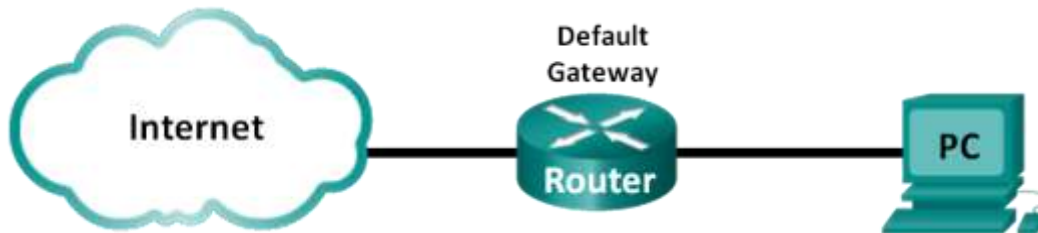# Lab - Using Wireshark to Examine a UDP DNS Capture

Topology

Objectives

Part 1: Record the IP Configuration Information of a PC

Part 2: Use Wireshark to Capture DNS Queries and Responses

Part 3: Analyze Captured DNS or UDP Packets

Background / Scenario

If you have ever used the internet, you have used 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 IP address. Your PC DNS server query and the DNS server 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.

Note: This lab cannot be completed using Netlab. This lab assumes that you have internet access.

Required Resources

1 PC (Windows 7, 8, or 10 with command prompt access, internet access, and Wireshark installed)

Part 1:   Record a PC's IP Configuration Information

In Part 1, you will use the **ipconfig /all** command on your local PC to find and record the MAC and IP addresses of your PC 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	

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 to demonstrate the use of the UDP transport protocol while communicating with a DNS server.

a. Click the Windows **Start** button and navigate to the Wireshark program.

b. Select an interface for Wireshark to capture packets. Select (highlight) the active capturing interface.
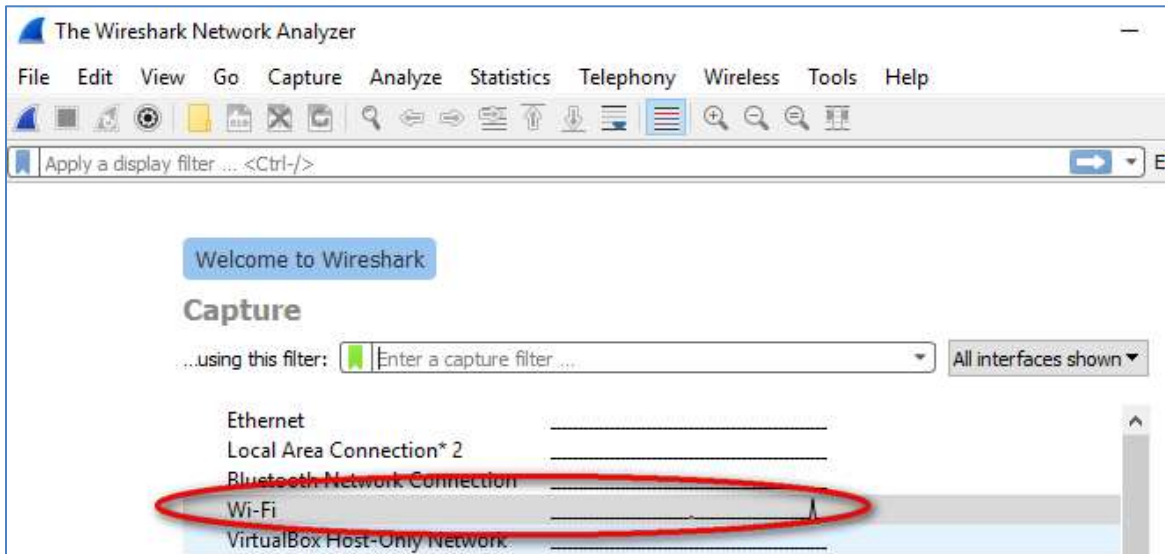
c. After selecting the desired interface, click **Start** to capture the packets.

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 the Google 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 entry area of the **Filter** toolbar and press **Enter**.

