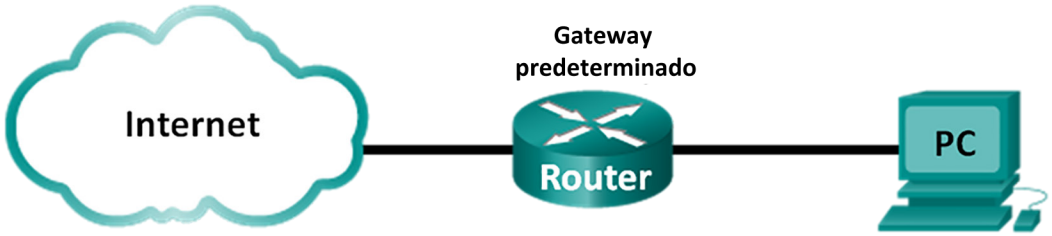
Práctica de laboratorio: Uso de Wireshark para examinar una captura de UDP y DNS

Topología



Objetivos

Parte 1: Registrar la información de configuración IP de una PC

Parte 2: Utilizar Wireshark para capturar consultas y respuestas DNS

Parte 3: Analizar los paquetes capturados de DNS o UDP

Aspectos básicos/situación

Si alguna vez utilizó Internet, utilizó el sistema de nombres de dominio (DNS). DNS es una red distribuida de servidores que traduce nombres de dominio descriptivos como www.google.com a una dirección IP. Cuando se escribe la URL de un sitio web en el navegador, la PC realiza una consulta de DNS a la dirección IP del servidor DNS. La consulta del servidor DNS de su PC y la respuesta del servidor DNS utilizan el protocolo de datagramas de usuario (UDP) como protocolo de capa de transporte. A diferencia de TCP, UDP funciona sin conexión y no requiere una configuración de sesión. Las consultas y respuestas de DNS son muy pequeñas y no requieren la sobrecarga de TCP.

En esta práctica de laboratorio, establecerá comunicación con un servidor DNS enviando una consulta de DNS mediante el protocolo de transporte UDP. Utilizará Wireshark para examinar los intercambios de consulta y respuesta de DNS con el mismo servidor.

Nota: Esta práctica de laboratorio no se puede realizar con Netlab. Para esta práctica de laboratorio, se asume que usted tiene acceso a Internet.

Recursos necesarios

1 PC (Windows 7, 8 o 10 con acceso a la petición de ingreso de comando, acceso a Internet y Wireshark instalado)

Parte 1: Registrar la información de configuración de IP de una PC

En la parte 1, utilizará el comando **ipconfig /all** en su PC local para buscar y registrar las direcciones IP y MAC de la tarjeta de interfaz de red (NIC) de su PC, la dirección IP del gateway predeterminado especificado y la dirección IP del servidor DNS especificado para la PC. Registre esta información en la tabla proporcionada. La información se utilizará en partes de este laboratorio con el análisis de paquetes.

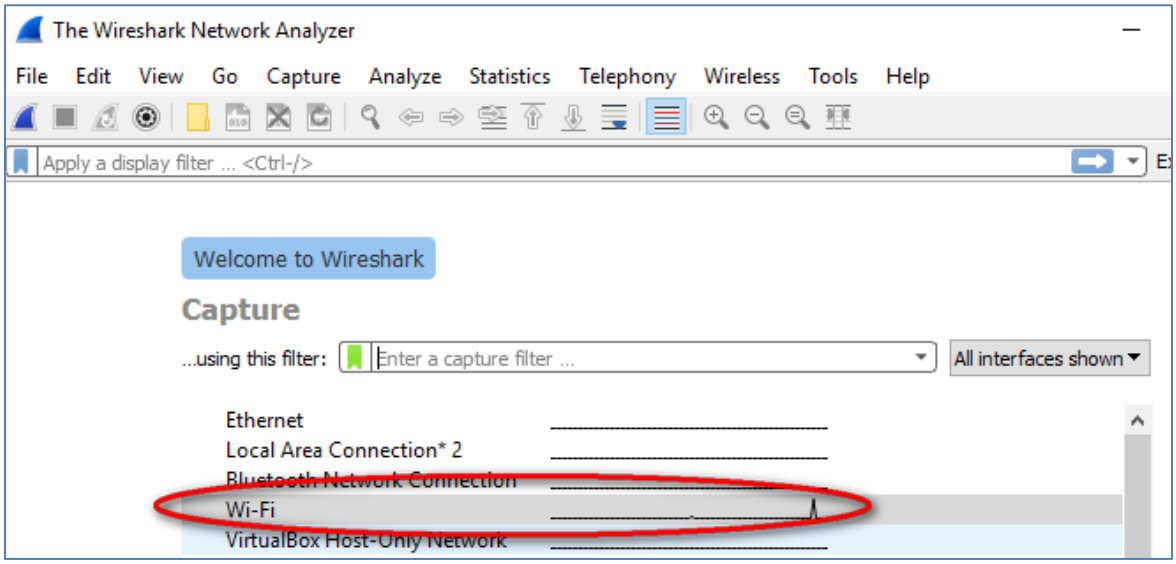
Dirección IP	
Dirección MAC	
Dirección IP del gateway predeterminado	
Dirección IP del servidor DNS	

