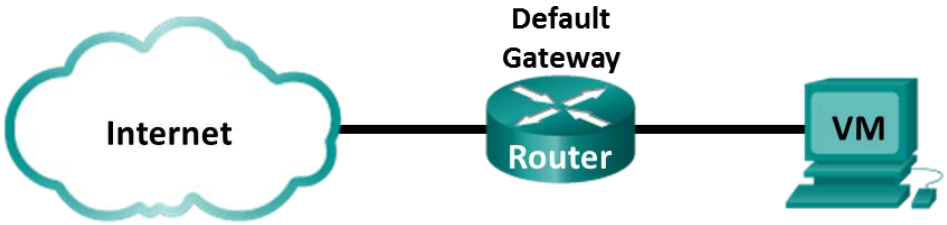
Lab - Using Wireshark to Examine a UDP DNS Capture

Topology



Objectives

Part 1: Record a PC's IP Configuration Information

Part 2: Use Wireshark to Capture DNS Queries and Responses

Part 3: Analyze Captured DNS or UDP Packets

Background / Scenario

When you use the Internet, you use the Domain Name System (DNS). DNS is a distributed network of servers that translates user-friendly domain names like www.google.com to an IP address. When you type a website URL into your browser, your PC performs a DNS query to the DNS server's IP address. Your PC's DNS query and the DNS server's response make use of the User Datagram Protocol (UDP) as the transport layer protocol. UDP is connectionless and does not require a session setup as does TCP. DNS queries and responses are very small and do not require the overhead of TCP.

In this lab, you will communicate with a DNS server by sending a DNS query using the UDP transport protocol. You will use Wireshark to examine the DNS query and response exchanges with the same server.

Required Resources

- CyberOps Workstation Virtual Machine
- Internet access

Part 1: Record VM's IP Configuration Information

In Part 1, you will use commands on your CyberOps Workstation VM to find and record the MAC and IP addresses of your VM's virtual network interface card (NIC), the IP address of the specified default gateway, and the DNS server IP address specified for the PC. Record this information in the table provided. The information will be used in parts of this lab with packet analysis.

IP address	
MAC address	
Default gateway IP address	
DNS server IP address	

a. Open a terminal in the VM. Enter **ifconfig** at the prompt to display interface information.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.19  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::997f:9b16:5aae:1868  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c9:fa:a1  txqueuelen 1000  (Ethernet)
        RX packets 1381  bytes 87320 (85.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1857 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0xd000
<some output omitted>
```

b. At the terminal prompt, enter **cat /etc/resolv.conf** to determine the DNS server.

```
[analyst@secOps ~]$ cat /etc/resolv.conf
# Generated by resolvconf
nameserver 192.168.1.1
```

c. At the terminal prompt, enter **netstat -r** to display the IP routing table to the default gateway IP address.

```
[analyst@secOps ~]$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.1.1     0.0.0.0         UG        0 0          0 enp0s3
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
```

Note: The DNS IP address and default gateway IP address are often the same, especially in small networks. However, in a business or school network, the addresses would most likely be different.

Part 2: Use Wireshark to Capture DNS Queries and Responses

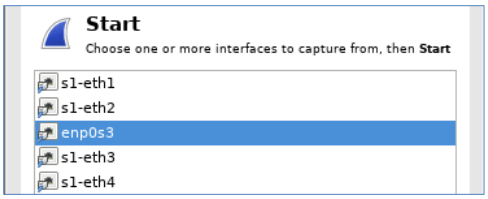
In Part 2, you will set up Wireshark to capture DNS query and response packets. This will demonstrate the use of the UDP transport protocol while communicating with a DNS server.

a. In the terminal window, start Wireshark and click **OK** when prompted.

```
[analyst@secOps ~]$ sudo wireshark-gtk
[sudo] password for analyst:

