

Práctica 1

Observación de la negociación en 3 pasos de Topología TCP

- Antonio J. Galán Herrera

| | |
|---|----------|
| Parte 1: Preparar Wireshark para capturar paquetes | 2 |
| Paso 1 | 2 |
| Parte 2: Capturar, localizar y examinar paquetes | 3 |
| Paso 1 | 3 |
| Paso 2 | 3 |
| Paso 3 | 4 |
| Reflexión | 7 |

Parte 1: Preparar Wireshark para capturar paquetes

Paso 1

Recuperar las direcciones de interfaz de la PC.

```
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Realtek PCIe GbE Family Controller
Dirección física. . . . . : FC-AA-14-23-1F-90
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::986:b751:388e:64ab%20(Preferido)
Dirección IPv4. . . . . : 192.168.1.30(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 117221908
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-05-84-15-FC-AA-14-23-1F-90
Servidores DNS. . . . . : 80.58.61.254
                        80.58.61.250
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Dirección IP del host: 192.168.1.30.

Dirección MAC del host: FC.AA.14.23.1F.90.

Parte 2: Capturar, localizar y examinar paquetes

Paso 1

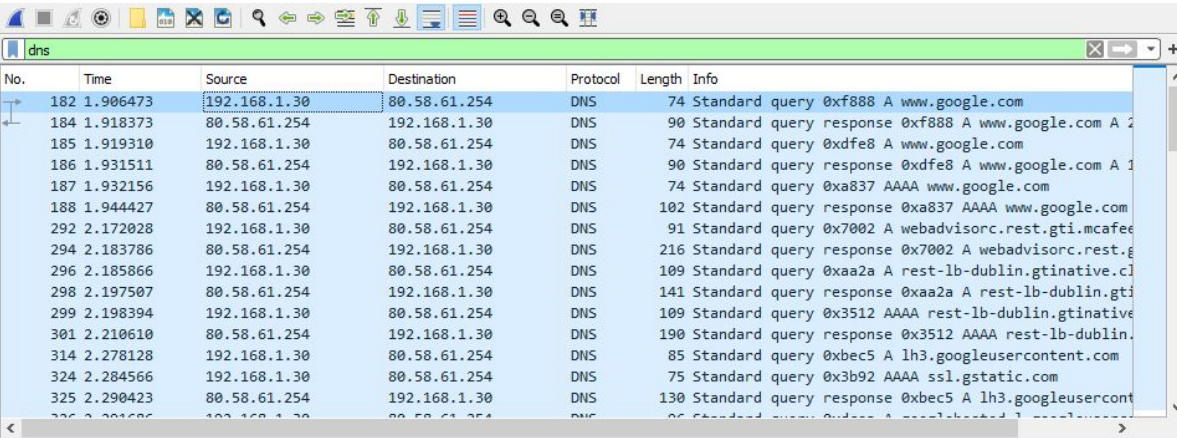
Capturar los datos.

Los datos fueron capturados en la traza adjunta a este documento.

Paso 2

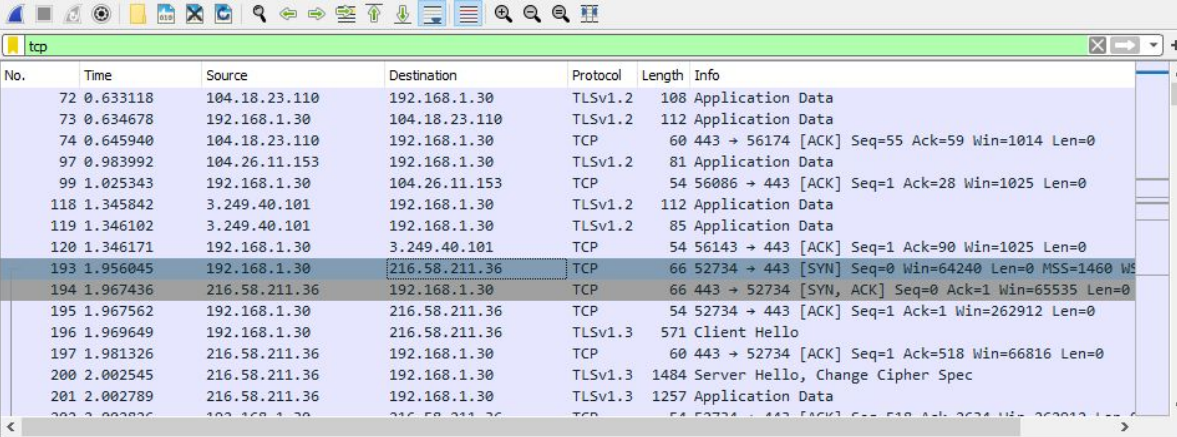
Iniciar Wireshark y seleccionar la interfaz apropiada.