Parte 2: Utilizar Wireshark para capturar consultas y respuestas de DNS

En la parte 2, configurará Wireshark para capturar paquetes de consultas y respuestas de DNS a fin de demostrar el uso del protocolo de transporte UDP en la comunicación con un servidor DNS.

a. Haga clic en el botón **Inicio** de Windows y busque el programa Wireshark.

b. Seleccione una interfaz para que Wireshark capture paquetes. Seleccione (resalte) la interfaz de captura activa.



c. Después de seleccionar la interfaz deseada, haga clic en **Start** (Comenzar) para capturar los paquetes.

d. Abra un navegador web y escriba **www.google.com**. Presione **Enter** (Introducir) para continuar.

e. Haga clic en **Stop** (Detener) para detener la captura de Wireshark cuando vea la página de inicio de Google.

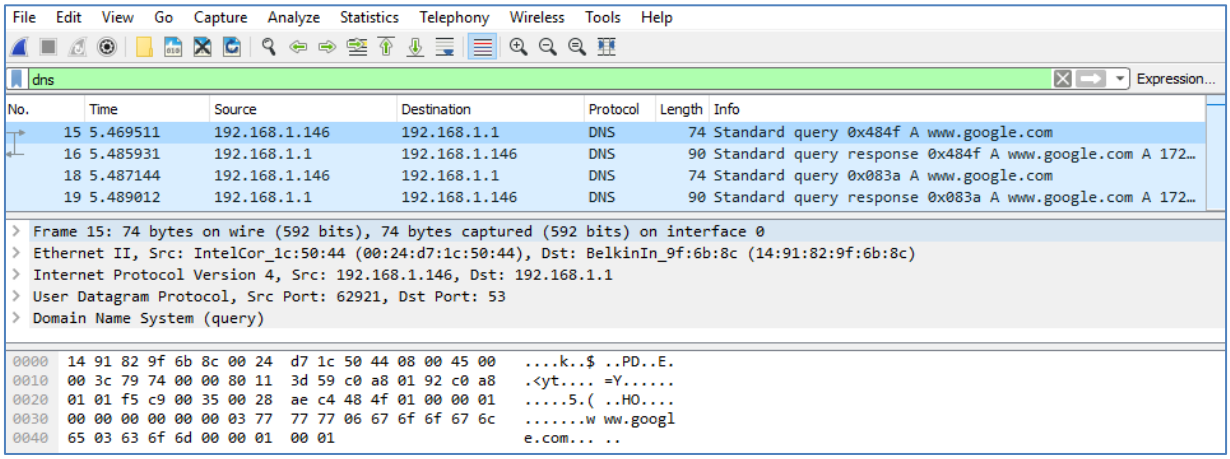
Parte 3: Analizar los paquetes capturados de DNS o UDP

En la parte 3, examinará los paquetes de UDP que se generaron al comunicarse con un servidor DNS para las direcciones IP de www.google.com.

Paso 1: Filtrar los paquetes de DNS

a. En la ventana principal de Wireshark, escriba **dns** en el área de entrada de la barra de herramientas **Filter** (Filtro) y presione **Enter** (Introducir).

