Práctica de laboratorio: Examinación de Telnet y SSH en Wireshark

Topología

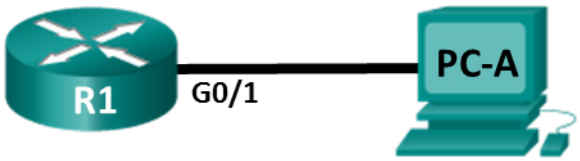


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: configurar los dispositivos para el acceso por SSH

Parte 2: examinar una sesión de Telnet con Wireshark

Parte 3: examinar una sesión de SSH con Wireshark

Aspectos básicos/situación

En esta actividad de laboratorio, deberá configurar un router para que acepte la conectividad de SSH y usará Wireshark para capturar y ver las sesiones de Telnet y SSH. Esto demostrará la importancia del cifrado con SSH.

Nota: Los routers que se utilizan en las actividades prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces de router al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
- 1 PC (Windows 7, 8 o 10 con un programa de emulación de terminal, como Tera Term, y Wireshark instalado)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: Configurar los dispositivos para el acceso por SSH

En la parte 1, establecerá la topología de la red y configurará los ajustes básicos, como las direcciones IP de la interfaz, el acceso al dispositivo y las contraseñas del router.

Paso 1: Realizar el cableado de red tal como se muestra en la topología

Paso 2: Iniciar y Volver a cargar el router

Paso 3: Configurar los ajustes básicos en el router

a. Acceda al router mediante el puerto de la consola e ingrese al modo EXEC privilegiado.

b. Entre al modo de configuración.

c. Configure el nombre del dispositivo como se indica en la tabla de direccionamiento.

d. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

f. Asigne **cisco** como la contraseña de consola y permita el inicio de sesión.

g. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

h. Encripte las contraseñas de texto no cifrado.

i. Cree un banner que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

j. Configure y active la interfaz G0/1 utilizando la información de la tabla de direccionamiento.

Paso 4: Configurar R1 para el acceso por SSH

a. Configure el dominio para el dispositivo.

```
R1(config)# ip domain-name ccna-lab.com
```

b. Configure el método de cifrado de clave.

```
R1(config)# crypto key generate rsa modulus 1024
```

c. Configure un nombre de usuario de la base de datos local.

```
R1(config)# username admin privilege 15 secret adminpass
```

d. Habilite Telnet y SSH en las líneas VTY.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

e. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

```
R1(config-line)# login local
R1(config-line)# end
```

Paso 5: Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 6: Configurar PC-A

a. Configure PC-A con una dirección IP y una máscara de subred.

b. Configure una puerta de enlace predeterminada para PC-A.

Paso 7: Verificar la conectividad de la red

Haga ping a R1 desde PC-A. Si el ping falla, resuelva los problemas de la conexión.

Parte 2: Examinar una sesión de Telnet con Wireshark

En la parte 2, deberá usar Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet en el router. Utilizará Tera Term para acceder a R1 mediante Telnet, se registrará y luego emitirá el comando **show run** en el router.

Nota: Si no tiene un paquete de software de cliente Telnet/SSH instalado en la PC, deberá instalarlo antes de continuar. Dos paquetes populares de software gratuito de Telnet/SSH son Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) y PuTTY (www.putty.org).

Nota: Telnet no está disponible desde el símbolo del sistema enWindows 7, de manera predeterminada. Para habilitar Telnet para usarlo en la ventana de símbolo del sistema, haga clic en **Start** (Comenzar) > **Control Panel** (Panel de control) > **Programs** (Programas) > **Programs and Features** (Programas y funciones) > **Turn Windows features on or off** (Activar o desactivar las funciones de Windows). Haga clic en la casilla de verificación **Telnet Client** (Cliente Telnet) y luego haga clic en **OK** (Aceptar).