** (wireshark-gtk:950): WARNING **: Couldn't connect to accessibility bus:
Failed to connect to socket /tmp/dbus-REDRWOHelr: Connection refused
Gtk-Message: GtkDialog mapped without a transient parent. This is
discouraged.
```

b. In the Wireshark window, select **enp0s3** from the interface list and click **Start**.



c. After selecting the desired interface, click Start to capture the packets.

d. Open a web browser and type **www.google.com**. Press Enter to continue.

e. Click **Stop** to stop the Wireshark capture when you see Google's home page.

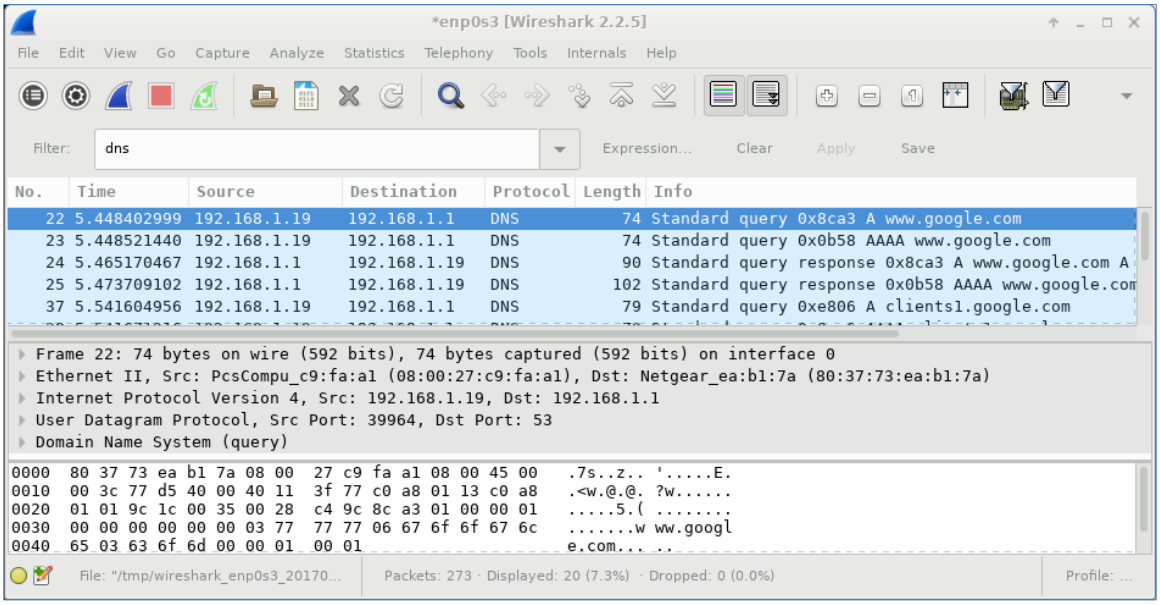
Part 3: Analyze Captured DNS or UDP Packets

In Part 3, you will examine the UDP packets that were generated when communicating with a DNS server for the IP addresses for www.google.com.

Step 1: Filter DNS packets.

a. In the Wireshark main window, type **dns** in the **Filter** field. Click **Apply**.

Note: If you do not see any results after the DNS filter was applied, close the web browser. In the terminal window, type ping **www.google.com** as an alternative to the web browser.



b. In the packet list pane (top section) of the main window, locate the packet that includes Standard query and A www.google.com. See frame 22 above as an example.

Step 2: Examine the fields in a DNS query packet.

The protocol fields, highlighted in gray, are displayed in the packet details pane (middle section) of the main window.

a. In the first line in the packet details pane, frame 22 had 74 bytes of data on the wire. This is the number of bytes it took to send a DNS query to a named server requesting the IP addresses of www.google.com. If you used a different web address, such as www.cisco.com, the byte count might be different.

b. The Ethernet II line displays the source and destination MAC addresses. The source MAC address is from your VM because your VM originated the DNS query. The destination MAC address is from the default gateway because this is the last stop before this query exits the local network.

