

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

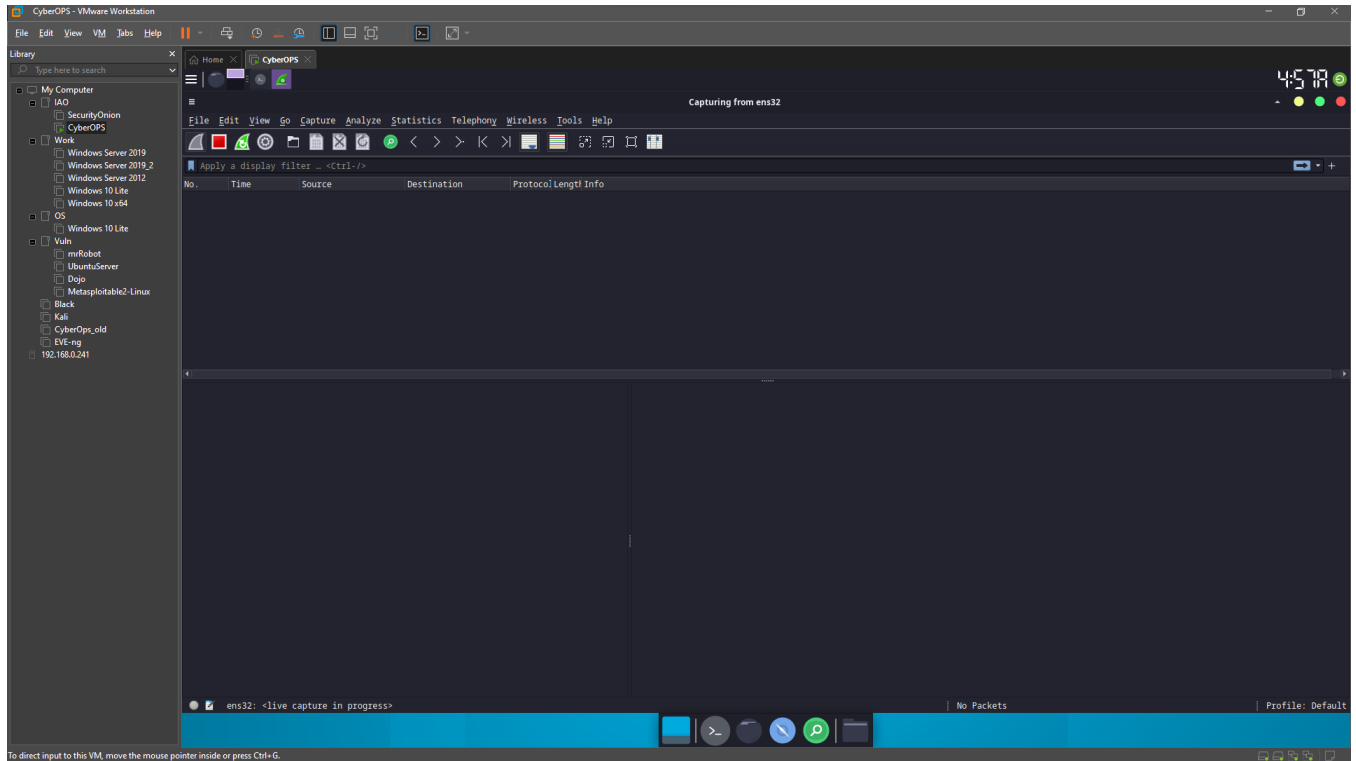
Step 1: Download and install Wireshark.

- 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.

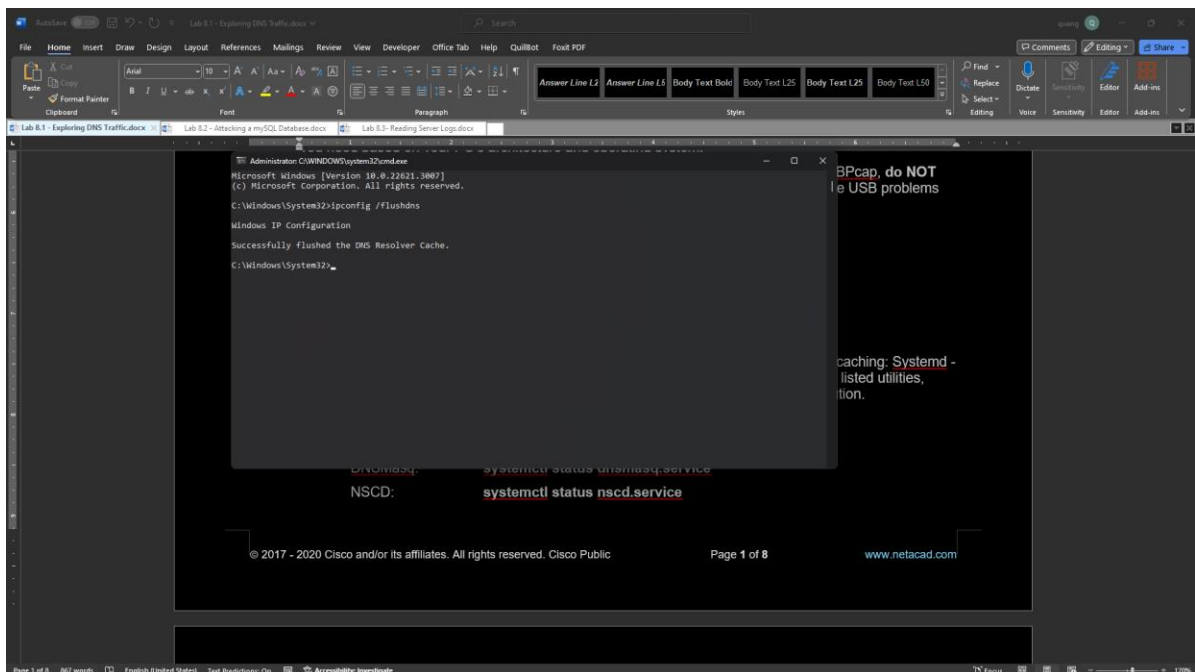
- a. Start Wireshark. Select an active interface with traffic for packet capture.