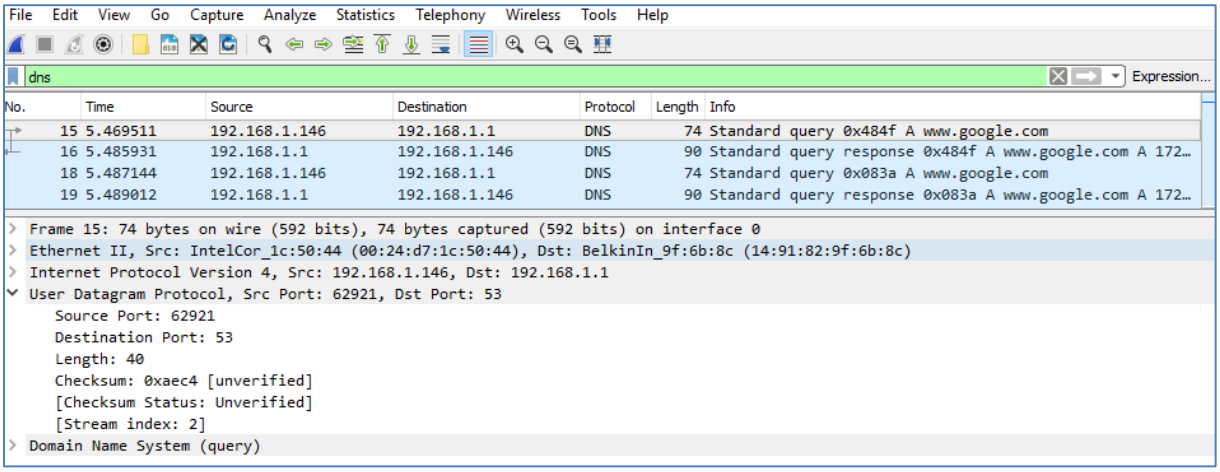
Nota: Si no ve ningún resultado después de aplicar el filtro DNS, cierre el navegador web. En la ventana del símbolo del sistema, escriba **ipconfig /flushdns** para eliminar todos los resultados de DNS anteriores. Reinicie la captura de Wireshark y repita las instrucciones de las partes 2b a 2e. Si esto no resuelve el problema, escriba **nslookup www.google.com** en la ventana del símbolo del sistema como alternativa para el navegador web.



b. En el panel de lista de paquetes (sección superior) de la ventana principal, localice el paquete que incluye **Standard query** (Consulta estándar) y **A www.google.com**. Consulte la trama 15 como ejemplo.

Paso 2: Examinar un segmento de UDP utilizando una consulta de DNS

Examine el UDP utilizando una consulta de DNS para www.google.com según la captura de Wireshark. En este ejemplo, se seleccionó para el análisis la trama 15 de la captura de Wireshark en el panel de la lista de paquetes. Los protocolos de esta consulta se muestran en el panel de detalles del paquete (sección media) de la ventana principal. Las entradas de protocolo están resaltadas en gris.



a. En la primera línea del panel de detalles del paquete, la trama 15 tenía 74 bytes de datos de conexión. Esta es la cantidad de bytes para enviar una consulta DNS a un servidor de nombres que solicita direcciones IP de www.google.com.

b. La línea Ethernet II muestra las direcciones MAC de origen y destino. La dirección MAC de origen proviene de su PC local porque la PC local originó la consulta de DNS. La dirección MAC de destino proviene del gateway predeterminado porque esta es la última parada antes de que esta consulta salga de la red local.

¿Es la dirección MAC de origen la misma que la registrada en la parte 1 para la PC local?

c. En la línea Internet Protocol Version 4, la captura de Wireshark del paquete IP indica que la dirección IP de origen de esta consulta de DNS es 192.168.1.146 y la dirección IP de destino es 192.168.1.1. En este ejemplo, la dirección de destino es el gateway predeterminado. El router es el gateway predeterminado en esta red.

¿Puede identificar las direcciones IP y MAC para los dispositivos de origen y de destino?

Dispositivo	Dirección IP	Dirección MAC
PC local		
Gateway predeterminado		

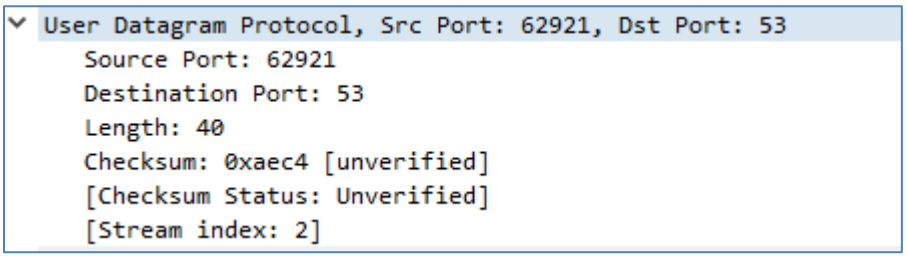
El paquete IP y el encabezado encapsulan el segmento de UDP. El segmento de UDP contiene la consulta de DNS como datos.

d. Un encabezado de UDP solo tiene cuatro campos: puerto de origen, puerto de destino, longitud y checksum. Cada campo de un encabezado de UDP tiene solo 16 bits, como se muestra a continuación.