Is the source MAC address the same as the one recorded from Part 1 for the VM?

_____

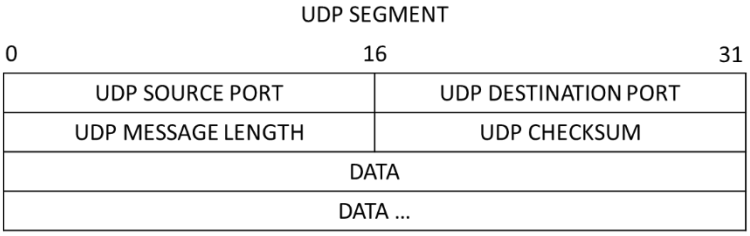
c. In the Internet Protocol Version 4 line, the IP packet Wireshark capture indicates that the source IP address of this DNS query is 192.168.1.19 and the destination IP address is 192.168.1.1. In this example, the destination address is the default gateway. The router is the default gateway in this network.

Can you identify the IP and MAC addresses for the source and destination devices?

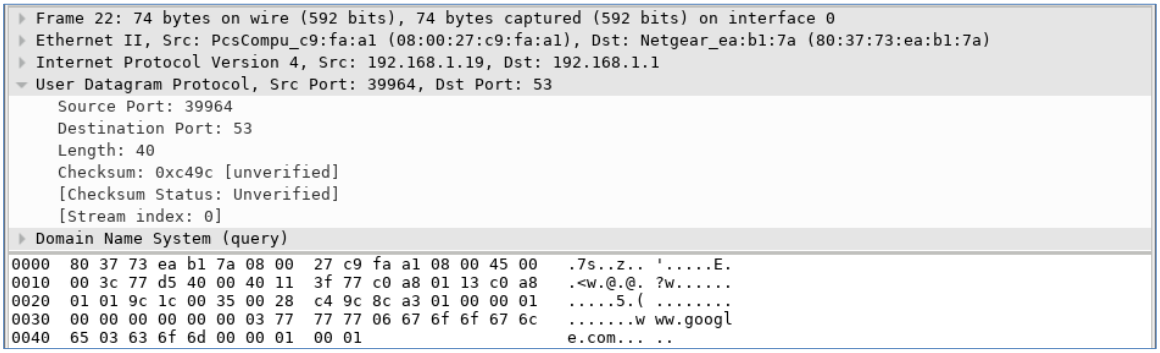
Device	IP Address	MAC Address
VM		
Default Gateway		

The IP packet and header encapsulates the UDP segment. The UDP segment contains the DNS query as the data.

d. Click the arrow next to User Datagram Protocol to view the details. A UDP header only has four fields: source port, destination port, length, and checksum. Each field in a UDP header is only 16 bits as depicted below.

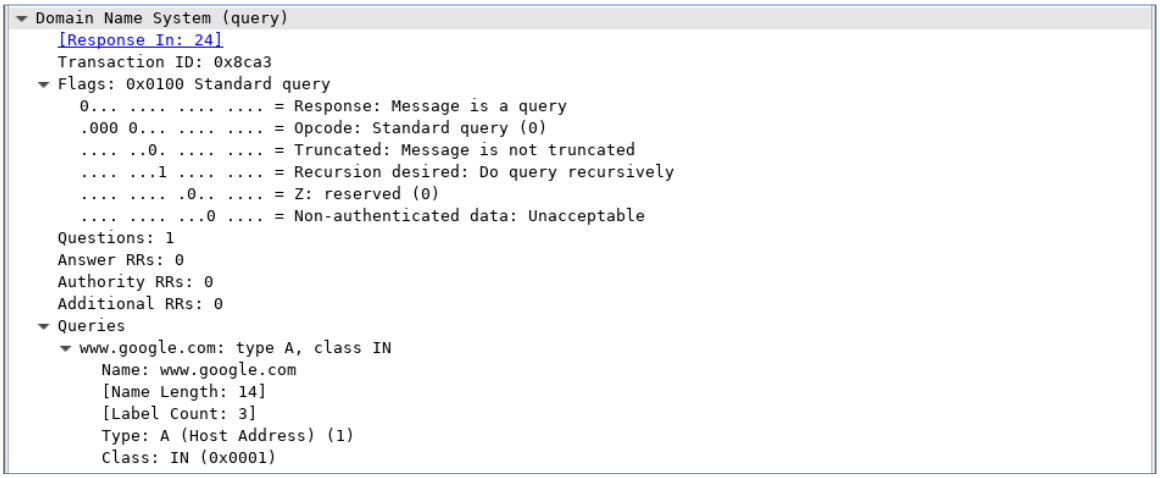


e. Click the arrow next to User Datagram Protocol to view the details. Notice that there are only four fields. The source port number in this example is 39964. The source port was randomly generated by the VM using port numbers that are not reserved. The destination port is 53. Port 53 is a well-known port reserved for use with DNS. DNS servers listen on port 53 for DNS queries from clients.



In this example, the length of the UDP segment is 40 bytes. The length of the UDP segment in your example may be different. Out of 40 bytes, 8 bytes are used as the header. The other 32 bytes are used

by DNS query data. The 32 bytes of DNS query data is in the following illustration in the packet bytes pane (lower section) of the Wireshark main window.



The checksum is used to determine the integrity of the UDP header after it has traversed the Internet.

The UDP header has low overhead because UDP does not have fields that are associated with the three-way handshake in TCP. Any data transfer reliability issues that occur must be handled by the application layer.

