

Capítulo 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

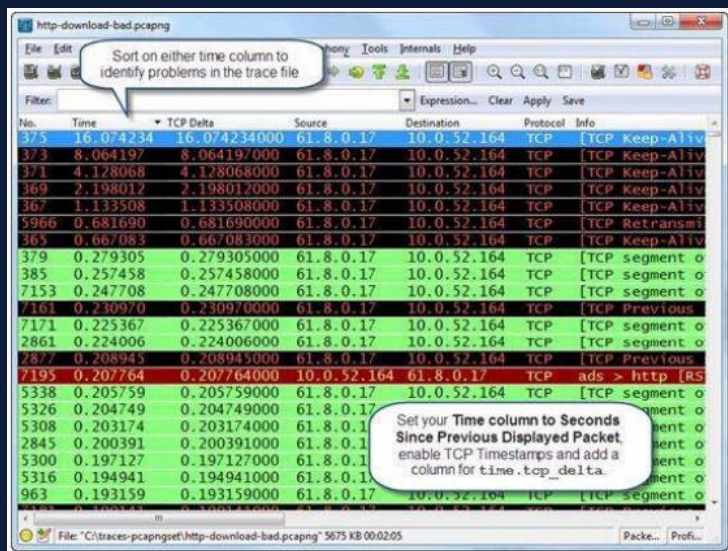


Figura 340. Ordenar en la columna tiempo después de filtrar en una conversación

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.

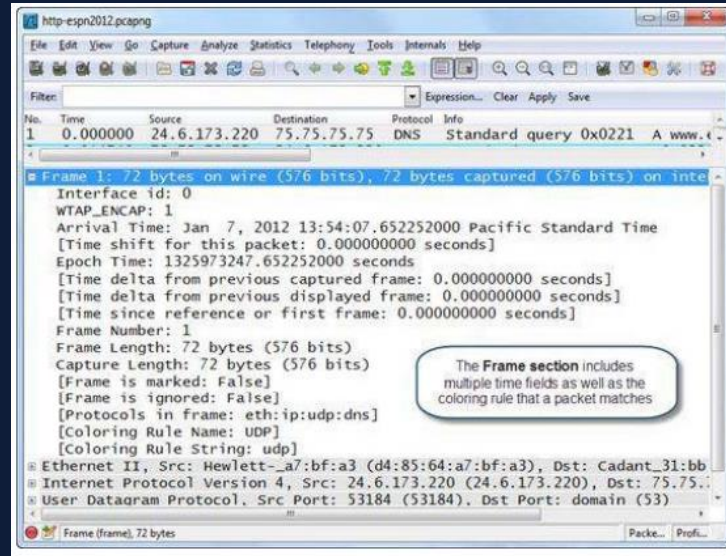


Figura 341. Expanda la sección Marco para ver detalles de tiempo

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 las conversaciones.

Seleccione Editar



Preferencias

Protocolos TCP



Habilite Calcular conversación Marcas de tiempo.

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

http-slowboat (1).pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	68.87.76.182	DNS	73	Standard query 0x427b A www.pcapr.net
2	0.121581	68.87.76.182	24.6.173.220	DNS	89	Standard query response 0x427b A www.pcapr.net A 74.8
3	0.122049	24.6.173.220	68.87.76.182	DNS	73	Standard query 0xe370 AAAA www.pcapr.net
4	0.253649	68.87.76.182	24.6.173.220	DNS	133	Standard query response 0xe370 AAAA www.pcapr.net SOA
5	0.254553	24.6.173.220	74.85.18.172	TCP	66	61520 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
6	0.291963	74.85.18.172	24.6.173.220	TCP	66	80 → 61520 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
7	0.292076	24.6.173.220	74.85.18.172	TCP	54	61520 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	0.292515	24.6.173.220	74.85.18.172	HTTP	713	GET /home HTTP/1.1
9	0.330017	74.85.18.172	24.6.173.220	TCP	60	80 → 61520 [ACK] Seq=1 Ack=660 Win=7160 Len=0
10	4.736895	74.85.18.172	24.6.173.220	TCP	1514	80 → 61520 [ACK] Seq=1 Ack=660 Win=7160 Len=1460 [TCP
11	4.772257	74.85.18.172	24.6.173.220	TCP	1514	80 → 61520 [ACK] Seq=1461 Ack=660 Win=7160 Len=1460 [
12	4.772532	24.6.173.220	74.85.18.172	TCP	54	61520 → 80 [ACK] Seq=660 Ack=2921 Win=65700 Len=0
13	4.778563	24.6.173.220	68.87.76.182	DNS	80	Standard query 0xcfb6 A pcapr.googlecode.com

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.85.18.172
> Transmission Control Protocol, Src Port: 61520, Dst Port: 80, Seq: 0, Len: 0