Lab - Exploring DNS Traffic



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**

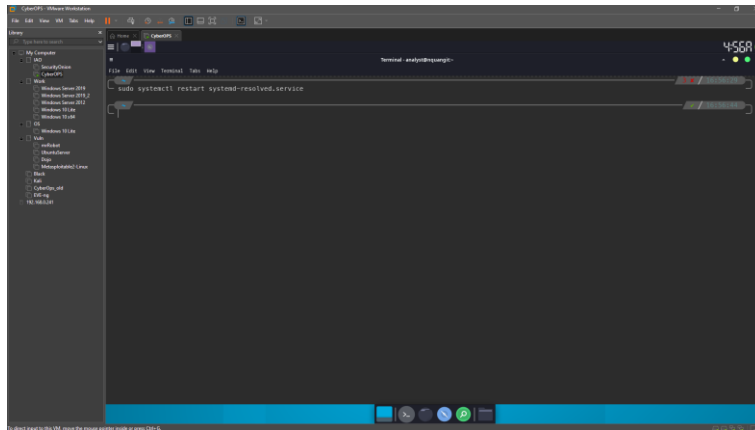
NSCD: **systemctl status nscd.service**

- (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**

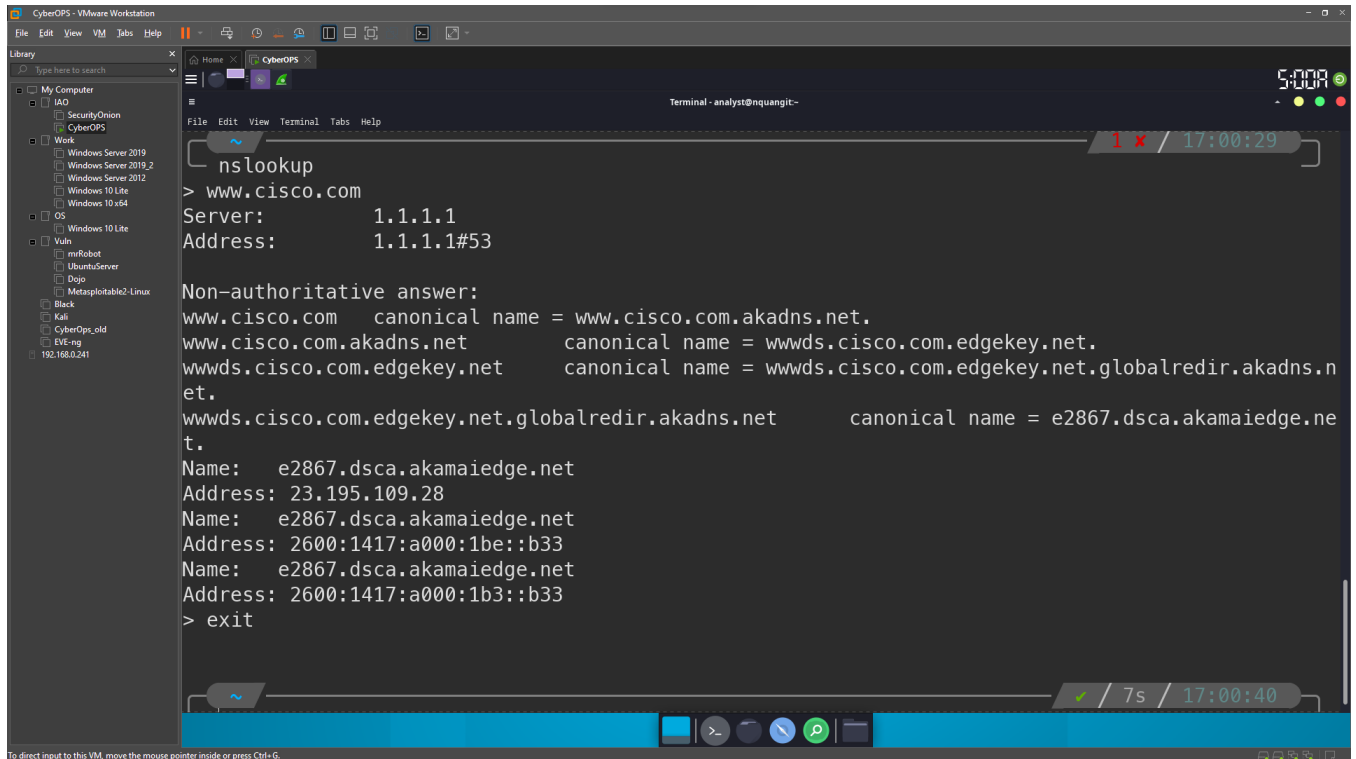
DNSMasq: **sudo systemctl restart dnsmasq.service**

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.