Paso 1: Capturar los datos

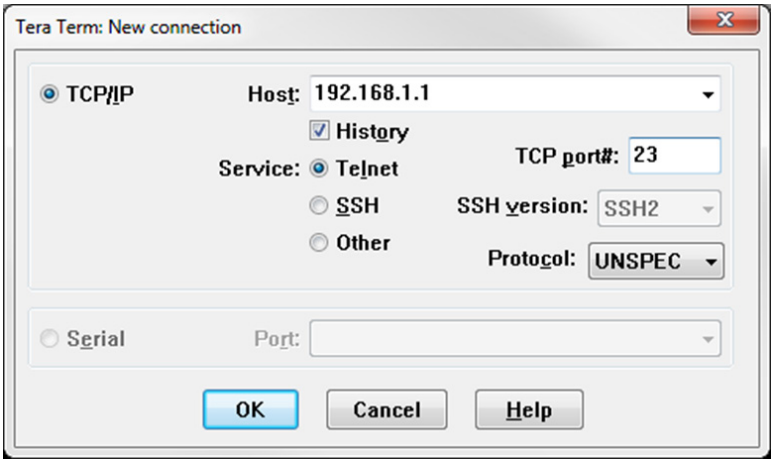
a. Abra Wireshark.

b. Comience a capturar los datos en la interfaz de LAN.

Nota: Si no puede comenzar la captura en la interfaz LAN, deberá abrir Wireshark con la opción **Run as Administrator** (Ejecutar como administrador).

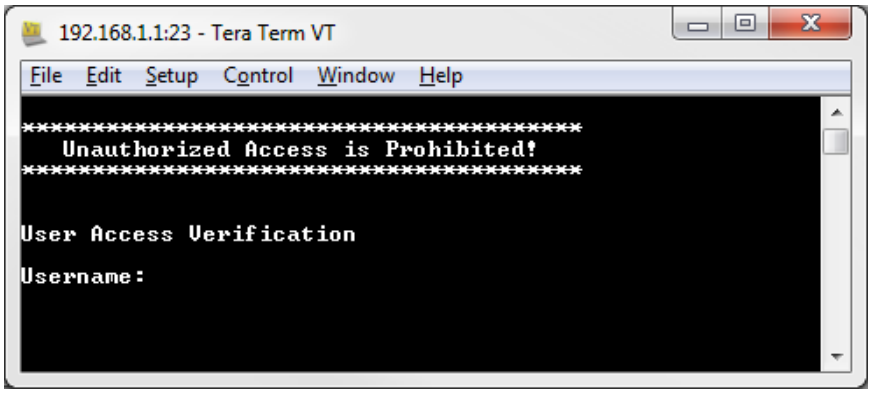
Paso 2: Iniciar una sesión de Telnet en el router

a. Abra Tera Term y seleccione el botón de opción **Telnet** del campo Service (Servicio) y, en el campo Host, ingrese **192.168.1.1**.



¿Cuál es el puerto TCP predeterminado para las sesiones de Telnet?

b. En la petición **Username:** (Nombre de usuario:), ingrese **admin** y en la petición **Password:** (Contraseña:), ingrese **adminpass**. Estas peticiones se generan porque configuró las líneas VTY para que utilicen la base de datos local con el comando **login local**.



c. Emita el comando **show run**.

```
R1# show run
```

d. Ingrese **exit** (Salir) para cerrar la sesión de Telnet y Tera Term.