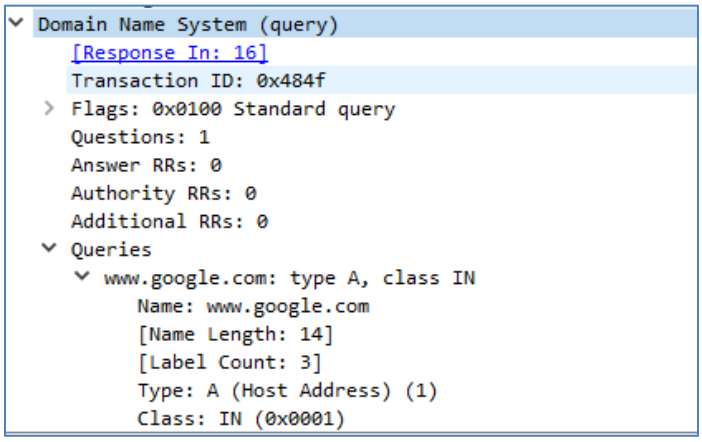
SEGMENTO UDP

0	16	31
PUERTO DE ORIGEN UDP	PUERTO DE DESTINO UDP	
LONGITUD DE MENSAJE UDP	CHECKSUM DE UDP	
DATOS		
DATOS...		

Expanda el protocolo de datagramas de usuario en el panel de detalles del paquete haciendo clic en el signo más (+). Observe que solo hay cuatro campos. El número del puerto de origen en este ejemplo es 60868. La PC local generó de manera aleatoria el puerto de origen utilizando números de puerto que no están reservados. El puerto de destino es 53. El puerto 53 es un puerto conocido reservado para el uso con DNS. Los servidores DNS esperan en el puerto 53 las consultas de DNS de los clientes.



En este ejemplo, la longitud del segmento de UDP es de 40 bytes. De los 40 bytes, 8 bytes se utilizan como encabezado. Los datos de la consulta de DNS utilizan los otros 32 bytes. Los 32 bytes de los datos de consulta de DNS se resaltan en la siguiente ilustración en el panel de bytes del paquete (sección inferior) de la ventana principal de Wireshark.



La checksum se utiliza para determinar la integridad del paquete después de haber atravesado Internet.

El encabezado de UDP tiene poca sobrecarga porque UDP no tiene campos que estén asociados con la negociación en tres pasos en TCP. Cualquier problema de confiabilidad de la transferencia de datos que ocurra debe ser manejado por la capa de aplicaciones.

Registre sus resultados de Wireshark en la tabla siguiente:

Tamaño de la trama	
Dirección MAC de origen	
Dirección MAC de destino	
Dirección IP de origen	
Dirección IP de destino	
Puerto de origen	
Puerto de destino	

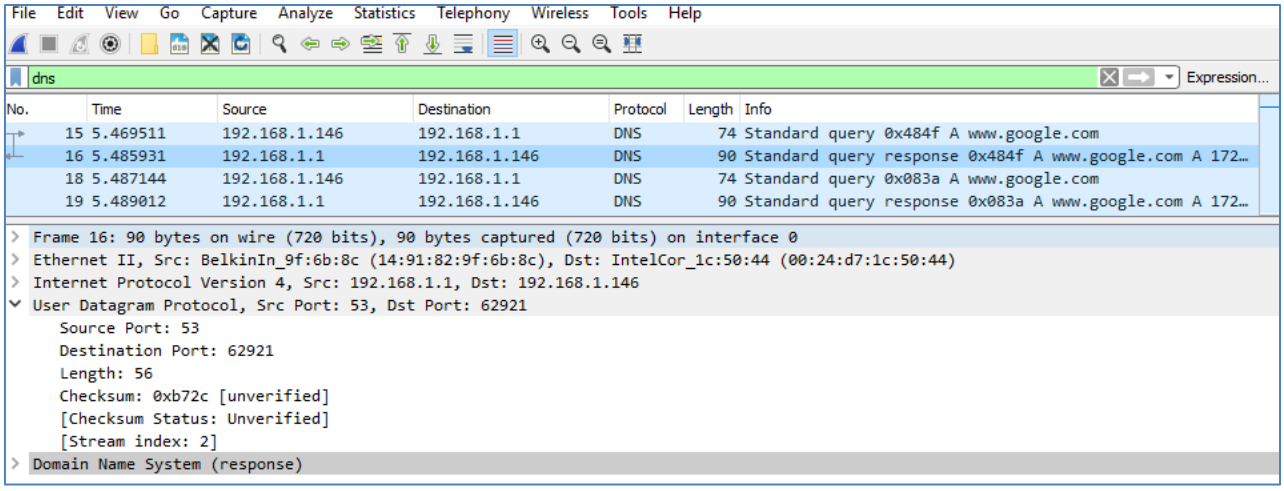
¿Es la dirección IP de origen la misma que la dirección IP de la PC local que registró en la parte 1?

