Capitulo 29

Encuentre las principales causas de rendimiento

01

Solucionar

problemas de rendimiento

Una de las metodologías de resolución de problemas más populares comienza en la capa física y avanza hasta la capa de aplicación en orden ascendente.

Cuando un usuario se queja de un rendimiento deficiente, los síntomas pueden ser:

- Tiempo de carga de la aplicación lento.
- Archivo lento.
- Tiempo de transferencia.
- Imposibilidad de conectarse a servicios específicos, etc.

También pueden surgir problemas en el proceso de resolución

Por ejemplo, los problemas de DNS pueden evitar que un host obtenga la dirección IP de un host de destino.

- Los valores incorrectos de la máscara de subred pueden causar un host para realizar el descubrimiento de un host local que es, de hecho, remoto.
- Valores incorrectos de la tabla de ruta o no disponible las puertas de enlace pueden aislar un host.
- Las líneas de base de las comunicaciones de red normales se pueden comparar con comunicaciones defectuosas para localizar diferencias y detectar rápidamente el origen de los problemas.

02

Identificar

tiempos de alta latencia

Los tiempos de latencia altos pueden deberse a la distancia (como en el caso de las comunicaciones por satélite), retrasos en las colas a lo largo de una ruta, retrasos en el procesamiento, etc.

Una de las formas más sencillas de identificar retrasos en un archivo de seguimiento es establecer la columna Tiempo en Segundos desde el anterior.

Paquete mostrado, luego ordene esta columna y observe los grandes espacios de tiempo entre paquetes en el archivo de seguimiento como se muestra en la Figura 340.

Filtrar una conversación antes de ordenar la columna de tiempo

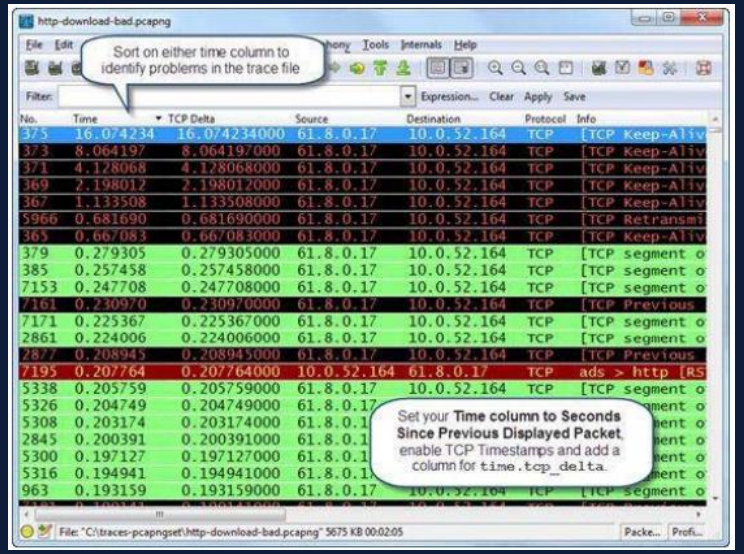


Figura 340. Ordenar en la columna tiempo después de filtrar en una conversación

Si su rastro contiene numerosas conversaciones, asegúrese de filtrar una conversación antes de ordenar el tiempo columna para asegurarse de que está comparando tiempos dentro de una sola conversación.

Alternativamente, puede agregar una columna para Delta Time (conversación) para identificar grandes espacios de tiempo entre paquetes en una conversación. Crea esta columna a través de Preferencias | Columnas

También puede ver numerosos valores de tiempo dentro de la sección Marco. Aunque estos valores no son campos reales en el paquete, Wireshark puede encontrar paquetes en función de sus valores.

