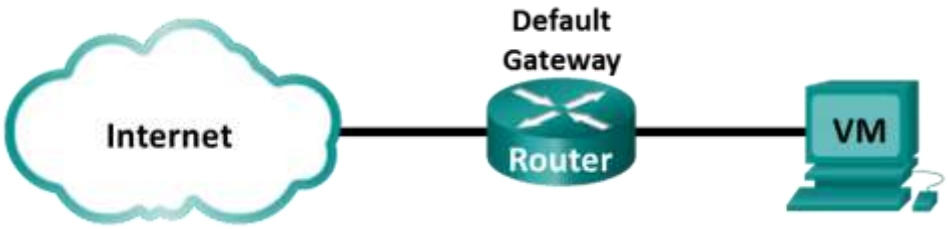
Práctica de laboratorio: Utilizar Wireshark para examinar una captura DNS de UDP

Topología



Objetivos

Parte 1: Registrar la información de configuración de 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 / Escenario

Cuando utiliza Internet, está utilizando 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 hacen uso del 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.

Recursos necesarios

- Máquina virtual (Virtual Machine) CyberOps Workstation
- Acceso a Internet

Instrucciones

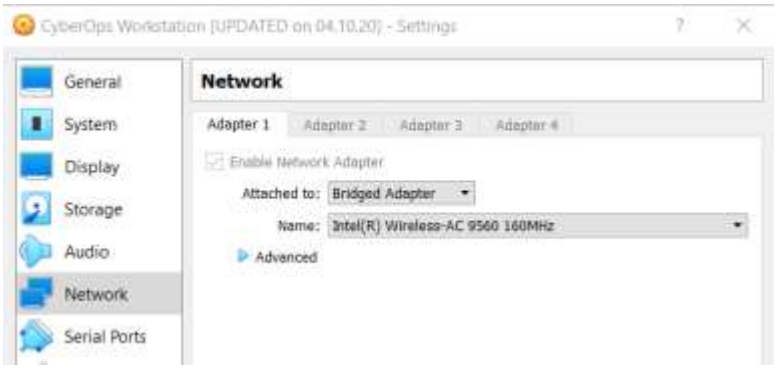
Parte 1: Registrar la información sobre la configuración IP de la VM

En la Parte 1, utilizarán los comandos de sus VM CyberOps Workstation para encontrar y registrar las direcciones IP y MAC de las tarjetas de interfaz de red (NIC) virtuales de sus VM, 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.

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

a. Las configuraciones de red de su CyberOps Workstation VM deben estar establecidas en un adaptador puente (bridged adapter). Para revisar su configuración de red vaya a: **Machine** > **Settings**, seleccione **Network**, la opción **Adapter 1, Attached to: Bridged Adapter**.



b. Abra una ventana de terminal en la VM. Escriban **ifconfig** en el cursor para mostrar la información de la interfaz. Si no tiene una dirección IP en su red local, utilice el siguiente comando en la ventana de terminal.

```
[analyst@secOps ~]$ sudo lab.support.files/scripts/configure_as_dhcp.sh
Configuring the NIC to request IP info via DHCP...
Requesting IP information...
IP Configuration successful.
```

Nota: En la parte 1, sus resultados varían dependiendo de las configuraciones de su red de área local y conexión a internet.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.8.10 netmask 255.255.255.0 broadcast 192.168.8.255
        inet6 fe80::a00:27ff:fe82:75df prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:82:75:df txqueuelen 1000 (Ethernet)
        RX packets 41953 bytes 14354223 (13.6 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 15249 bytes 1723493 (1.6 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
<some output omitted>
```

c. En el prompt del terminal escriba **cat /etc/resolv.conf** para determinar el servidor DNS.

```
[analyst@secOps ~]$ cat /etc/resolv.conf
```

```
# Resolver configuration file.
# See resolv.conf(5) for details.
nameserver 8.8.4.4
nameserver 209.165.200.235
```

d. En el prompt del terminal, ingrese **netstat-rn** para mostrar la tabla de enrutamiento IP a la dirección IP predeterminada del gateway.

