Análisis del protocolo TCP de enlace de tres vías: paso 1

Mediante el resultado del software de análisis de protocolos, como los resultados de Wireshark, se puede examinar la operación del protocolo TCP de enlace de tres vías:

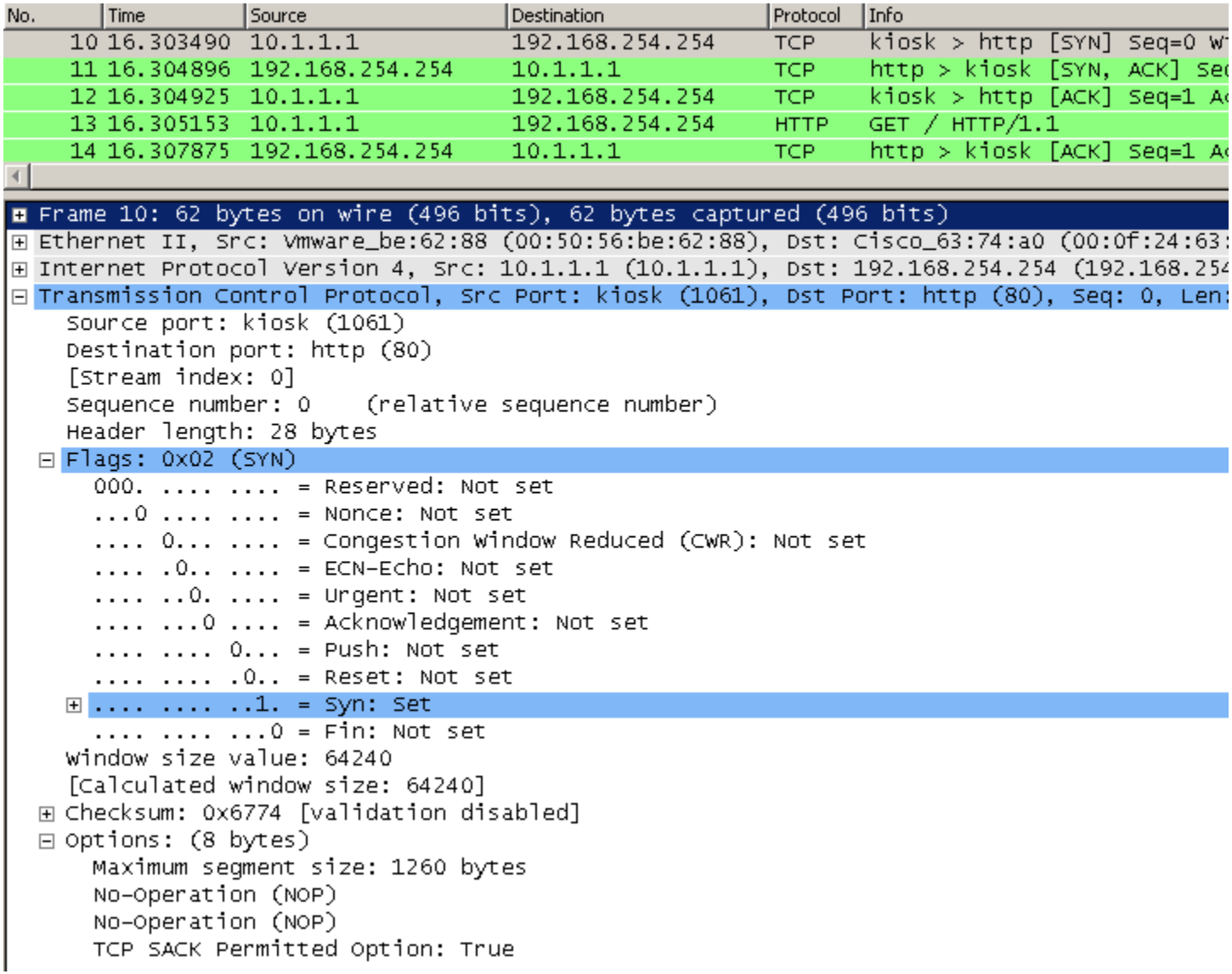
Paso 1: el cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.

