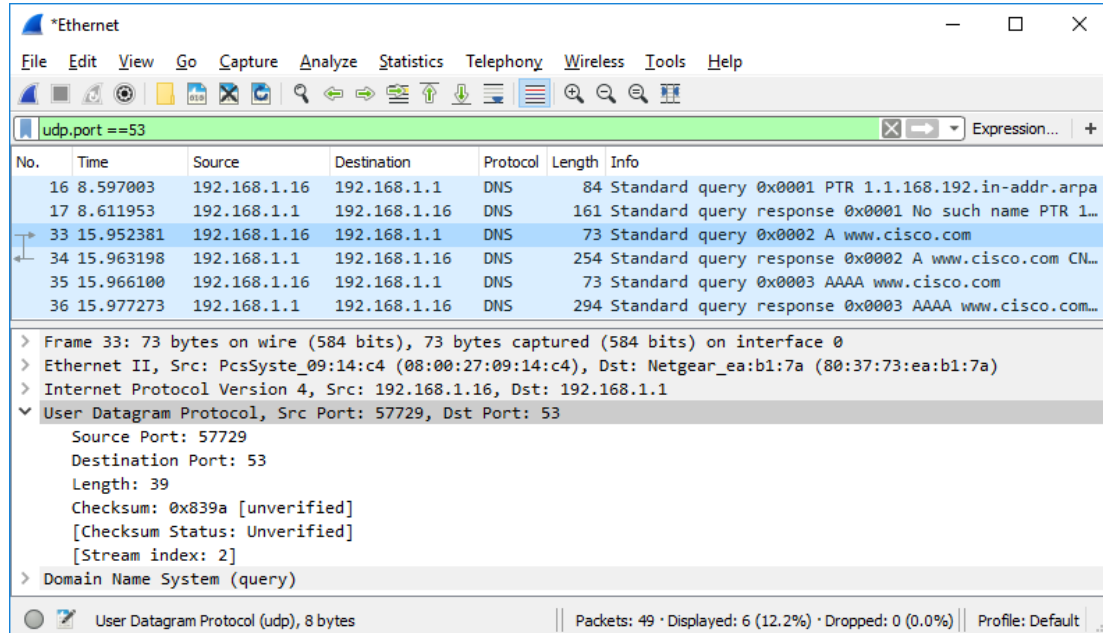
Internet Protocol Version 4 (p), 20 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Question:

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

Answer: The source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

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



Question:

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

Answer: The source port number is 577729 and the destination port is 53, which is the default DNS port number.

- g. Determine the IP and MAC address of the PC.

- 1) In a Windows command prompt, enter **arp -a** and **ipconfig /all** to record the MAC and IP addresses of the PC.
- 2) For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

Question:

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

Answer: The IP and MAC addresses captured in the Wireshark results are the same as the addresses listed in **ipconfig /all** command.

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

Lab - Exploring DNS Traffic

- i. 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 a Wireshark packet capture window titled "*Ethernet". The filter bar at the top is set to "udp.port == 53". The packet list shows several DNS packets. Packet 33 is a standard query for "www.cisco.com" (type A, class IN) with transaction ID 0x0002. Packet 34 is the corresponding response, showing the IP address 192.168.1.16.

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

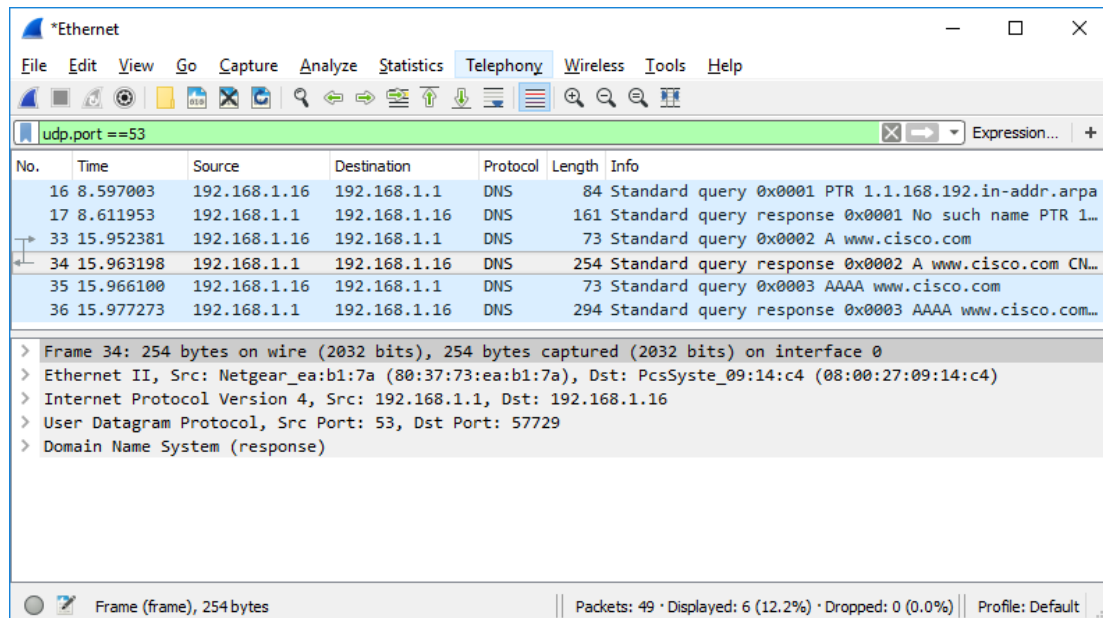
The packet details pane for packet 34 shows the following structure:

- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 57729, Dst Port: 53
- Domain Name System (query)
 - [Response In: 34]
 - 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)

The status bar at the bottom indicates: Domain Name System (dns), 31 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Part 3: Explore DNS Response Traffic

- Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.



Question:

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?

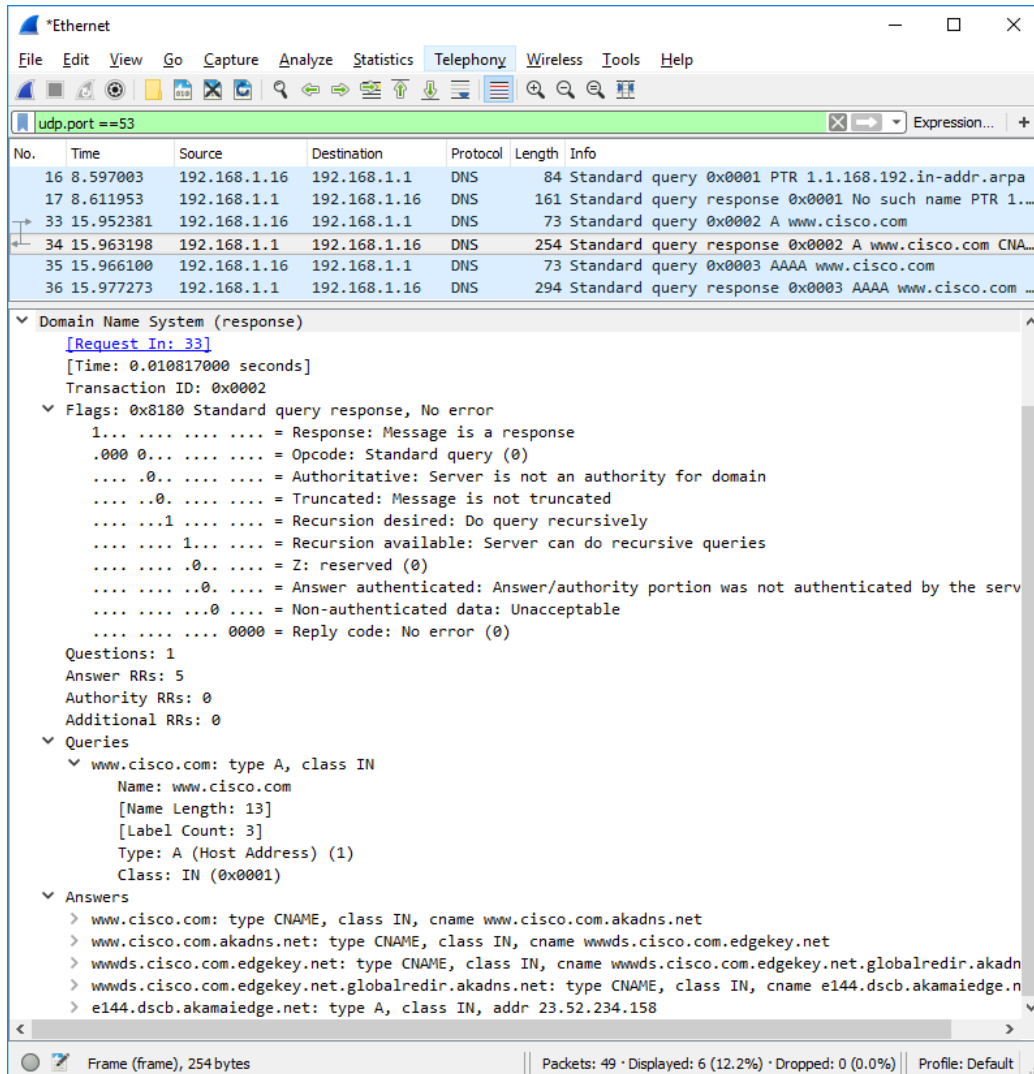
Answer: The source IP, MAC address, and port number in the query packet are now destination addresses. The destination IP, MAC address, and port number in the query packet are now source addresses.

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

Question:

Can the DNS server do recursive queries?

Answer: Yes, the DNS can handle recursive queries.



- d. Observe the CNAME and A records in the Answers details.

Question:

How do the results compare to nslookup results?

Answer: The results in the Wireshark should be the same as the results from nslookup in the Command Prompt or terminal.

Reflection

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

Answer: 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?

Answer: 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.

End of document