Note: If you do not see any results after the DNS filter was applied, close the web browser. In the command prompt window, type **ipconfig /flushdns** to remove all previous DNS results. Restart the Wireshark capture and repeat the instructions in Part 2b –2e. If this does not resolve the issue, type **nslookup www.google.com** in the command prompt window as an alternative to the web browser.
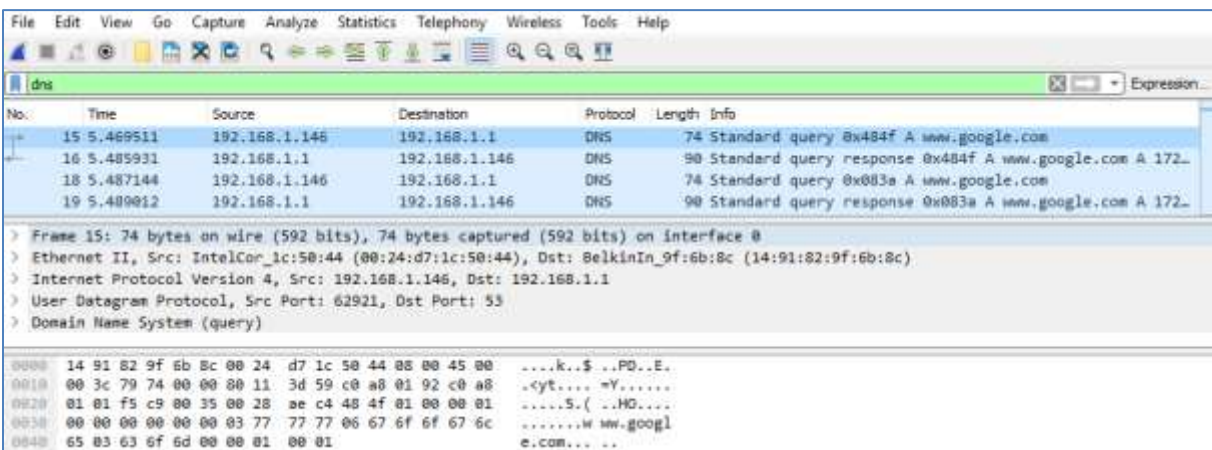
b. In the packet list pane (top section) of the main window, locate the packet that includes **Standard query** and **A www.google.com**. See frame 15 as an example.

Step 2: Examine a UDP segment using DNS query.

Examine the UDP by using a DNS query for www.google.com as captured by Wireshark. In this example, Wireshark capture frame 15 in the packet list pane is selected for analysis. The protocols in this query are displayed in the packet details pane (middle section) of the main window. The protocol entries are highlighted in gray.
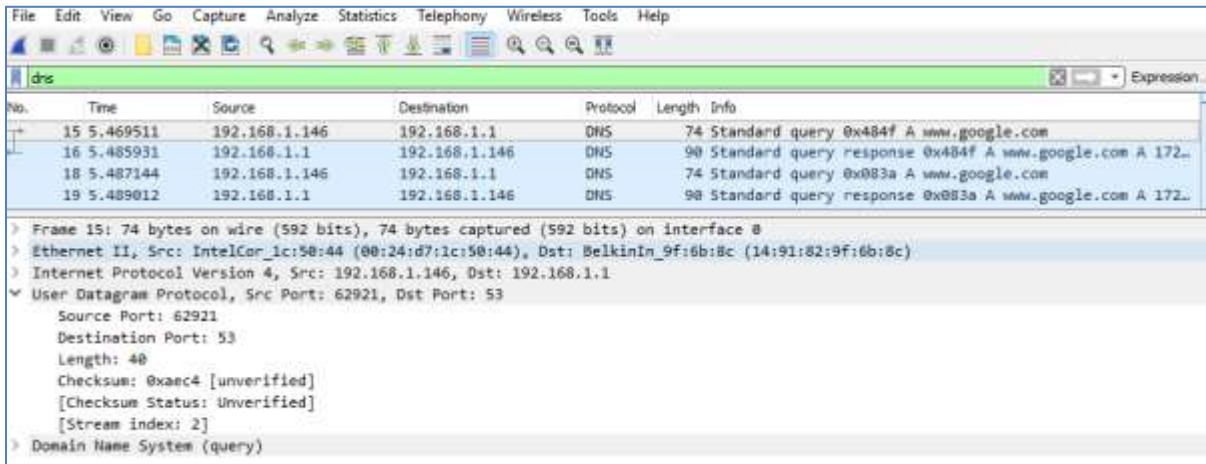
a. In the first line in the packet details pane, frame 15 had 74 bytes of data on the wire. This is the number of bytes to send a DNS query to a name server requesting the IP addresses of www.google.com.

b. The Ethernet II line displays the source and destination MAC addresses. The source MAC address is from your local PC because your local PC 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 local PC?

_____

c. In the Internet Protocol Version 4 line, the IP packet Wireshark capture indicates that the source IP address of this DNS query is 192.168.1.146 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
Local PC		
Default Gateway		

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

d. 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.