Record your Wireshark results in the table below:

Frame size	
Source MAC address	
Destination MAC address	
Source IP address	
Destination IP address	
Source port	
Destination port	

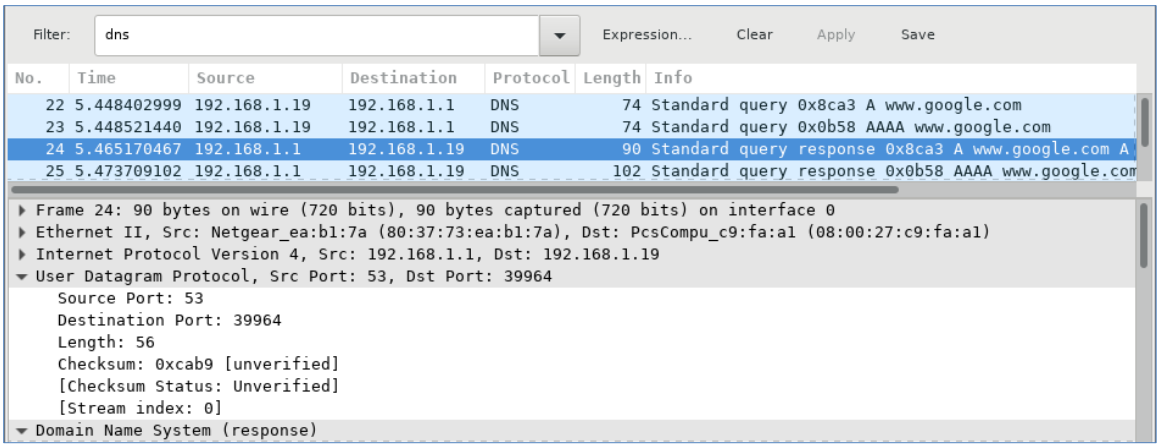
Is the source IP address the same as the local PC's IP address you recorded in Part 1? _____

Is the destination IP address the same as the default gateway noted in Part 1? _____

Step 3: Examine the fields in a DNS response packet.

In this step, you will examine the DNS response packet and verify that the DNS response packet also uses the UDP.

a. In this example, frame 24 is the corresponding DNS response packet. Notice the number of bytes on the wire is 90. It is a larger packet compared to the DNS query packet. This is because the DNS response packet will include a variety of information about the domain.



b. In the Ethernet II frame for the DNS response, what device is the source MAC address and what device is the destination MAC address?

_____

c. Notice the source and destination IP addresses in the IP packet. What is the destination IP address? What is the source IP address?

Destination IP address: _____Source IP address: _____

What happened to the roles of source and destination for the VM and default gateway?

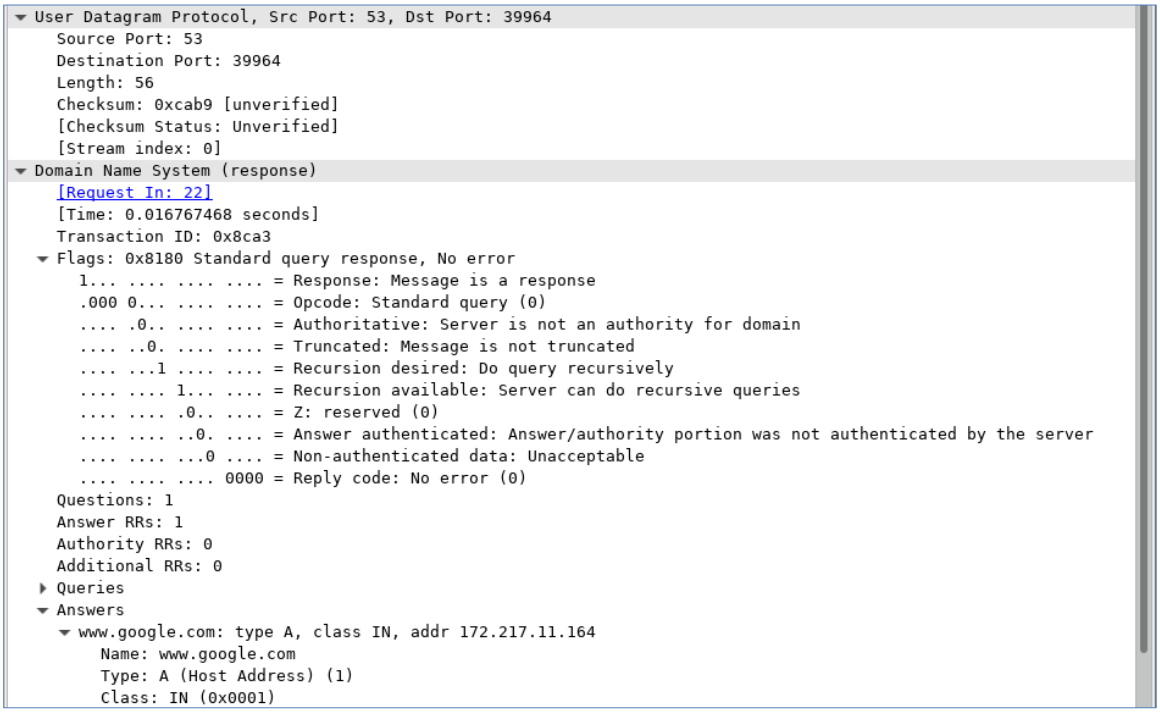
_____

_____

d. In the UDP segment, the role of the port numbers has also reversed. The destination port number is 39964. Port number 39964 is the same port that was generated by the VM when the DNS query was sent to the DNS server. Your VM listens for a DNS response on this port.

The source port number is 53. The DNS server listens for a DNS query on port 53 and then sends a DNS response with a source port number of 53 back to the originator of the DNS query.

When the DNS response is expanded, notice the resolved IP addresses for www.google.com in the **Answers** section.



Reflection

What are the benefits of using UDP instead of TCP as a transport protocol for DNS?

_____

_____