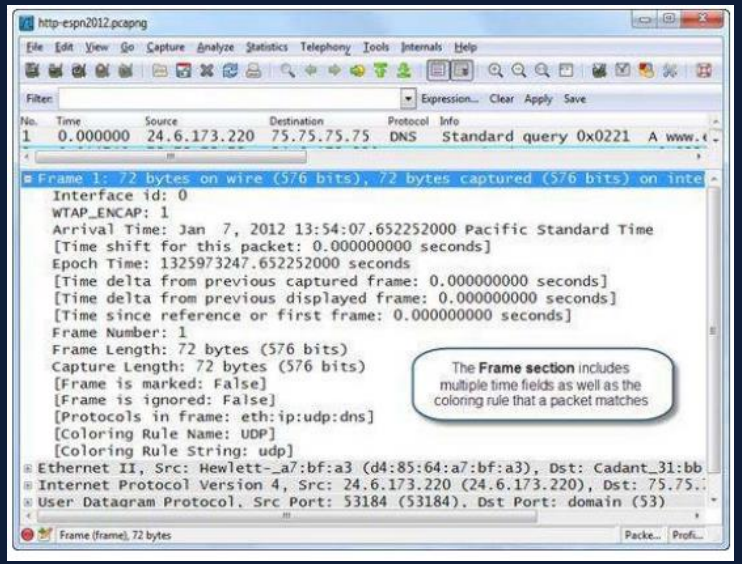


Figura 341. Expanda la sección Marco para ver detalles de tiempo

En la Figura 341 hemos expandido el Marco sección que precede a un encabezado de Ethernet II para ver los seis campos de tiempo enumerados en el mismo. La capacidad Time Shift fue agregado en Wireshark 1.8.

03

Filtrar

por horarios de llegada

El valor de Hora de llegada se basa en la hora del sistema en el momento en que se capturó el paquete.

La siguiente lista proporciona ejemplos de filtrado en la hora de llegada de los paquetes.

frame.time == "Mar 1, 2010 12:21:31.121493000"
frame.time < "Jan 15, 2010 00:00:00.000000000"
frame.time > "Jan 27, 2010 23:59:59.000000000"

04

Filtrar

por Delta Times

El delta de tiempo de la trama capturada anterior muestra cuándo llegó un paquete en comparación con el anterior, paquete capturado, independientemente de los filtros.

Por ejemplo, si filtró una comunicación HTTP, pero su seguimiento contiene consultas DNS antes del protocolo de enlace TCP con el servidor HTTP, el valor de tiempo del primer protocolo de enlace TCP paquete compararía el tiempo desde el final del paquete de respuesta DNS hasta el final del primer TCP paquete de handshake

La siguiente lista proporciona algunos ejemplos de filtrado en este valor de tiempo.

frame.time_delta==0.001536000
frame.time_delta < 0.001
frame.time_delta > 1

05

Filtrar

por el tiempo desde la referencia
o el primer paquete

Esta referencia de tiempo compara el tiempo actual del paquete con el primer paquete en el archivo de seguimiento o el más reciente, paquete que tiene la referencia de tiempo establecida.

La siguiente lista proporciona ejemplos de filtrado en este valor de tiempo.

frame.time_relative==0
frame.time_relative < 0.001
frame.time_relative > 1

El filtro de visualización frame.time_relative == 0 mostraría el primer paquete en el archivo de seguimiento y cualquier paquete marcado con una referencia de tiempo.

06

Filtrar

por tiempos de conversación TCP

Esta es una gran opción para detectar latencia en conversaciones TCP. No es necesario filtrar y separar los conversaciones.