Consulta al dominio www.google.com.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|--|
| 182 | 1.906473 | 192.168.1.30 | 80.58.61.254 | DNS | 74 | Standard query 0xf888 A www.google.com |
| 184 | 1.918373 | 80.58.61.254 | 192.168.1.30 | DNS | 90 | Standard query response 0xf888 A www.google.com A 2 |
| 185 | 1.919310 | 192.168.1.30 | 80.58.61.254 | DNS | 74 | Standard query 0xdfe8 A www.google.com |
| 186 | 1.931511 | 80.58.61.254 | 192.168.1.30 | DNS | 90 | Standard query response 0xdfe8 A www.google.com A 1 |
| 187 | 1.932156 | 192.168.1.30 | 80.58.61.254 | DNS | 74 | Standard query 0xa837 AAAA www.google.com |
| 188 | 1.944427 | 80.58.61.254 | 192.168.1.30 | DNS | 102 | Standard query response 0xa837 AAAA www.google.com |
| 292 | 2.172028 | 192.168.1.30 | 80.58.61.254 | DNS | 91 | Standard query 0x7002 A webadvisorc.rest.gti.mcafee |
| 294 | 2.183786 | 80.58.61.254 | 192.168.1.30 | DNS | 216 | Standard query response 0x7002 A webadvisorc.rest.g |
| 296 | 2.185866 | 192.168.1.30 | 80.58.61.254 | DNS | 109 | Standard query 0xaa2a A rest-lb-dublin.gtinitiative.cl |
| 298 | 2.197507 | 80.58.61.254 | 192.168.1.30 | DNS | 141 | Standard query response 0xaa2a A rest-lb-dublin.gti |
| 299 | 2.198394 | 192.168.1.30 | 80.58.61.254 | DNS | 109 | Standard query 0x3512 AAAA rest-lb-dublin.gtinitiative |
| 301 | 2.210610 | 80.58.61.254 | 192.168.1.30 | DNS | 190 | Standard query response 0x3512 AAAA rest-lb-dublin. |
| 314 | 2.278128 | 192.168.1.30 | 80.58.61.254 | DNS | 85 | Standard query 0xbec5 A lh3.googleusercontent.com |
| 324 | 2.284566 | 192.168.1.30 | 80.58.61.254 | DNS | 75 | Standard query 0x3b92 AAAA ssl.gstatic.com |
| 325 | 2.290423 | 80.58.61.254 | 192.168.1.30 | DNS | 130 | Standard query response 0xbec5 A lh3.googleusercontent |