Un cliente TCP inicia un protocolo de enlace de tres vías al enviar un segmento con el indicador de control de sincronizar números de secuencia (SYN) establecido, lo que indica un valor inicial en el campo de número de secuencia en el encabezado. Este valor inicial para el número de secuencia, conocido como número de secuencia inicial (ISN), se elige de manera aleatoria y se utiliza para comenzar a rastrear el flujo de datos de esta sesión desde el cliente hasta el servidor. El ISN en el encabezado de cada segmento se incrementa en uno por cada byte de datos enviados desde el cliente hacia el servidor mientras continúa la conversación de datos.

Como se muestra en la figura 1, el resultado de un analizador de protocolos muestra el señalizador de control SYN y el número de secuencia relativa.

El indicador de control SYN está establecido y el número de secuencia relativa está en 0. Aunque el analizador de protocolos en el gráfico indique los valores relativos para los números de secuencia y de acuse de recibo, los verdaderos valores son números binarios de 32 bits. En la ilustración, se muestran los cuatro bytes representados en un valor hexadecimal.

Figura 1: Protocolo TCP de enlace de tres vías (SYN)



Análisis del protocolo TCP de enlace de tres vías: paso 2

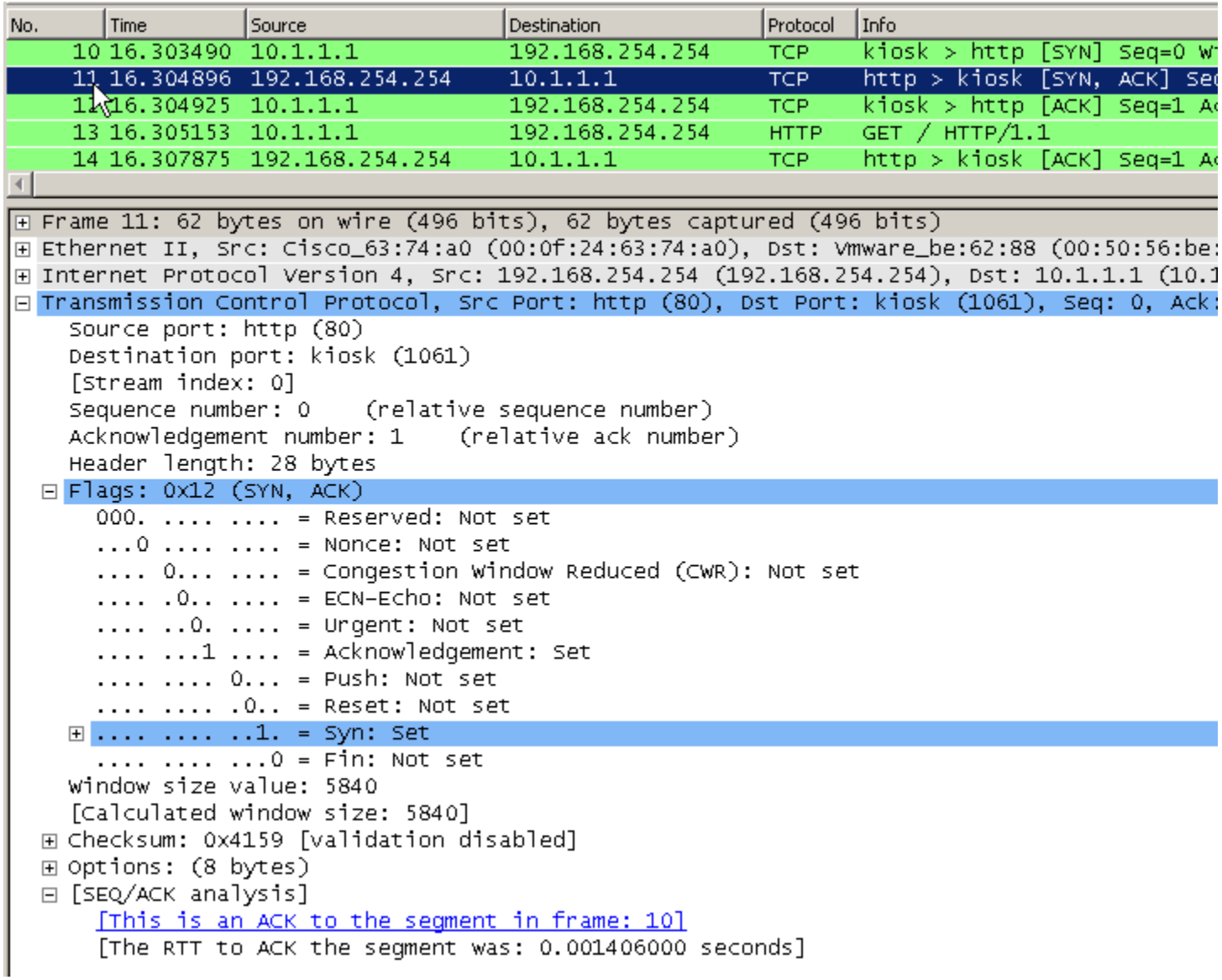
Paso 2: el servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.