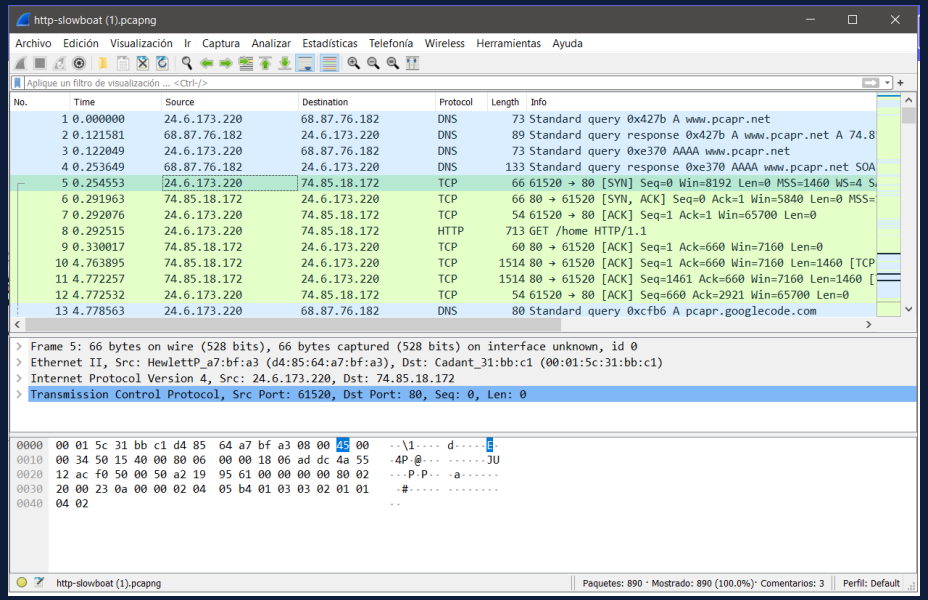
Ahora puede aplicar filtros basados en el valor del campo tcp.time_delta. Lo siguiente proporciona ejemplos de filtrado en este valor de tiempo.