```
[analyst@secOps ~]$ netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.8.1 0.0.0.0 UG 0 0 0 enp0s3
192.168.8.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3
192.168.8.1 0.0.0.0 255.255.255.255 UH 0 0 0 enp0s3
```

Nota: La dirección IP del DNS y la del gateway predeterminado a menudo son la misma, especialmente en redes pequeñas. Sin embargo, en la red de una empresa o de una escuela, las direcciones muy probablemente sean diferentes.

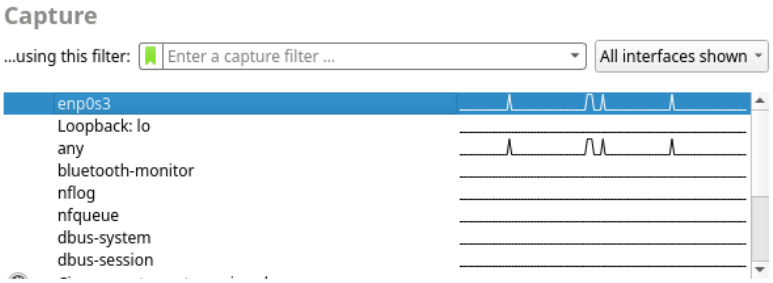
Parte 2: Utilizar Wireshark para capturar consultas y respuestas DNS

En la Parte 2 configurará Wireshark para capturar paquetes de consultas y respuestas DNS. Con esto se demostrará el uso del protocolo de transporte UDP al comunicarse con un servidor DNS.

a. En la ventana del terminal, inicie Wireshark y haga clic en **OK** (Aceptar) cuando el sistema se lo solicite.