El servidor TCP debe dar acuse de recibo del segmento SYN del cliente para establecer la sesión de cliente a servidor. Para hacerlo, el servidor envía un segmento al cliente con el indicador de acuse de recibo (ACK) establecido que indica que el número de acuse de recibo es significativo. Con este señalizador establecido en el segmento, el cliente interpreta esto como acuse de recibo de que el servidor ha recibido el SYN del cliente TCP.

El valor del campo de número de acuse de recibo es igual al ISN más 1. Esto establece una sesión del cliente al servidor. El indicador ACK permanece establecido para mantener el equilibrio de la sesión. Recuerde que la conversación entre el cliente y el servidor son, en realidad, dos sesiones unidireccionales: una del cliente al servidor y otra del servidor al cliente. En este segundo paso del protocolo de enlace de tres vías, el servidor debe iniciar la respuesta al cliente. Para comenzar esta sesión, el servidor utiliza el señalizador SYN de la misma manera en que lo hizo el cliente. Establece el señalizador de control SYN en el encabezado para establecer una sesión del servidor al cliente. El señalizador SYN indica que el valor inicial del campo de número de secuencia se encuentra en el encabezado. Este valor se utiliza para hacer un seguimiento del flujo de datos en esta sesión del servidor al cliente.

Como se muestra en la figura 2, el resultado del analizador de protocolos muestra que se establecieron los indicadores de control ACK y SYN, y que se muestran los números de reconocimiento y de secuencia relativa.

Figura 2: Protocolo TCP de enlace de tres vías (SYN, ACK)



Análisis del protocolo TCP de enlace de tres vías: paso 3

Paso 3: el cliente de origen reconoce la sesión de comunicación de servidor a cliente.

Por último, el cliente TCP responde con un segmento que contiene un ACK que actúa como respuesta al SYN de TCP enviado por el servidor. No existen datos de usuario en este segmento. El valor del campo de número de acuse de recibo contiene uno más que el ISN recibido del servidor. Una vez que se establecen ambas sesiones entre el cliente y el servidor, todos los segmentos adicionales que se intercambian en esta comunicación tendrán establecido el indicador ACK.