06

Practica

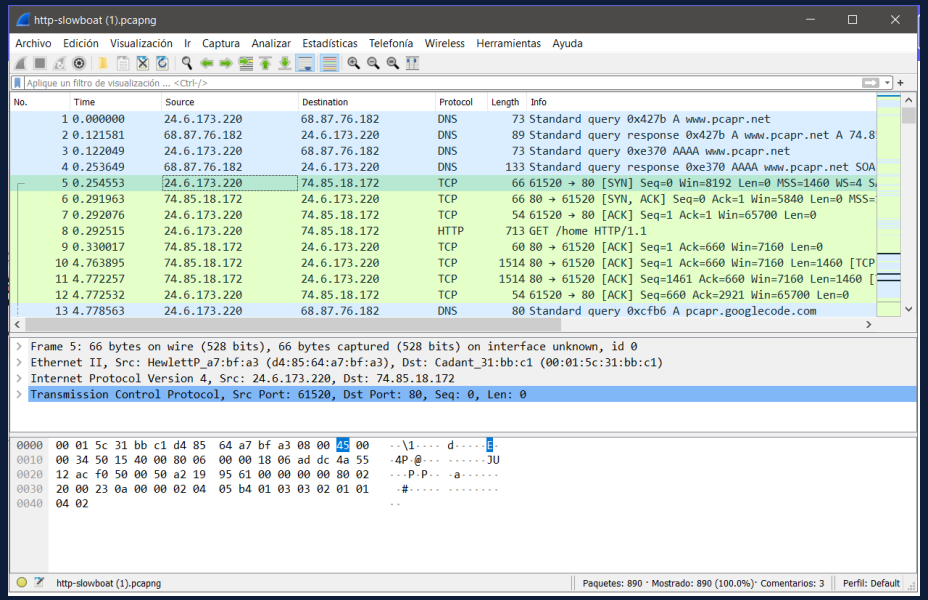
trabajando con problemas de tiempo

Paso 1



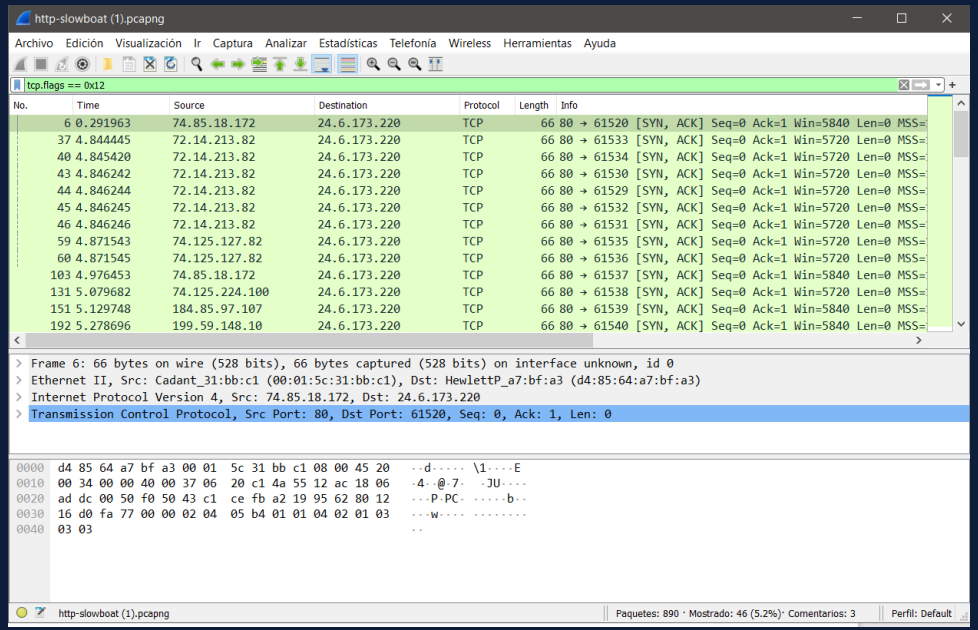
En primer lugar, céntrese en los tiempos de latencia de ida y vuelta de TCP en los handshake de TCP. Aplicar un filtro para tcp.flags == 0x12 (Paquetes SYN / ACK)

Paso 2



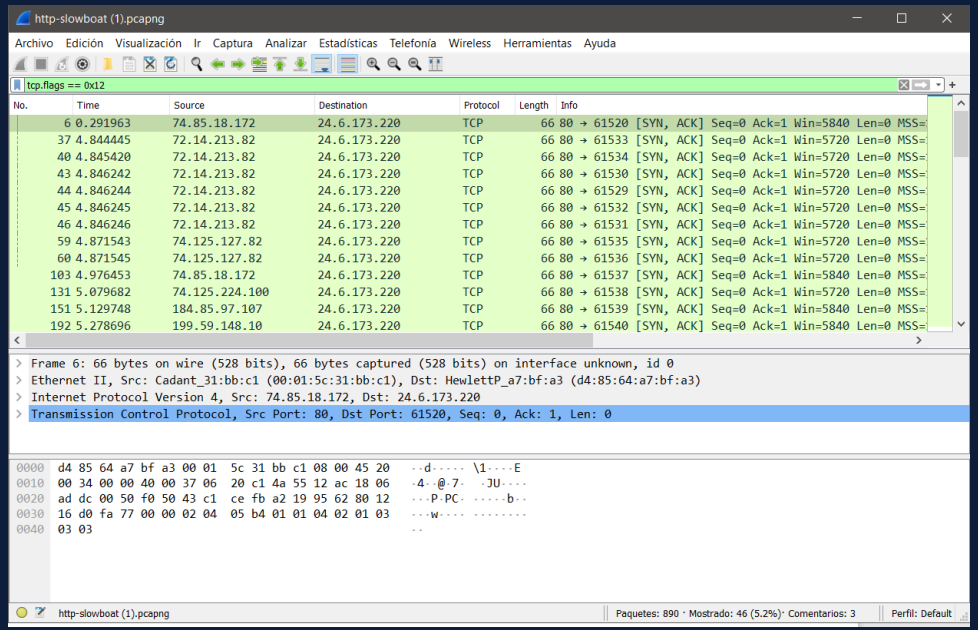
Haga clic con el botón derecho en un encabezado TCP en el panel Detalles del paquete y habilite Calcular marcas de tiempo de conversación.

Paso 3



Aplique una columna para el tiempo desde el fotograma anterior en esta secuencia de TCP (tcp.time_delta). Ordenar esta columna para familiarícese con los tiempos de latencia de ida y vuelta de las conexiones TCP.

Paso 4



Quite su filtro y haga clic dos veces en la columna TCP Delta para ordenar de mayor a menor.

Esto le permite ver las principales demoras entre paquetes en cada secuencia TCP separada. Ahora es el momento de considere lo que quiere solucionar y lo que NO quiere solucionar.

¡Gracias por su atención!