```
[analyst@secOps ~]$ wireshark &
```

b. En la ventana del Wireshark, seleccione con doble clic **enp0s3** desde la lista de interfaces.



c. Abra el navegador web y diríjase a **www.google.com**

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

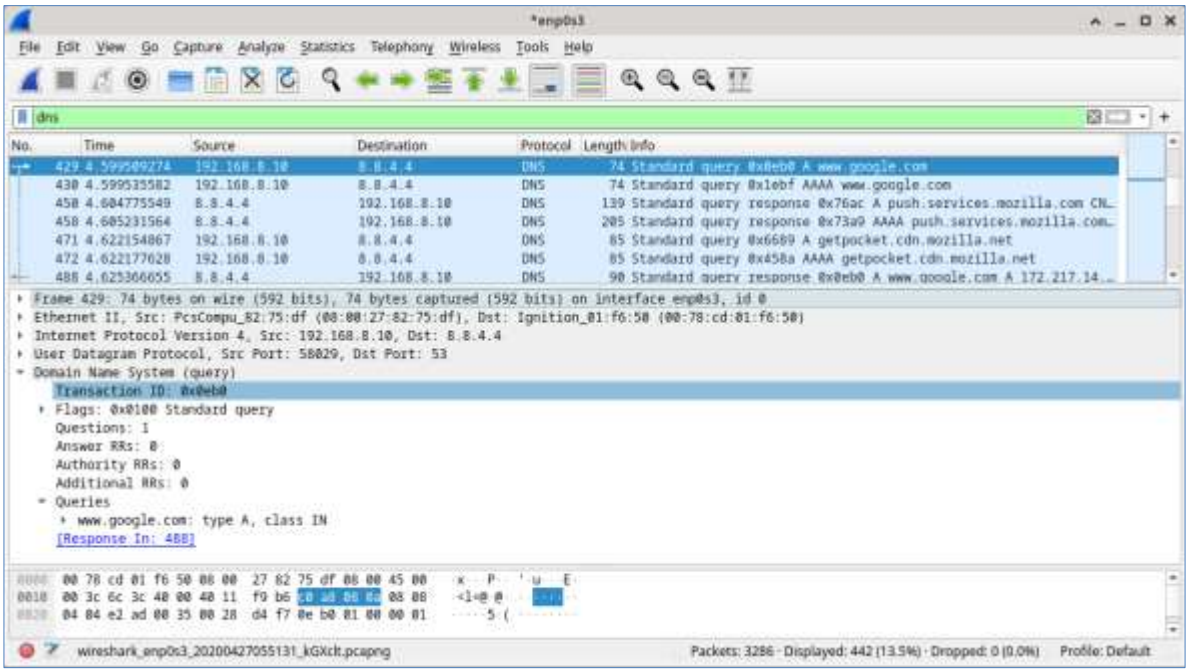
Parte 3: Analizar los paquetes capturados de DNS o UDP

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 campo **Filter** (Filtro). Haga clic en **Apply** (Aplicar).

Nota: Si no visualiza ningún resultado después de aplicar el filtro DNS, cierre el navegador web. En la ventana del terminal escriba **www.google.com** como alternativa al 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**. Observe la trama 429 anterior como ejemplo.

Paso 2: Examinar los campos presentes en un paquete de consulta DNS

Los espacios de protocolo, resaltados en color gris, se muestran en el panel de detalles del paquete (sección media) de la ventana principal.

a. En la primera línea del panel de detalles del paquete, el cuadro 429 tiene 74 bytes de datos en el cable. Esta es la cantidad de bytes que se necesitó para enviar una consulta DNS a un servidor con nombre que está solicitando las direcciones IP de www.google.com. Si utilizó otra dirección web, como www.cisco.com, la cantidad de bytes podría ser diferente.

b. La línea Ethernet II muestra las direcciones MAC de origen y destino. La dirección MAC de origen proviene de sus PC locales porque sus PC originaron la consulta 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 VM?