UDP SEGMENT

0	16	31
UDP SOURCE PORT	UDP DESTINATION PORT	
UDP MESSAGE LENGTH	UDP CHECKSUM	
DATA		
DATA ...		
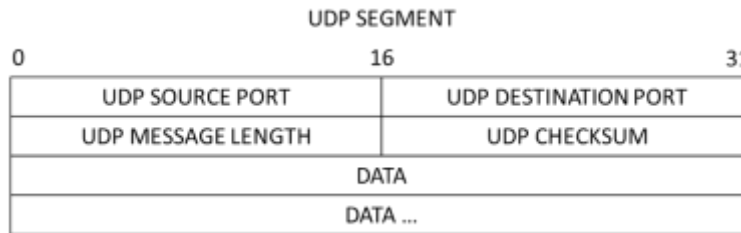
Expand the User Datagram Protocol in the packet details pane by clicking the plus (+) sign. Notice that there are only four fields. The source port number in this example is 60868. The source port was randomly generated by the local PC using port numbers that are not reserved. The destination port is 53. Port 53 is a well-known port reserved for use with DNS. DNS servers listen on port 53 for DNS queries from clients.

```
∨ User Datagram Protocol, Src Port: 62921, Dst Port: 53
      Source Port: 62921
      Destination Port: 53
      Length: 40
      Checksum: 0xaec4 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 2]
```

In this example, the length of the UDP segment is 40 bytes. 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 highlighted in the following illustration in the packet bytes pane (lower section) of the Wireshark main window.

```
∨ Domain Name System (query)
      [Response In: 16]
      Transaction ID: 0x484f
   >  Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
   ∨ Queries
      ∨ www.google.com: type A, class IN
            Name: www.google.com
            [Name Length: 14]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
```

The checksum is used to determine the integrity of the packet 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:

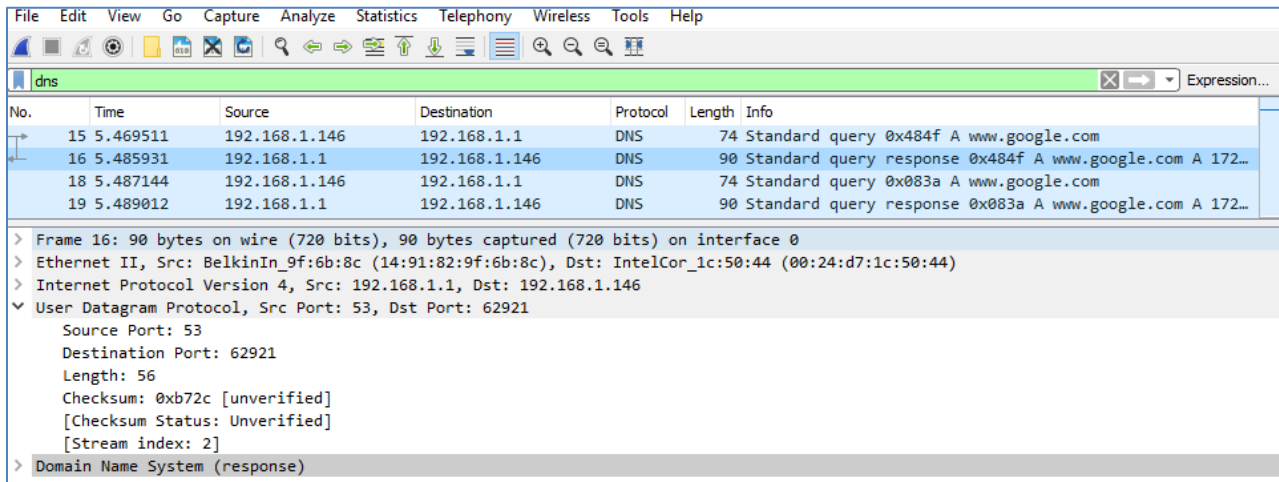|	
Frame size	
Source MAC address	
Destination MAC address	
Source IP address	
Destination IP address	
Source port	
Destination port	

Is the source IP address the same as the local PC 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 a UDP using DNS response.

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 16 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.

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 local host and default gateway?

_____

d. In the UDP segment, the role of the port numbers has also reversed. The destination port number is 62921. Port number 62921 is the same port that was generated by the local PC when the DNS query was sent to the DNS server. Your local PC 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.

```
✓ User Datagram Protocol, Src Port: 53, Dst Port: 62921
      Source Port: 53
      Destination Port: 62921
      Length: 56
      Checksum: 0xb72c [unverified]
      [Checksum Status: Unverified]
      [Stream index: 2]
✓ Domain Name System (response)
      [Request In: 15]
      [Time: 0.016420000 seconds]
      Transaction ID: 0x484f
   > Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 1
      Authority RRs: 0
      Additional RRs: 0
   > Queries
   ✓ Answers
      ✓ www.google.com: type A, class IN, addr 172.217.9.4
            Name: www.google.com
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 262
            Data length: 4
            Address: 172.217.9.4
```

Reflection

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

_____

_____

_____

_____