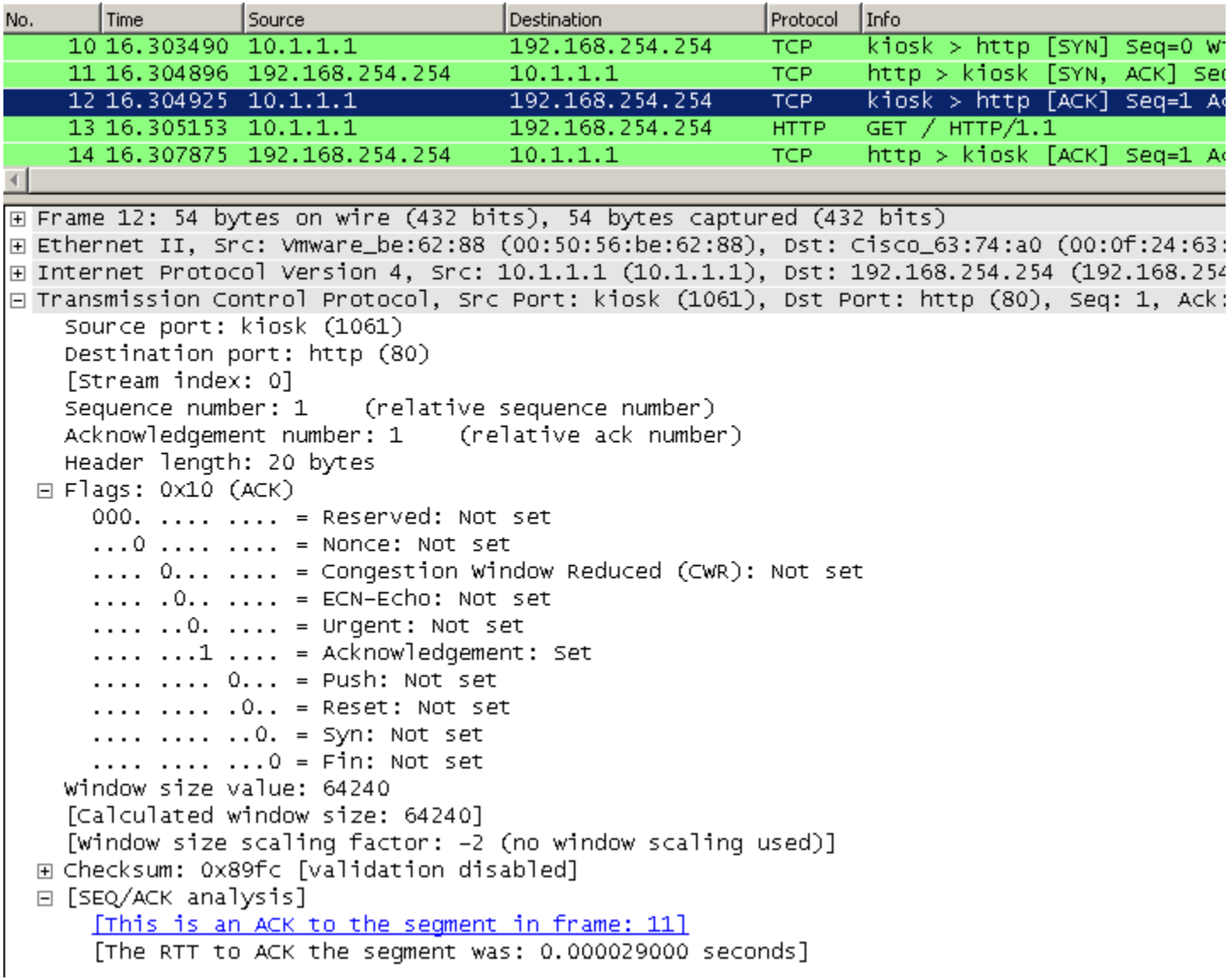
Como se muestra en la figura 3, el resultado del analizador de protocolos muestra el indicador de control ACK establecido y los números de reconocimiento y de secuencia relativa.

Se puede añadir seguridad a la red de datos de la siguiente manera:

- Denegar el establecimiento de sesiones del TCP
- Permitir sólo sesiones que se establezcan para servicios específicos
- Permitir sólo tráfico como parte de sesiones ya establecidas

Estas medidas de seguridad se pueden implementar para todas las sesiones TCP o solo para las sesiones seleccionadas.