c. En la línea del Protocolo de Internet Versión 4 (IPv4), la captura del paquete IP Wireshark indica que la dirección IP de origen de esta consulta de DNS es 192.168.8.10 y la dirección IP de destino es 8.8.4.4. En este ejemplo, la dirección de destino es la del servidor DNS.

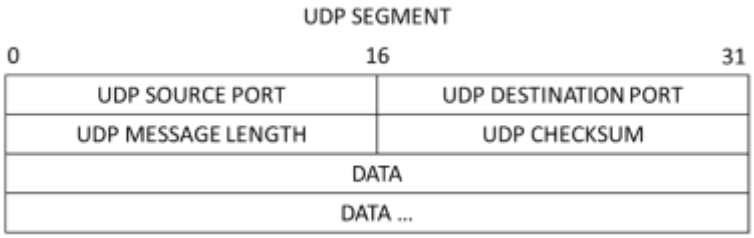
¿Puede identificar la dirección IP y dirección MAC de origen y destino de este paquete?

Dispositivo	Dirección IP	Dirección MAC
Estación de trabajo del cliente		
Destino Servidor DNS / Gateway predeterminado		

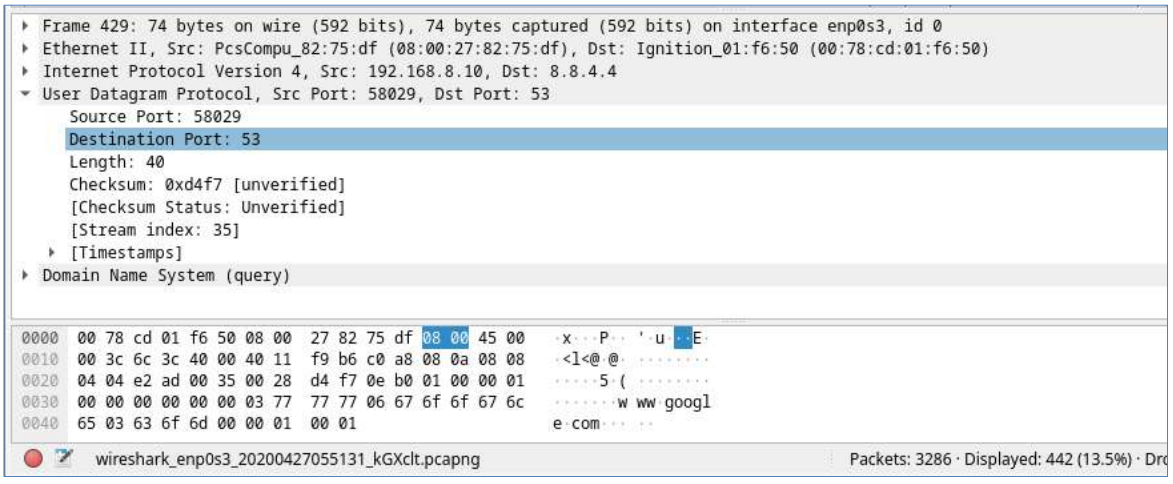
Nota: La dirección IP de destino es para el servidor DNS, pero el destino de la dirección MAC es para el gateway predeterminado.

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.

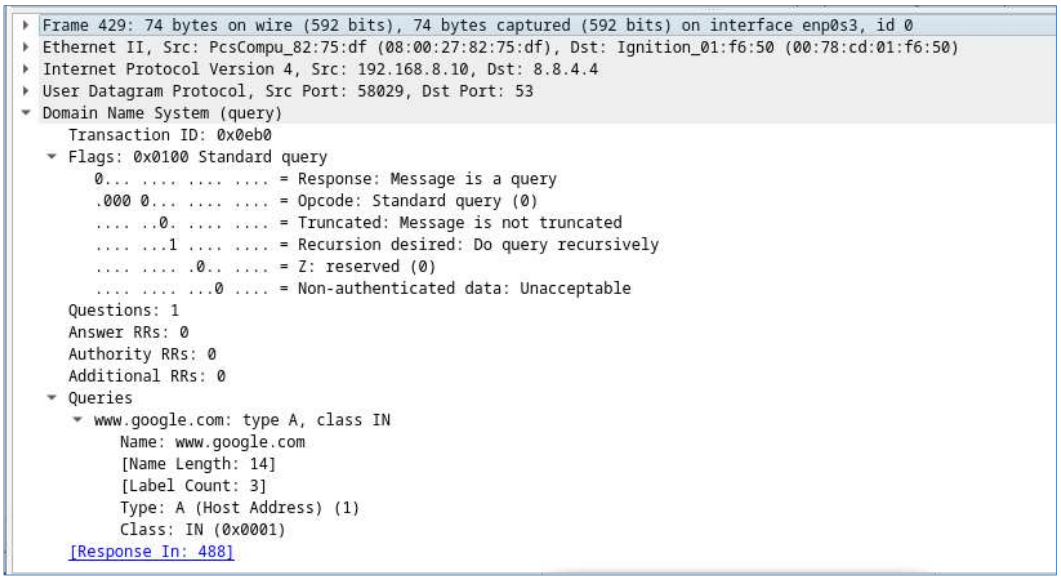


Haga clic en la flecha contigua a User Datagram Protocol para ver los detalles. Observen que solo hay cuatro campos. El número del puerto de origen en este ejemplo es 58029. La VM generó de manera aleatoria el puerto de origen utilizando números de puerto que no están reservados. El puerto de destino 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. La longitud del segmento UDP de su ejemplo puede ser diferente. 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 DNS están en la

siguiente ilustración en el panel de bytes del paquete (sección inferior) de la ventana principal de Wireshark.



El checksum es usado para determinar la integridad del encabezado de UDP después de haber atravesado el Internet.

El encabezado de UDP tiene poca sobrecarga porque UDP no tiene campos que estén asociados con el protocolo de enlace de tres vías en TCP. Cualquier problema de confiabilidad de la transferencia de datos que ocurra debe ser manejado por la capa de aplicación.