Dirección IP del servidor DNS que consultó el equipo: 80.58.61.254.

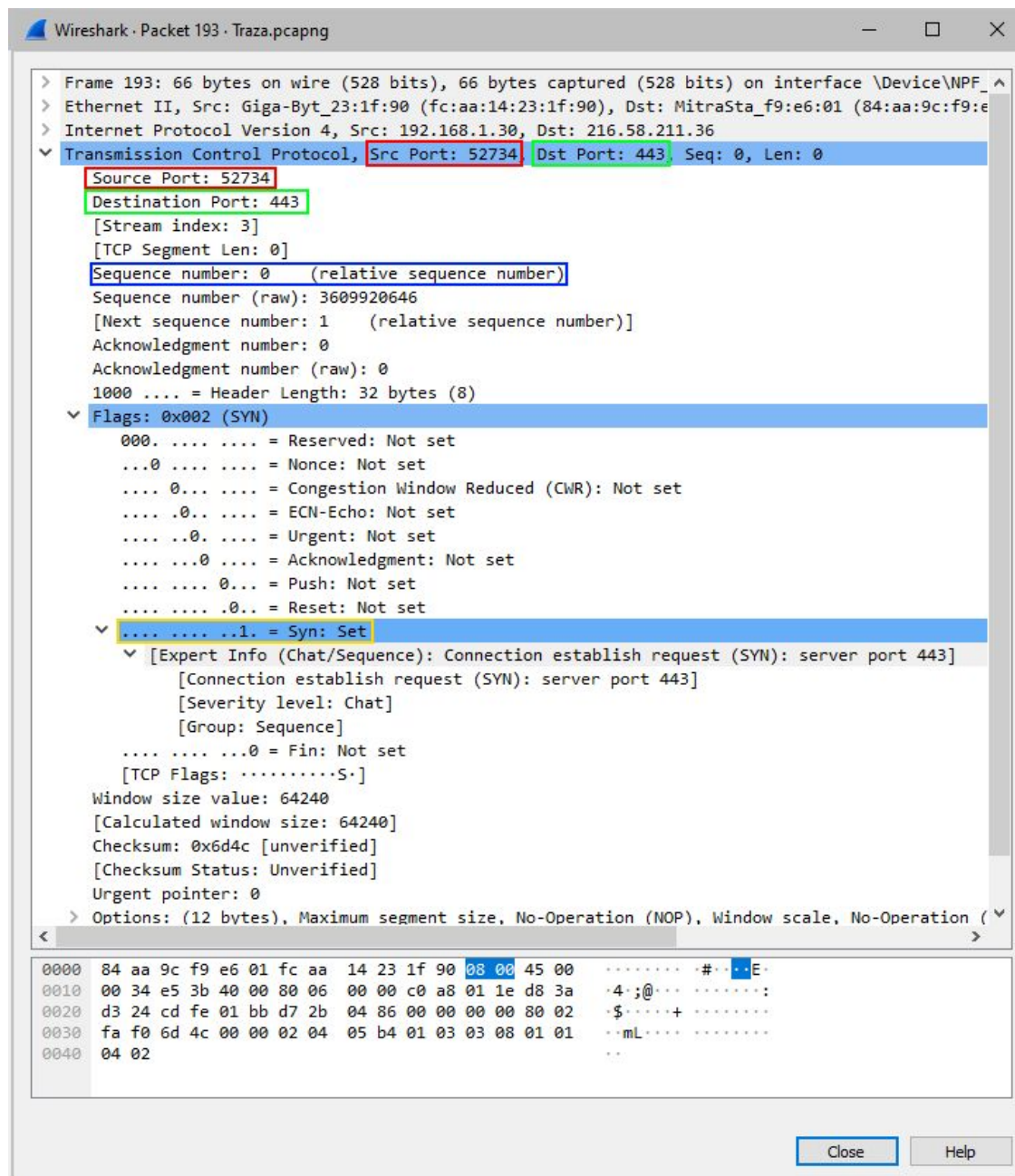


| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|---|
| 72 | 0.633118 | 104.18.23.110 | 192.168.1.30 | TLSv1.2 | 108 | Application Data |
| 73 | 0.634678 | 192.168.1.30 | 104.18.23.110 | TLSv1.2 | 112 | Application Data |
| 74 | 0.645940 | 104.18.23.110 | 192.168.1.30 | TCP | 60 | 443 → 56174 [ACK] Seq=55 Ack=59 Win=1014 Len=0 |
| 97 | 0.983992 | 104.26.11.153 | 192.168.1.30 | TLSv1.2 | 81 | Application Data |
| 99 | 1.025343 | 192.168.1.30 | 104.26.11.153 | TCP | 54 | 56086 → 443 [ACK] Seq=1 Ack=28 Win=1025 Len=0 |
| 118 | 1.345842 | 3.249.40.101 | 192.168.1.30 | TLSv1.2 | 112 | Application Data |
| 119 | 1.346102 | 3.249.40.101 | 192.168.1.30 | TLSv1.2 | 85 | Application Data |
| 120 | 1.346171 | 192.168.1.30 | 3.249.40.101 | TCP | 54 | 56143 → 443 [ACK] Seq=1 Ack=90 Win=1025 Len=0 |
| 193 | 1.956045 | 192.168.1.30 | 216.58.211.36 | TCP | 66 | 52734 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS |
| 194 | 1.967436 | 216.58.211.36 | 192.168.1.30 | TCP | 66 | 443 → 52734 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 |
| 195 | 1.967562 | 192.168.1.30 | 216.58.211.36 | TCP | 54 | 52734 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0 |
| 196 | 1.969649 | 192.168.1.30 | 216.58.211.36 | TLSv1.3 | 571 | Client Hello |
| 197 | 1.981326 | 216.58.211.36 | 192.168.1.30 | TCP | 60 | 443 → 52734 [ACK] Seq=1 Ack=518 Win=66816 Len=0 |
| 200 | 2.002545 | 216.58.211.36 | 192.168.1.30 | TLSv1.3 | 1484 | Server Hello, Change Cipher Spec |
| 201 | 2.002789 | 216.58.211.36 | 192.168.1.30 | TLSv1.3 | 1257 | Application Data |

Dirección IP del servidor web de Google: 216.58.211.36.