Figura 3: Protocolo TCP de enlace de tres vías (ACK)



No.	Time	Source	Destination	Protocol	Info
10	16.303490	10.1.1.1	192.168.254.254	TCP	kiosk > http [SYN] Seq=0 W
11	16.304896	192.168.254.254	10.1.1.1	TCP	http > kiosk [SYN, ACK] Se
12	16.304925	10.1.1.1	192.168.254.254	TCP	kiosk > http [ACK] Seq=1 A
13	16.305153	10.1.1.1	192.168.254.254	HTTP	GET / HTTP/1.1
14	16.307875	192.168.254.254	10.1.1.1	TCP	http > kiosk [ACK] Seq=1 A

```
⊞ Frame 12: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Vmware_be:62:88 (00:50:56:be:62:88), Dst: Cisco_63:74:a0 (00:0f:24:63:
⊞ Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254
⊟ Transmission Control Protocol, Src Port: kiosk (1061), Dst Port: http (80), Seq: 1, Ack:
    Source port: kiosk (1061)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
  ⊞ Checksum: 0x89fc [validation disabled]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 11]
      [The RTT to ACK the segment was: 0.000029000 seconds]
```

Análisis de terminación de sesión TCP

Para cerrar una conexión, se debe establecer el marcador de control de finalización (FIN) en el encabezado del segmento. Para finalizar todas las sesiones TCP de una vía, se utiliza un enlace de dos vías, que consta de un segmento FIN y un segmento ACK. Por lo tanto, para terminar una única conversación que admite TCP, se requieren cuatro intercambios para finalizar ambas sesiones, como se muestra en la figura 1.

Nota: En esta explicación, los términos “cliente” y “servidor” se utilizan como referencia con fines de simplificación, pero el proceso de finalización puede ser iniciado por dos hosts cualesquiera que tengan una sesión abierta:

Paso 1: cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el marcador FIN establecido.

Paso 2: el servidor envía un ACK para reconocer el marcador FIN y terminar la sesión de cliente a servidor.

Paso 3: el servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.

Paso 4: el cliente responde con un ACK para reconocer el recibo del FIN desde el servidor.

Cuando el cliente no tiene más datos que transferir, establece el indicador FIN en el encabezado de un segmento. A continuación, el extremo servidor de la conexión envía un segmento normal que contiene datos con el indicador ACK establecido utilizando el número de acuse de recibo, lo que confirma que se recibieron todos los bytes de datos. Una vez reconocidos todos los segmentos, la sesión se cierra.

La sesión en la otra dirección se cierra con el mismo proceso. El receptor indica que no existen más datos para enviar estableciendo el señalizador FIN en el encabezado del segmento enviado al origen. Un acuse de recibo devuelto confirma que todos los bytes de datos se recibieron y que la sesión, a su vez, finalizó.

Consulte las figuras 4 y 5 para ver los indicadores de control FIN y ACK establecidos en el encabezado del segmento, lo que finaliza la sesión HTTP.

También es posible terminar la conexión por medio de un enlace de tres vías. Cuando el cliente no posee más datos para enviar, envía un señalizador FIN al servidor. Si el servidor tampoco tiene más datos para enviar, puede responder con los señalizadores FIN y ACK, combinando dos pasos en uno. A continuación, el cliente responde con un ACK.

Figura 4: Finalización de la sesión de TCP (FIN)