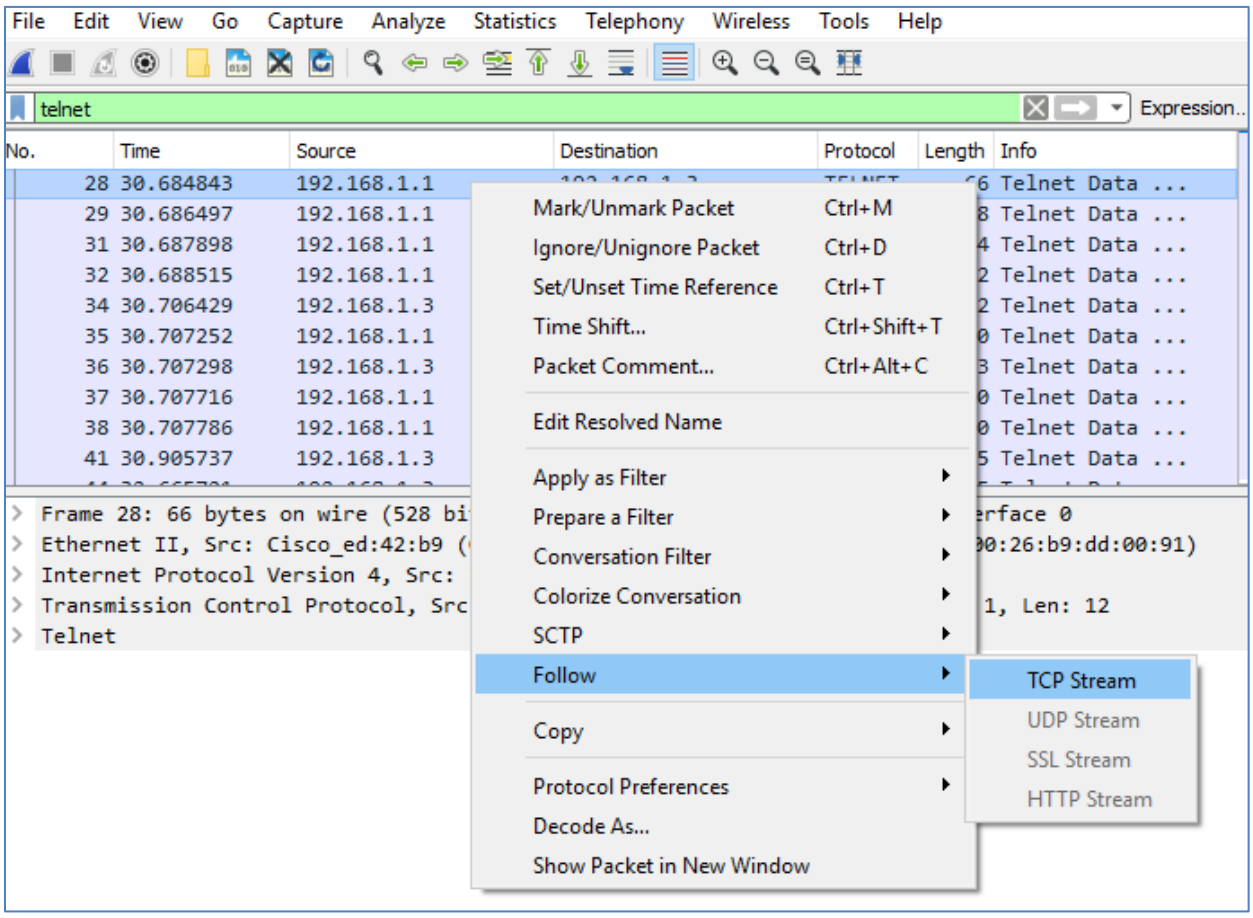
```
R1# exit
```

Paso 3: Detener la captura Wireshark

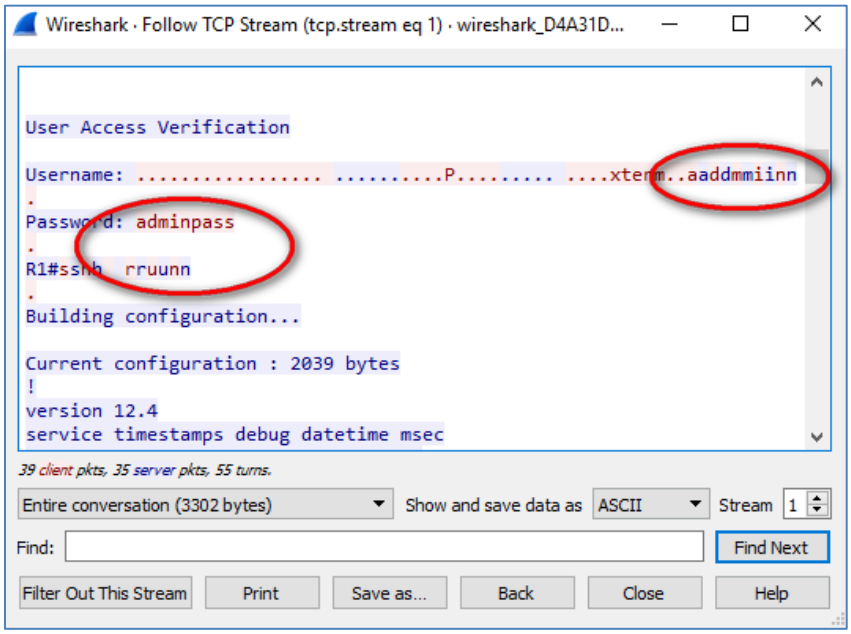
Paso 4: Aplicar un filtro de Telnet a los datos de captura de Wireshark