Expanda lo necesario para ver los detalles. Registre sus resultados de Wireshark en la tabla siguiente:

Descripción	Resultados del Wireshark
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	

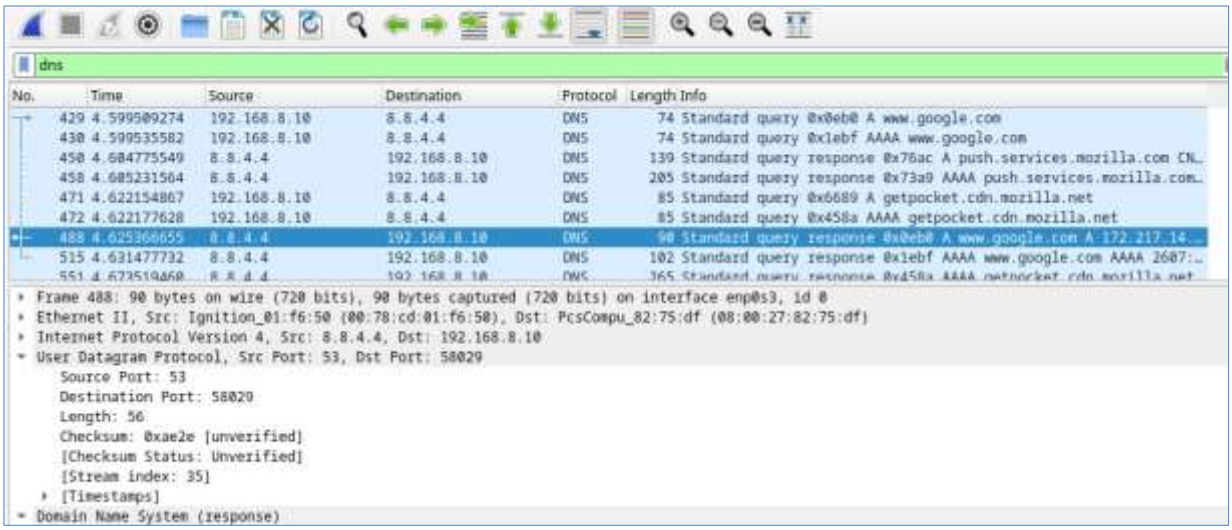
¿Es la dirección IP de origen la misma que la dirección IP de la PC local que registró en la parte 1?

¿Es la dirección IP de destino la misma que la puerta de enlace predeterminada (gateway) que observó en la parte 1?

Paso 3: Examinar los campos en un paquete de respuesta DNS

En este paso, examinarán el paquete de respuesta DNS y comprobarán que también utiliza UDP.

a. En este ejemplo, la trama 488 es el paquete de respuesta DNS correspondiente. Observen que la cantidad de bytes en la conexión es 90. Es un paquete más grande en comparación con el paquete de consulta de DNS. Esto se debe a que el paquete de respuesta DNS incluirá información variada sobre el dominio.



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?

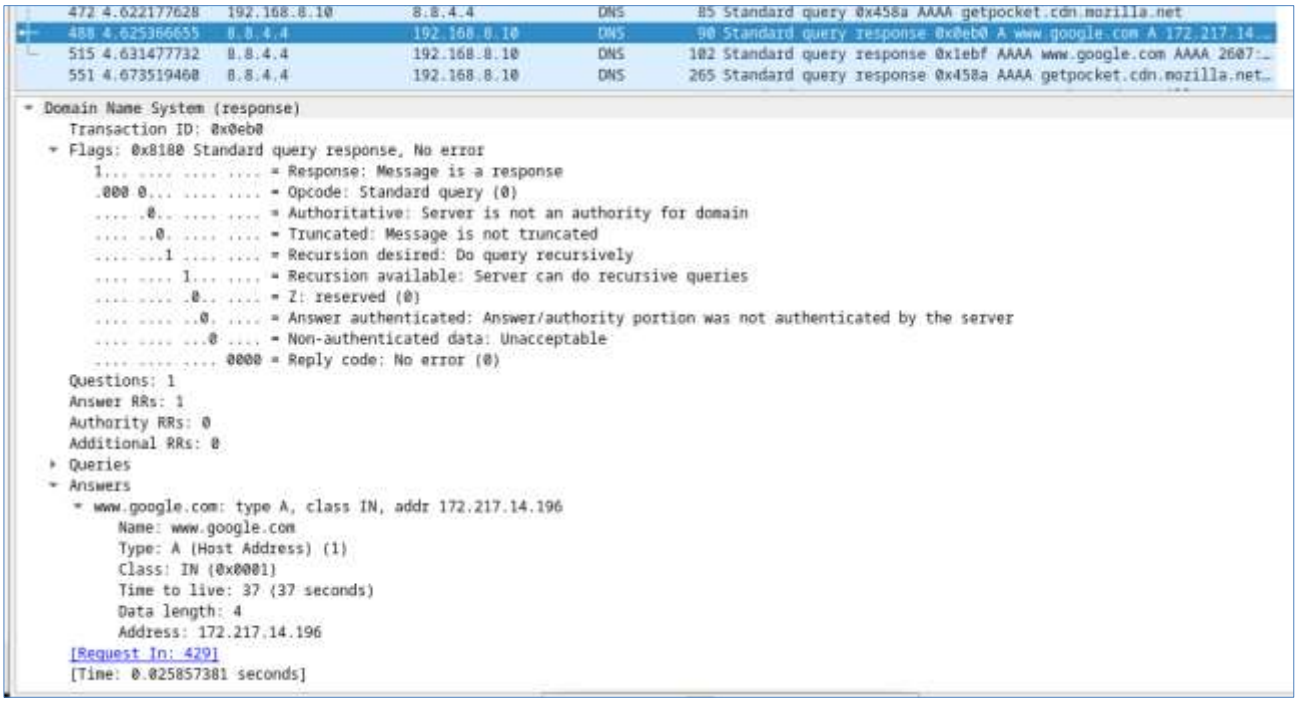
¿Cuál es la dirección IP de origen?

¿Qué sucedió con los roles de origen y destino correspondientes a la VM y al gateway predeterminado?

d. En el segmento UDP, el rol de los números de puerto también se invirtió. El número del puerto de destino es 58029. El número de puerto 58029 es el mismo puerto que generó la VM cuando se envió la consulta DNS al servidor DNS. La VM espera una respuesta 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 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).



Pregunta de reflexión

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