Lab - Exploring DNS Traffic



The screenshot shows a VMware Workstation window titled 'CyberOps - VMware Workstation'. On the left is a 'Library' pane with a tree view containing 'My Computer', 'IAO', 'SecurityOnion', 'CyberOps', 'Work', 'Windows Server 2019', 'Windows Server 2019.2', 'Windows Server 2012', 'Windows 10 Lite', 'Windows 10 x64', 'OS', 'Windows 10 Lite', 'Vuln', 'miRobot', 'UbuntuServer', 'Dogs', 'Metasploitab2-Linux', 'Black', 'Kali', 'CyberOps_old', 'EVE-ng', and '192.168.0.241'. The main area is a terminal window titled 'Terminal - analyst@nquangit-'. It shows the command 'nslookup' and its output for 'www.cisco.com'. The output includes the server address (1.1.1.1), a non-authoritative answer with canonical names, and IP addresses for the final domain.

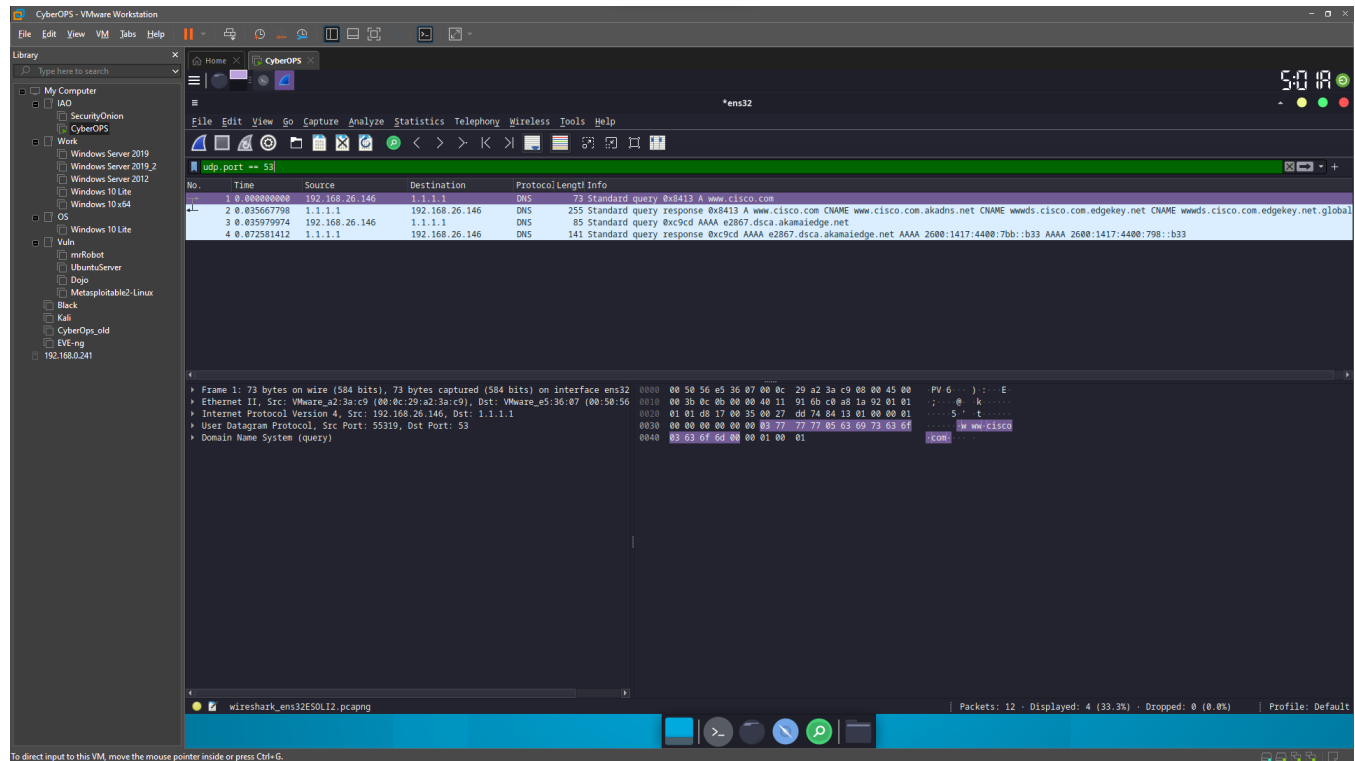
```
nslookup
> www.cisco.com
Server:          1.1.1.1
Address:         1.1.1.1#53

Non-authoritative answer:
www.cisco.com    canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net    canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net    canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net    canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 23.195.109.28
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1417:a000:1be::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1417:a000:1b3::b33
> exit
```