Paso 5: Utilizar la función Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

a. Haga clic con el botón derecho en una de las líneas **Telnet** y en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream**.



b. En la ventana **Follow TCP Stream** (Seguir stream de TCP), se muestran los datos para su sesión de Telnet con el router. Toda la sesión y la contraseña se muestran como texto no cifrado. Observe que el nombre de usuario y el comando **show run** que ingresó aparecen con caracteres duplicados. Esto se debe al ajuste de eco en Telnet para permitirle ver los caracteres que escribe en la pantalla.



c. Cuando termine de revisar la sesión de Telnet en la ventana **Follow TCP Stream** (Seguir stream de TCP), haga clic en **Close** (Cerrar).

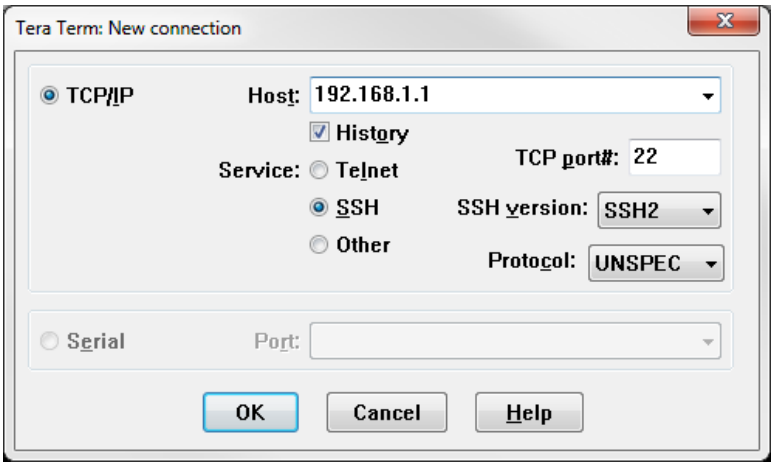
Parte 3: Examinar una sesión de SSH con Wireshark

En la parte 4, deberá usar el software Tera Term para establecer una sesión de SSH con el router. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN

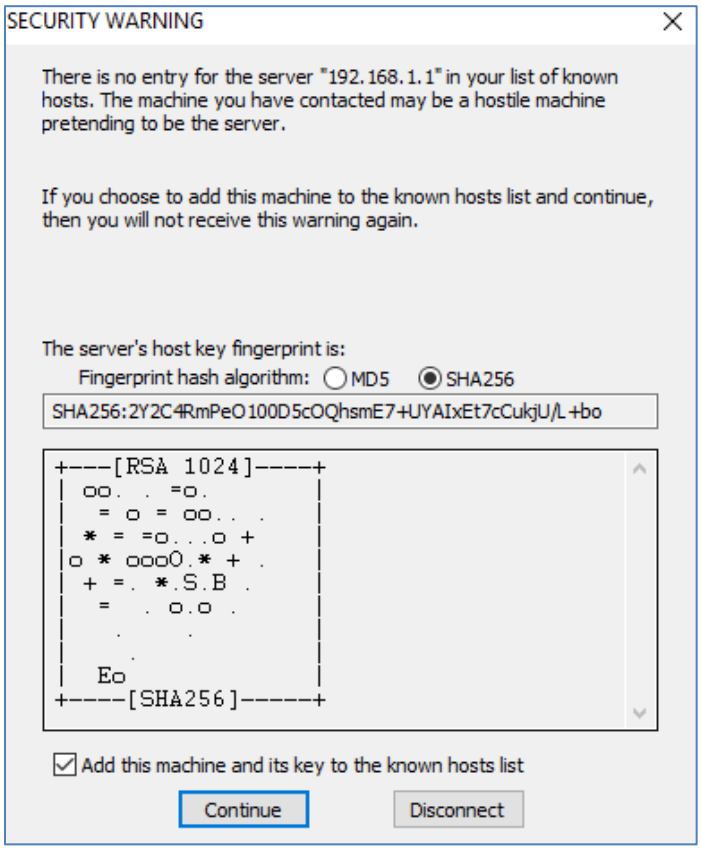
Paso 2: Iniciar una sesión de SSH en el router

