Wireshark: Análisis de gráficas de "tcptrace" de conexiones TCP

Arquitectura de Redes de Ordenadores
Arquitectura de Internet

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Abril 2016

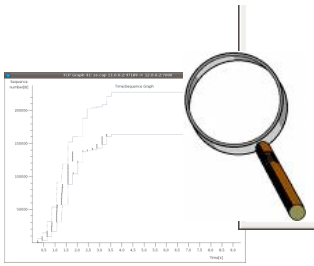
Gráfica de *tcptrace* dentro de Wireshark

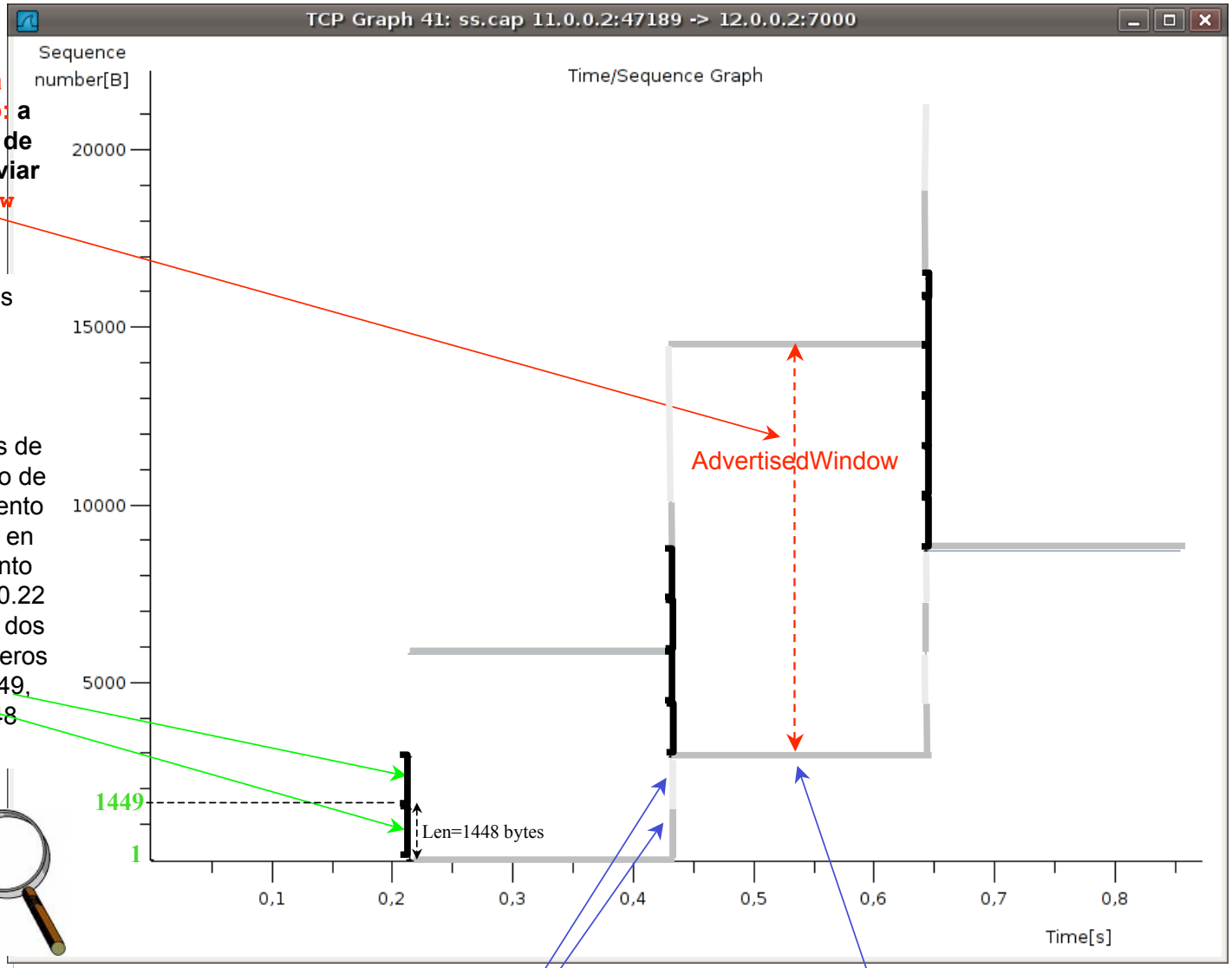
- En Wireshark, además de mirar el contenido de los paquetes de una conexión TCP, puede verse en una gráfica la **evolución del envío de datos y recepción de acks respecto al tiempo**.
- Wireshark permite mostrar varios tipos de gráficas de una conexión TCP: Nosotros utilizaremos la gráfica de *tcptrace*.
- Como una conexión TCP permite el envío de datos en ambos sentidos, se pueden visualizar 2 gráficas de *tcptrace* diferentes: las correspondientes a cada sentido de la comunicación.
- Para ver en Wireshark la gráfica de *tcptrace* de uno de los sentidos de una conexión TCP es necesario:
  - Cargar el fichero de una captura que contenga los paquetes de una conexión TCP.
  - Seleccionar un segmento de la conexión del sentido de la comunicación que queremos analizar (si el segmento seleccionado va del proceso A al proceso B, la gráfica que se mostrará será la correspondiente al envío de datos de A a B).
  - Seleccionar en el menú de Wireshark:
    Statistics→TCP Stream Graph→Time-Sequence Graph (tcptrace)

Ejemplo

Ventana anunciada por el otro extremo: a partir del último nº de ACK se pueden enviar `AdvertisedWindow` bytes

Segmentos verticales negros: **segmentos TCP de datos enviados**. Cada segmento ocupa un conjunto de números de secuencia: el número de secuencia del segmento TCP más la longitud en bytes de ese segmento TCP. En el instante 0.22 segundos se envían dos segmentos con números de secuencia 1 y 1449, cuya longitud es 1448 bytes.





Segmentos verticales grises: **segmentos TCP de ACK** recibidos

Línea inferior gris claro: **último nº de ACK recibido**

Acciones sobre la gráfica *tcptrace*

- **Click central**: zoom in
- **MAYS + Click central**: zoom out
- **Arrastrar con el botón derecho**: desplazar el gráfico (útil si se ha hecho "zoom in")
- **ESPACIO**: activa/desactiva una cruz para ayudar a ver sobre los ejes la posición del ratón.
- **Click izquierdo sobre un segmento**: seleccionar el paquete concreto en la lista de paquetes de Wireshark.
- **CTRL + arrastrar con el botón derecho**: lupa
- **s**: Alterna entre números de secuencia relativos y absolutos, sólo si está desactivada la opción Edit→Preferences→Protocols→TCP→Relative sequence numbers and window scaling.