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

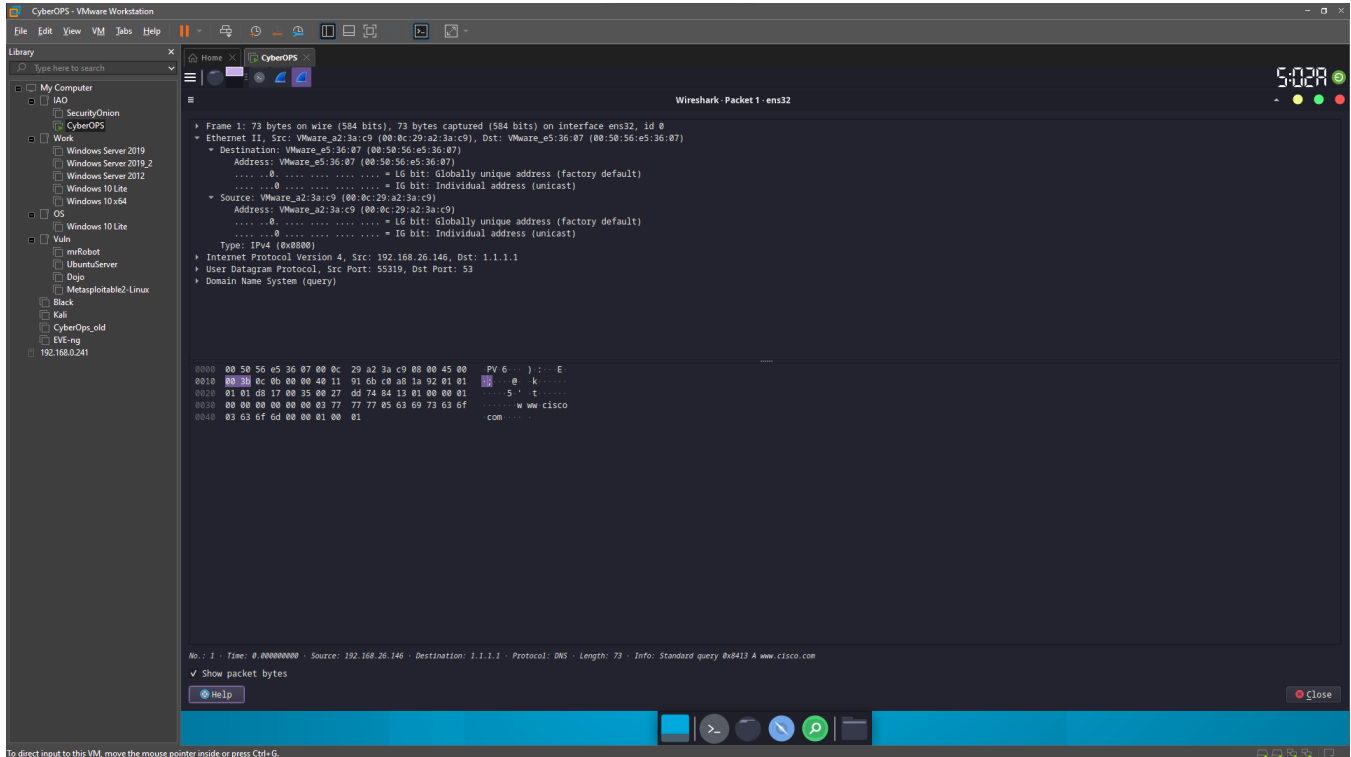
Part 2: Explore DNS Query Traffic

- 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. **Note:** The provided screenshots are just examples. Your output maybe slightly different.