a. Abra Tera Term e ingrese la dirección IP de la interfaz G0/1 de R1 en el campo **Host:** de la ventana **Tera Term: New Connection** (Tera Term: Conexión nueva). Asegúrese de que el botón de opción **SSH** esté seleccionado y haga clic en **OK** (Aceptar) para conectarse al router.

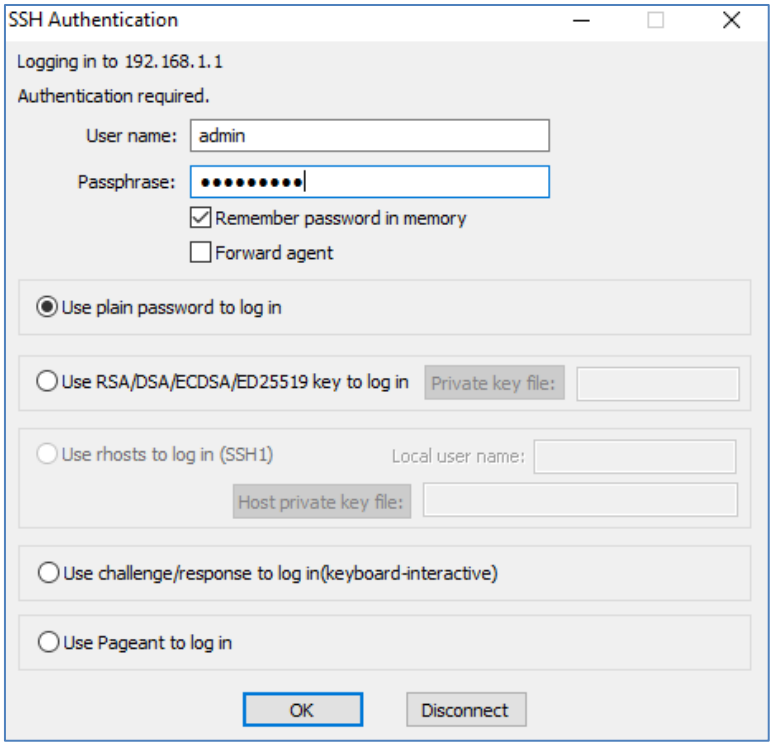


¿Cuál es el puerto TCP predeterminado que se usa para las sesiones de SSH?

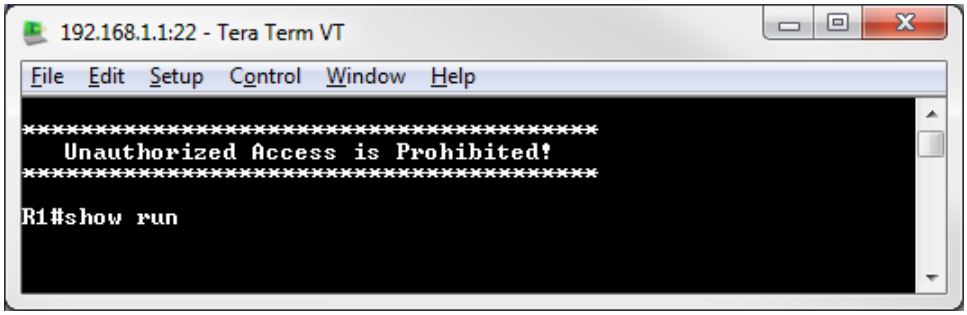
b. La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (Advertencia de seguridad) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y luego haga clic en **Continue** (Continuar).



c. En la ventana **SSH Authentication** (Autenticación de SSH), ingrese **admin** en username (Nombre de usuario) y **adminpass** en passphrase (Frase de contraseña). Haga clic en **OK** (Aceptar) para registrarse en el router.