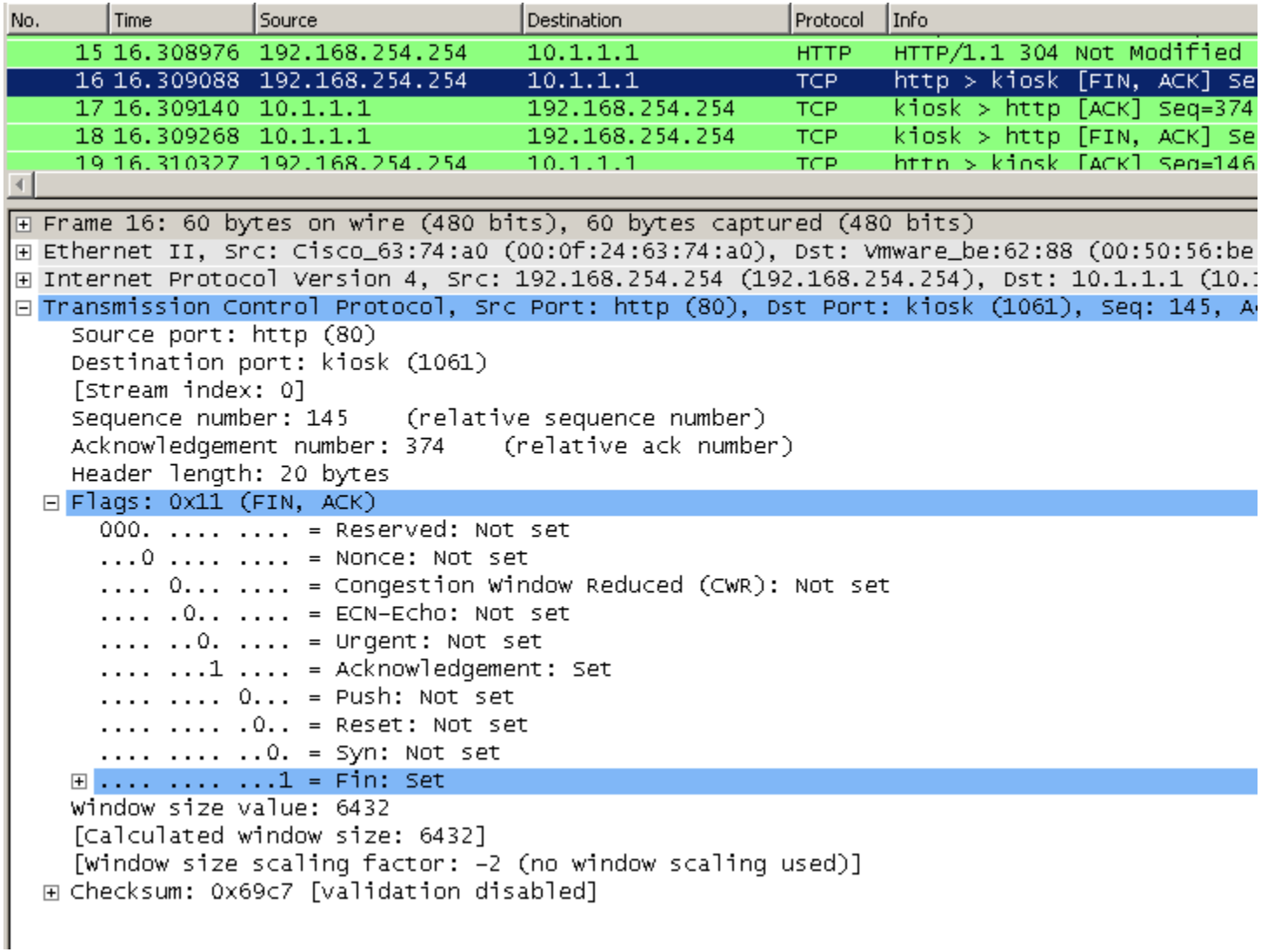
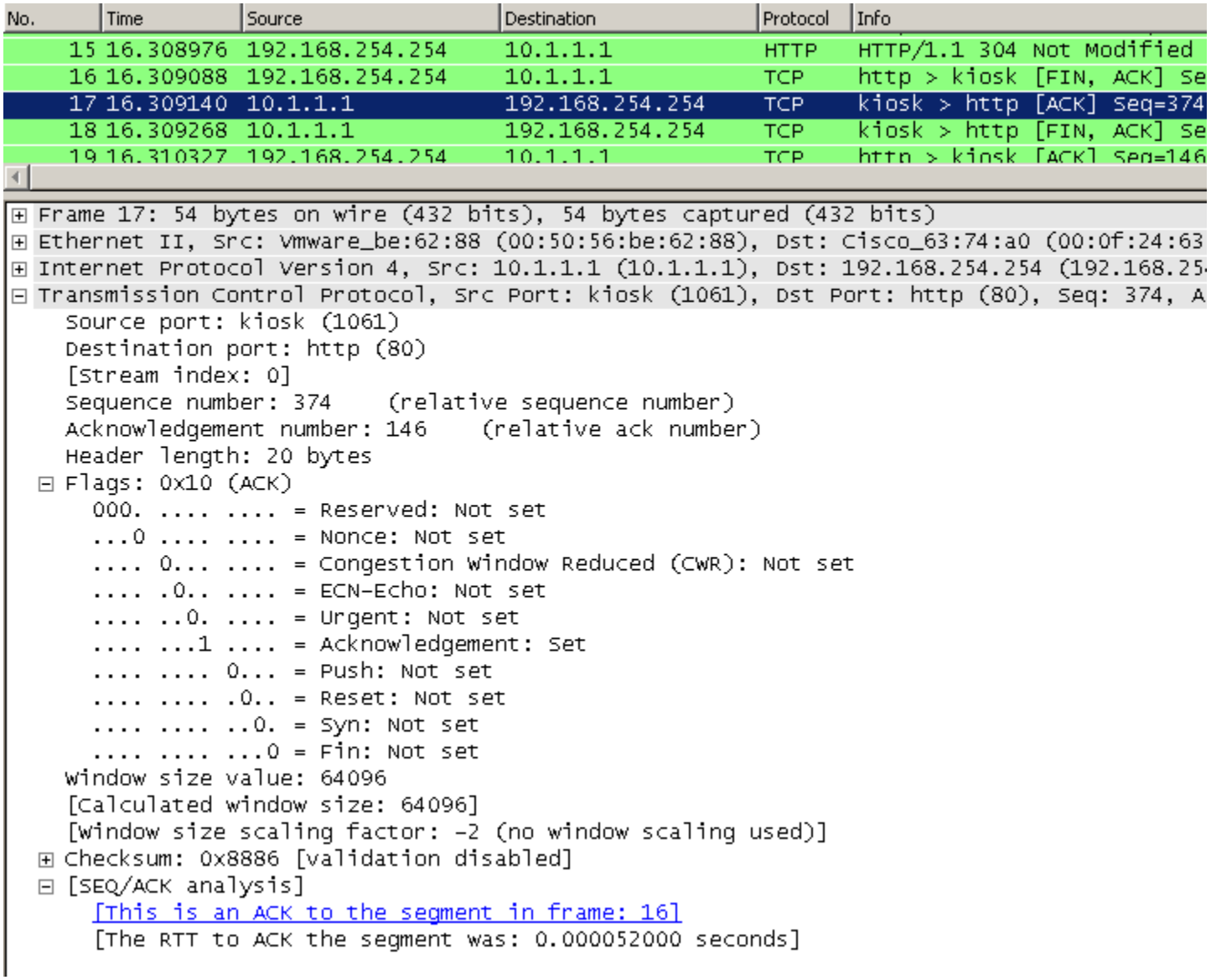