¿Es la dirección IP de destino la misma que el gateway predeterminado que observó en la parte 1?

Paso 3: Examinar un segmento de UDP utilizando una respuesta de DNS

En este paso, examinará el paquete de respuesta de DNS y comprobará que el paquete de respuesta de DNS también utiliza UDP.

a. En este ejemplo, la trama 16 es el paquete de respuesta DNS correspondiente. Observe que la cantidad de bytes en la conexión es 90. Es un paquete más grande en comparación con el paquete de consulta de DNS.



b. En la trama Ethernet II para la respuesta de DNS, ¿qué dispositivo es la dirección MAC de origen y qué dispositivo es la dirección MAC de destino?

c. Observe las direcciones IP de origen y destino en este paquete IP. ¿Cuál es la dirección IP de destino? ¿Cuál es la dirección IP de origen?

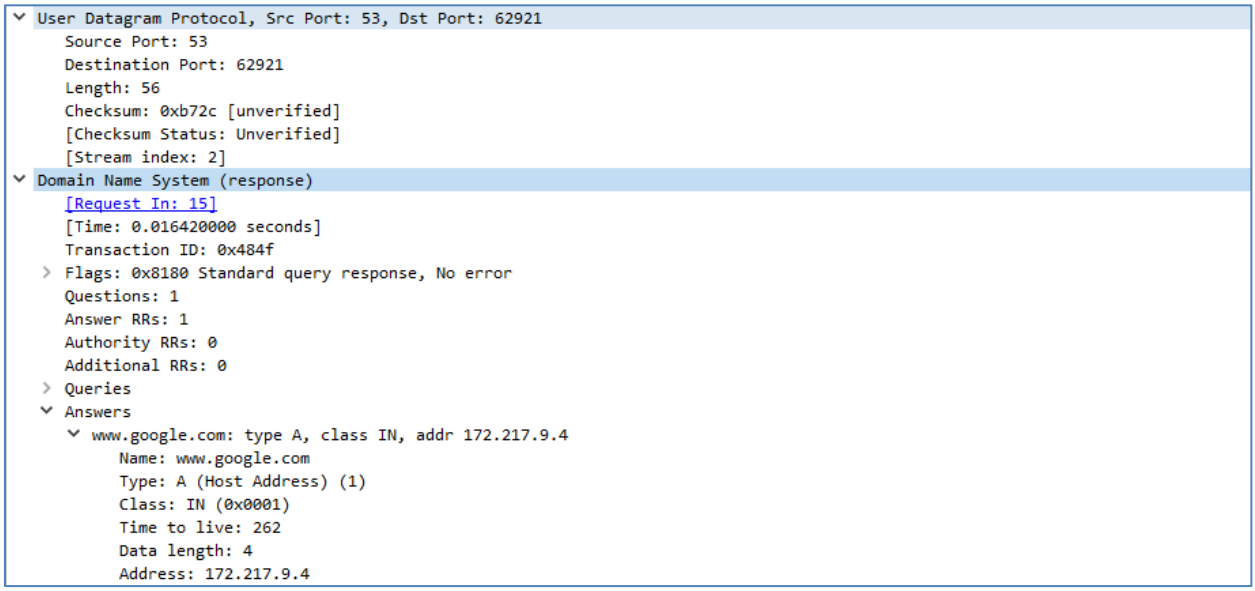
Dirección IP de destino: Dirección IP de origen:

¿Qué sucedió con los roles de origen y destino para el host local y el gateway predeterminado?

d. En el segmento de UDP, el rol de los números de puerto también se invirtió. El número del puerto de destino es 62921. El número de puerto 62921 es el mismo puerto que generó la PC local cuando se envió la consulta de DNS al servidor DNS. La PC local espera una respuesta de DNS en este puerto.

El número del puerto de origen es 53. El servidor DNS espera una consulta de DNS en el puerto 53 y luego envía una respuesta de DNS con un número de puerto de origen de 53 al originador de la consulta de DNS.

Al expandirse la respuesta de DNS, observe las direcciones IP resueltas para www.google.com en la sección **Answers** (Respuestas).



Reflexión

¿Cuáles son los beneficios de utilizar UDP en lugar de TCP como protocolo de transporte para DNS?