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



Lab - Exploring DNS Traffic

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

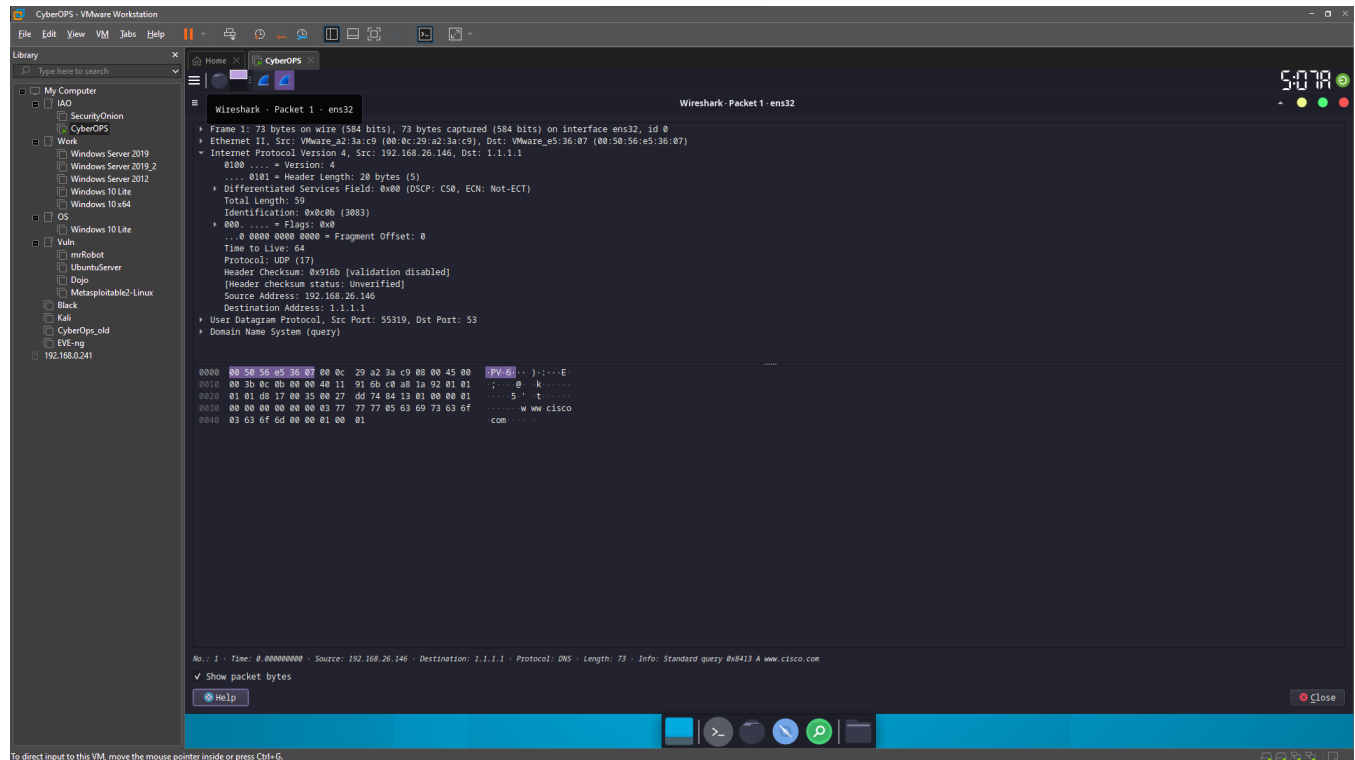
Source MAC: 00:0c:29:a2:3a:c9

Dest MAC: 00:50:56:e5:36:07

Source MAC is current device NIC

Dest MAC is the default gateway NIC

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



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

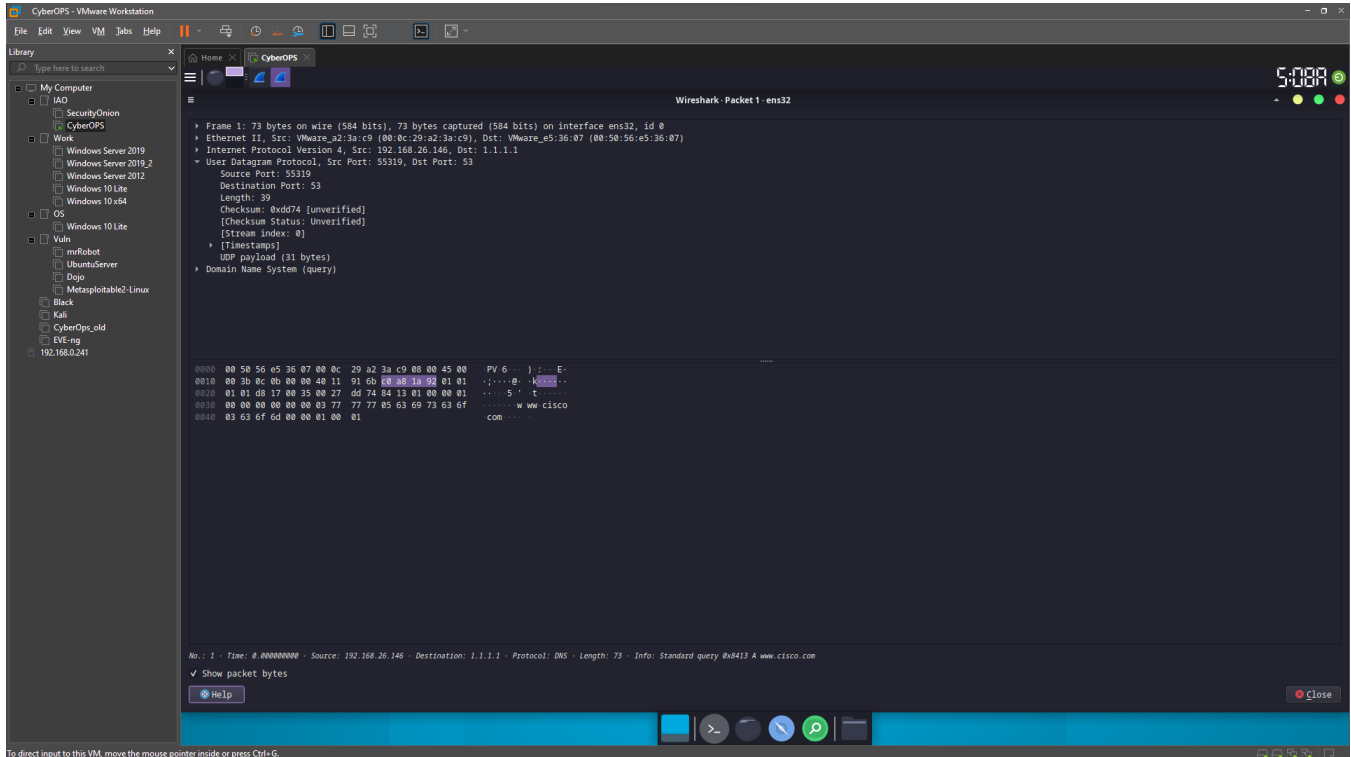
Source IP: 192.168.26.146

Dest IP: 1.1.1.1

Source IP is the current device's IP.

Dest IP is the DNS server's IP.

- 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?

Source port: 55319

Dest port: 53

Default DNS port number is 53

- 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.