Figura 5: Finalización de la sesión de TCP (ACK)



No.	Time	Source	Destination	Protocol	Info
15	16.308976	192.168.254.254	10.1.1.1	HTTP	HTTP/1.1 304 Not Modified
16	16.309088	192.168.254.254	10.1.1.1	TCP	http > kiosk [FIN, ACK] Se
17	16.309140	10.1.1.1	192.168.254.254	TCP	kiosk > http [ACK] Seq=374
18	16.309268	10.1.1.1	192.168.254.254	TCP	kiosk > http [FIN, ACK] Se
19	16.310327	192.168.254.254	10.1.1.1	TCP	http > kiosk [ACK] Seq=146

```
⊞ Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Vmware_be:62:88 (00:50:56:be:62:88), Dst: Cisco_63:74:a0 (00:0f:24:63
⊞ Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.25
⊟ Transmission Control Protocol, Src Port: kiosk (1061), Dst Port: http (80), Seq: 374, A
    Source port: kiosk (1061)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 374    (relative sequence number)
    Acknowledgement number: 146    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgement: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    Window size value: 64096
    [Calculated window size: 64096]
    [Window size scaling factor: -2 (no window scaling used)]
  ⊞ Checksum: 0x8886 [validation disabled]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 16]
      [The RTT to ACK the segment was: 0.000052000 seconds]
```