d. Estableció una sesión de SSH en el router. El software Tera Term parece muy similar a una ventana de comandos. En el símbolo del sistema, emita el comando **show run**.



e. Salga de la sesión de SSH emitiendo el comando **exit**.

```
R1# exit
```

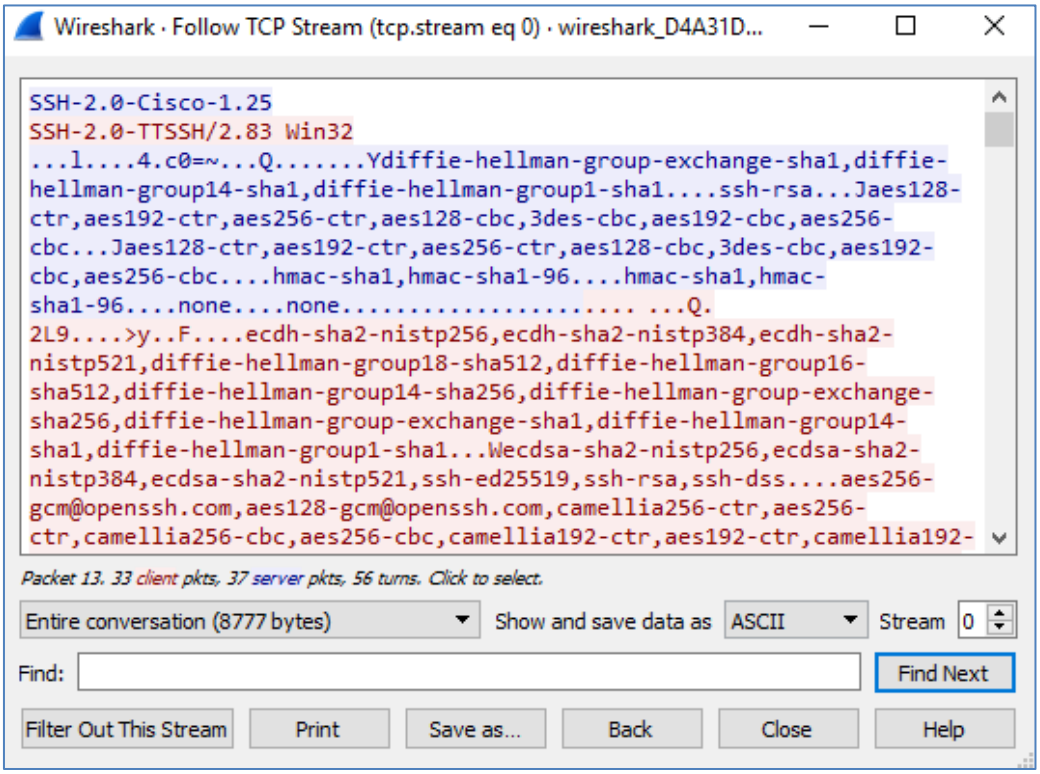
Paso 3: Detener la captura Wireshark

Paso 4: Aplicar un filtro de SSH a los datos de captura de Wireshark

Paso 5: Utilizar la función Follow TCP Stream en Wireshark para ver la sesión de SSH

a. Haga clic con el botón derecho en una de las líneas **SSHv2** en la sección Packet list (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).

b. Examine la ventana **Follow TCP Stream** (Seguir stream de TCP) en la sesión de SSH. Los datos se cifraron y son ilegibles. Compare los datos de la sesión de SSH con los datos de la sesión de Telnet.



¿Por qué se prefiere SSH en lugar de Telnet para las conexiones remotas?

c. Luego de haber examinado su sesión SSH, haga clic en **Close** (Cerrar).

d. Cierre Wireshark.

Reflexión

¿Cómo brindaría acceso a un dispositivo de red a varios usuarios, cada uno con un nombre de usuario diferente?

Tabla de resumen de interfaces de router

Resumen de interfaces de router				
Modelo de router	**Interfaz Ethernet 1**	**Interfaz Ethernet 2**	**Interfaz serial 1**	**Interfaz serial 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de hacer una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.