Lab - Exploring DNS Traffic

```
Windows PowerShell
Physical Address. . . . . : 00-50-56-C0-00-01
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.239.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, January 27, 2024 08:22:21 PM
Lease Expires . . . . . : Saturday, January 27, 2024 10:25:40 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.239.254
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Physical Address. . . . . : 00-50-56-C0-00-08
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.26.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, January 27, 2024 08:22:24 PM
Lease Expires . . . . . : Saturday, January 27, 2024 10:25:40 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.26.254
Primary WINS Server . . . . . : 192.168.26.2
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet2:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet2
Physical Address. . . . . : 00-50-56-C0-00-02
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::742d:8307:e94c:1125%26(Preferred)
IPv4 Address. . . . . : 192.168.13.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 1358975062
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-56-5A-F9-58-11-22-85-6D-09
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet13:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet13
Physical Address. . . . . : 00-50-56-C0-00-0D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c9cf:4232:cha2:2e8f%4(Preferred)
IPv4 Address. . . . . : 192.168.75.1(Preferred)
```

2) For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

```
CyberOps - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
  IAG
  Security Onion
  CyberOps
Work
  Windows Server 2019
  Windows Server 2019.2
  Windows Server 2015
  Windows 10 Lite
  Windows 10 x64
OS
  Windows 10 Lite
Vuln
  mifcobot
  Ubuntu Server
  Digo
  Metasploitable2-Linux
  Kali
  CyberOps-old
  EVE-ng
  NSL168.241

Terminal - analyst@nquangit~
File Edit View Terminal Tabs Help
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/ether 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:a2:3a:c9 brd ff:ff:ff:ff:ff:ff
   altname enp2s0
   inet 192.168.26.146/24 brd 192.168.26.255 scope global ens32
       valid_lft forever preferred_lft forever
   inet6 fe80::20c:29ff:fea2:3ac9/64 scope link proto kernel ll
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether 00:0c:29:a2:3a:d3 brd ff:ff:ff:ff:ff:ff
   altname enp2s2
```

Question:

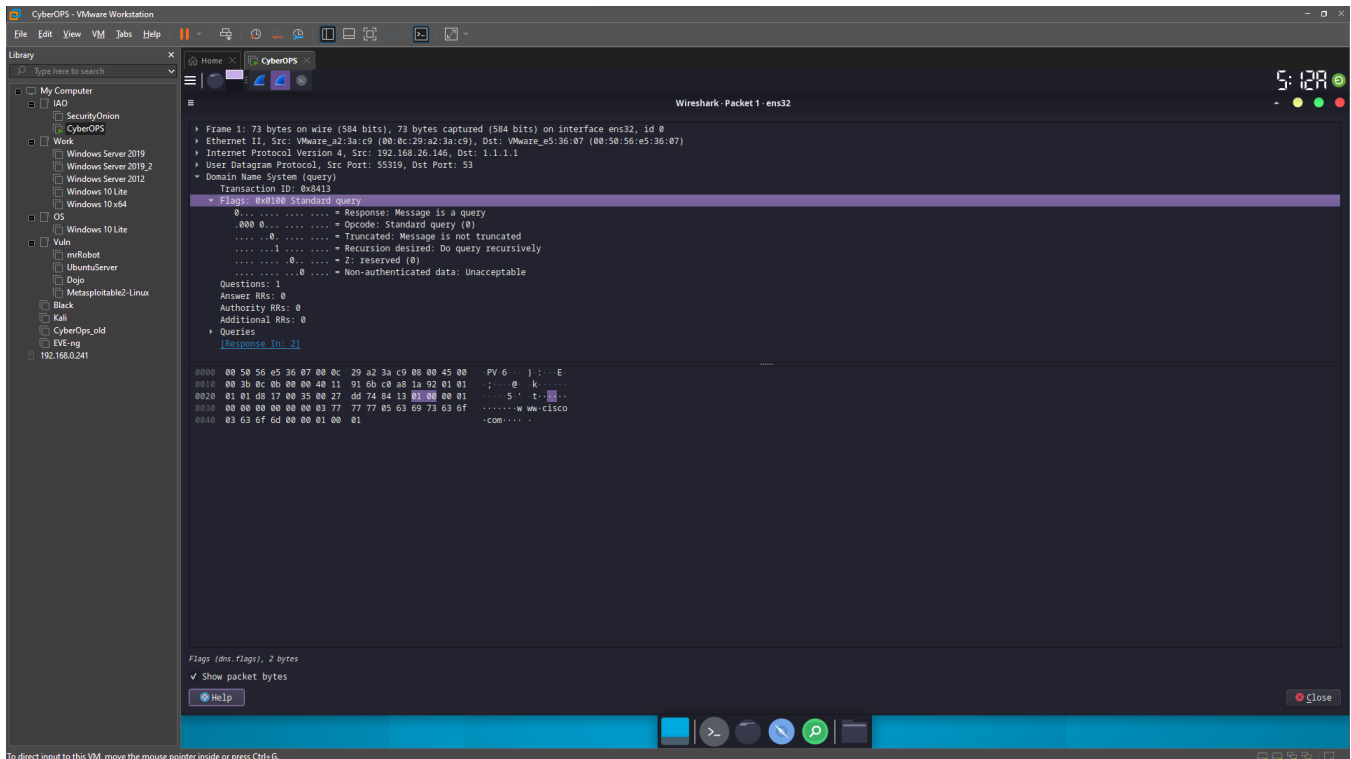
Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

The MAC and IP addresses in the Wireshark result are the same as the addresses in ip address command result