Paso 3

Examine la información dentro de los paquetes, incluidas las direcciones IP, los números de puerto TCP y los marcadores de control de TCP.



Abriendo la trama seleccionada de la imagen anterior, se obtiene esta ventana.

Puerto de origen: 52734.

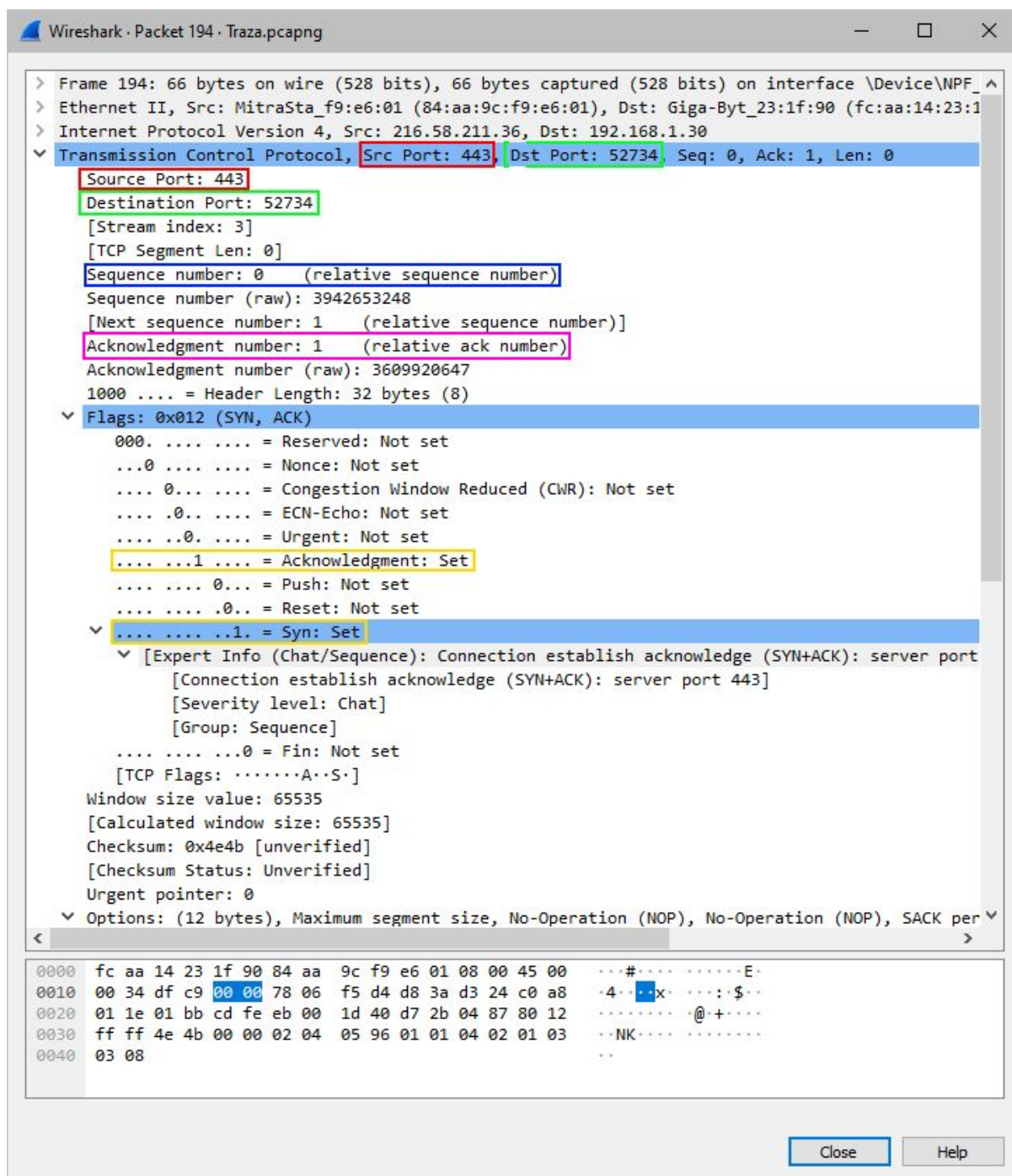
Clasificación: Dinámico / privado.

Puerto de destino: 443.

Clasificación: Conocido, registrado.

Marcadores establecidos: SYN.

Número de secuencia relativa: 0.



Información de la trama siguiente a la anterior.