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

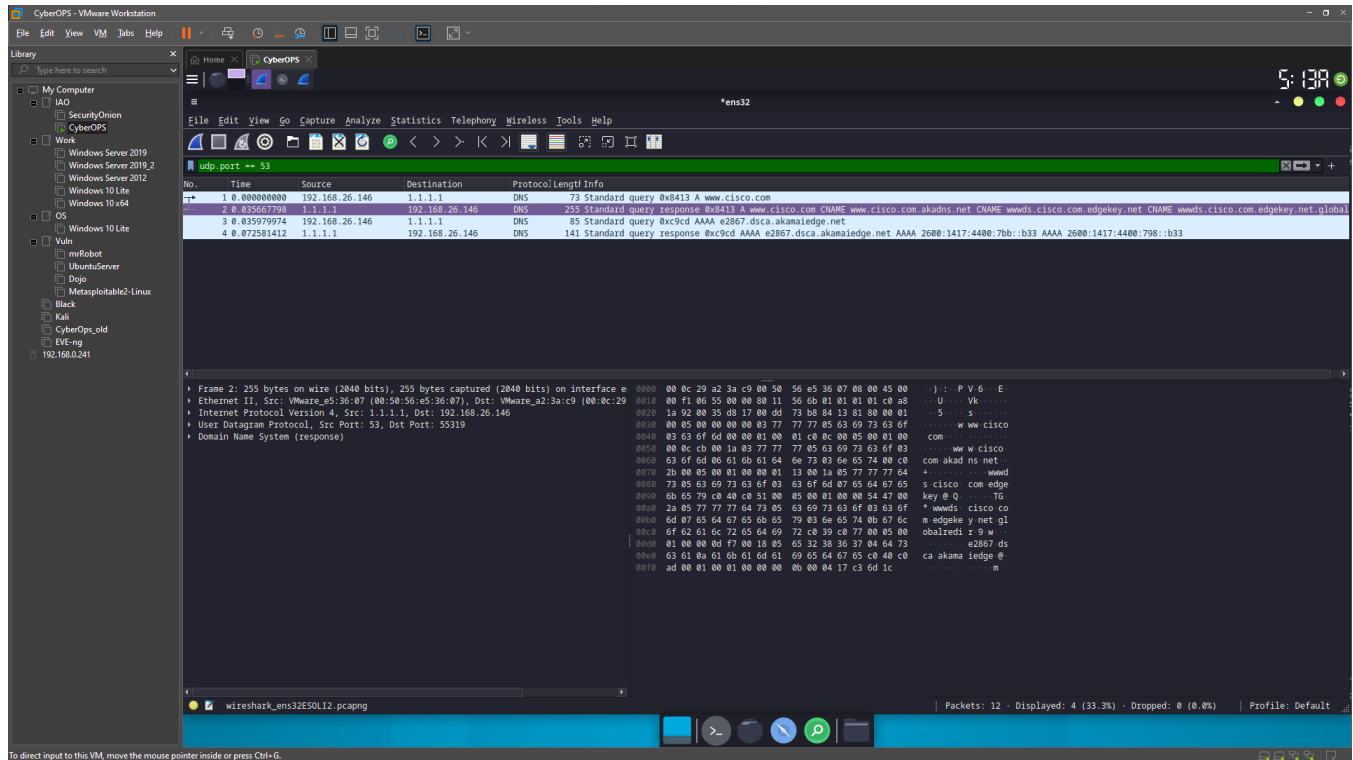
Lab - Exploring DNS Traffic

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



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.



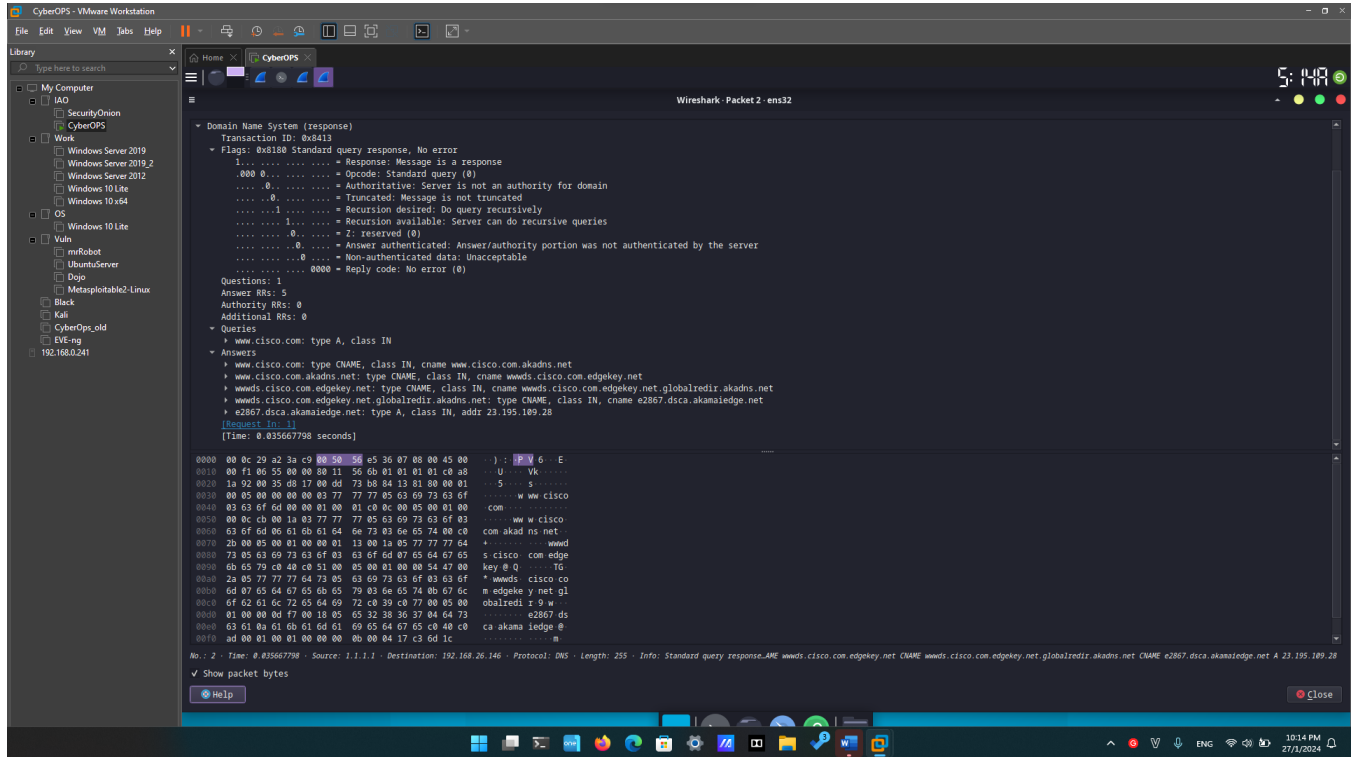
Question:

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?

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**.

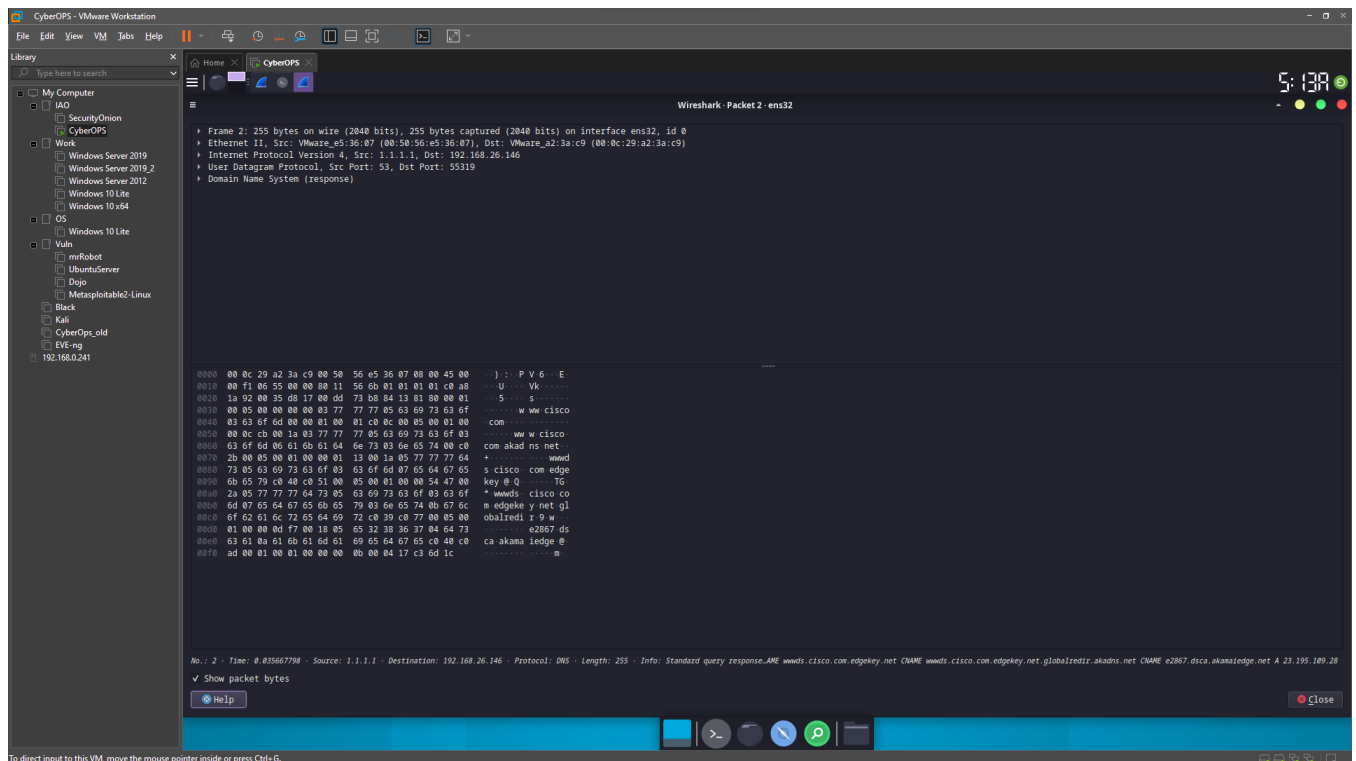
Lab - Exploring DNS Traffic



c. Observe the results.

Can the DNS server do recursive queries?

Yes



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

Question:

How do the results compare to nslookup results?

The result in Wireshark are the same with the nslookup results.

Reflection

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

If we remove the filter, other package will be display such as ARP, DHCP, HTTP, ... From these package and its information, we can learn how the network work, encapsulate packages, and many other protocol.

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

Attacker can use Wireshark to capture all traffic on LAN and can get some sensitive information if it is not encrypted.

End of document