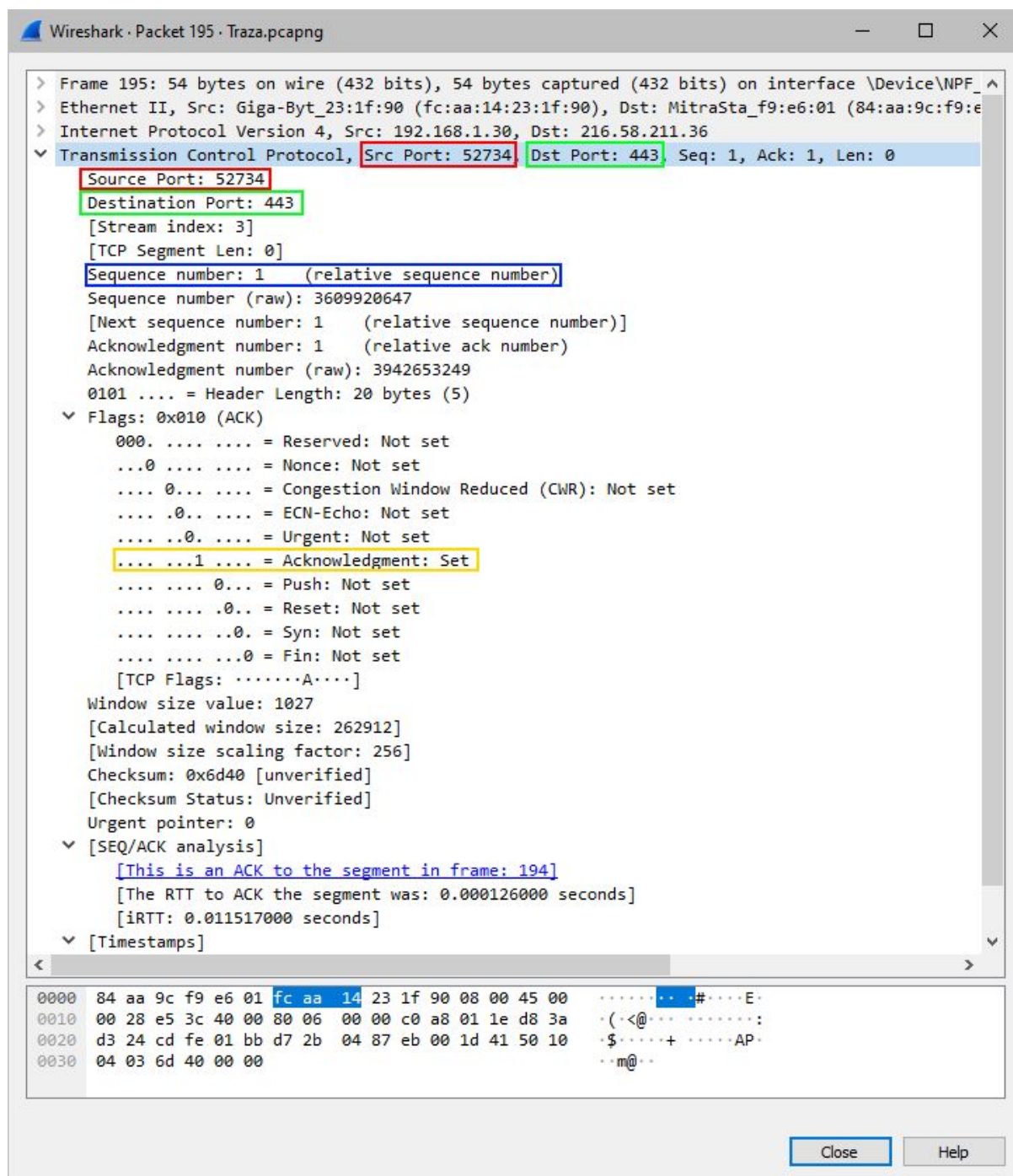
Puerto de origen: 443.

Número de secuencia relativa: 0.

Puerto de destino: 52734.

Número de reconocimiento relativo: 1.

Marcadores establecidos: SYN y ACK.



Marcador establecido: ACK.

Reflexión

Hay cientos de filtros disponibles en Wireshark. Una red grande podría tener numerosos filtros y muchos tipos diferentes de tráfico. Mencione tres filtros que podrían ser útiles para un administrador de redes.

tcp, dns, http.

¿Qué otros usos se le podrían dar a Wireshark en una red de producción?

Wireshark se utiliza generalmente para fines de seguridad, en el análisis a posteriori del tráfico normal o después de un ataque a la red. Es posible que deban capturarse nuevos protocolos o servicios para determinar cuáles puertos se utilizan.