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ...1.... d....
0010 00 34 50 15 40 00 00 00 00 18 06 ad dc 4a 55 ...4P@.....JU
0020 12 ac f0 50 00 50 a2 19 95 61 00 00 00 00 00 02 ...P.P...a....
0030 20 00 23 0a 00 00 02 04 05 b4 01 03 03 02 01 01 ...#.....
0040 04 02

http-slowboat (1).pcapng Paquetes: 890 · Mostrado: 890 (100.0%) Comentarios: 3 Perfil: Default

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

http-slowboat (1).pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.173.220	68.87.76.182	DNS	73	Standard query 0x427b A www.pcapr.net
2	0.121581	68.87.76.182	24.6.173.220	DNS	89	Standard query response 0x427b A www.pcapr.net A 74.8
3	0.122049	24.6.173.220	68.87.76.182	DNS	73	Standard query 0xe370 AAAA www.pcapr.net
4	0.253649	68.87.76.182	24.6.173.220	DNS	133	Standard query response 0xe370 AAAA www.pcapr.net SOA
5	0.254553	24.6.173.220	74.85.18.172	TCP	66	61520 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
6	0.291963	74.85.18.172	24.6.173.220	TCP	66	80 → 61520 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
7	0.292076	24.6.173.220	74.85.18.172	TCP	54	61520 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	0.292515	24.6.173.220	74.85.18.172	HTTP	713	GET /home HTTP/1.1
9	0.330017	74.85.18.172	24.6.173.220	TCP	60	80 → 61520 [ACK] Seq=1 Ack=660 Win=7160 Len=0
10	4.763895	74.85.18.172	24.6.173.220	TCP	1514	80 → 61520 [ACK] Seq=1 Ack=660 Win=7160 Len=1460 [TCP
11	4.772257	74.85.18.172	24.6.173.220	TCP	1514	80 → 61520 [ACK] Seq=1461 Ack=660 Win=7160 Len=1460 [
12	4.772532	24.6.173.220	74.85.18.172	TCP	54	61520 → 80 [ACK] Seq=660 Ack=2921 Win=65700 Len=0
13	4.778563	24.6.173.220	68.87.76.182	DNS	80	Standard query 0xcfb6 A pcapr.googlecode.com

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.85.18.172
> Transmission Control Protocol, Src Port: 61520, Dst Port: 80, Seq: 0, Len: 0

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ...1... d....
0010 00 34 50 15 40 00 00 00 00 18 06 ad dc 4a 55 ...4P@... ..JU
0020 12 ac f0 50 00 50 a2 19 95 61 00 00 00 00 02 ...P.P... a....
0030 20 00 23 0a 00 00 02 04 05 b4 01 03 03 02 01 01 ...#.....
0040 04 02

http-slowboat (1).pcapng Paquetes: 890 · Mostrado: 890 (100.0%) Comentarios: 3 Perfil: Default

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.

http-slowboat (1).pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.flags == 0x12

No.	Time	Source	Destination	Protocol	Length	Info
6	0.291963	74.85.18.172	24.6.173.220	TCP	66	80 → 61520 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
37	4.844445	72.14.213.82	24.6.173.220	TCP	66	80 → 61533 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
40	4.845420	72.14.213.82	24.6.173.220	TCP	66	80 → 61534 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
43	4.846242	72.14.213.82	24.6.173.220	TCP	66	80 → 61530 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
44	4.846244	72.14.213.82	24.6.173.220	TCP	66	80 → 61529 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
45	4.846245	72.14.213.82	24.6.173.220	TCP	66	80 → 61532 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
46	4.846246	72.14.213.82	24.6.173.220	TCP	66	80 → 61531 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
59	4.871543	74.125.127.82	24.6.173.220	TCP	66	80 → 61535 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
60	4.871545	74.125.127.82	24.6.173.220	TCP	66	80 → 61536 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
103	4.976453	74.85.18.172	24.6.173.220	TCP	66	80 → 61537 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
131	5.079682	74.125.224.100	24.6.173.220	TCP	66	80 → 61538 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
151	5.129748	184.85.97.107	24.6.173.220	TCP	66	80 → 61539 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
192	5.278696	199.59.148.10	24.6.173.220	TCP	66	80 → 61540 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=

> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
> Internet Protocol Version 4, Src: 74.85.18.172, Dst: 24.6.173.220
> Transmission Control Protocol, Src Port: 80, Dst Port: 61520, Seq: 0, Ack: 1, Len: 0

0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20 ..d....\1...E
0010 00 34 00 00 40 00 37 06 20 c1 4a 55 12 ac 18 06 -4-@7-3U...
0020 ad dc 00 50 f0 50 43 c1 ce fb a2 19 95 62 80 12 --P-PC-...b..
0030 16 d0 fa 77 00 00 02 04 05 b4 01 01 04 02 01 03 --w-...
0040 03 03 ..

Paquetes: 890 · Mostrado: 46 (5.2%) · Comentarios: 3 · Perfil: Default



Paso 4

http-slowboat (1).pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.flags == 0x12

No.	Time	Source	Destination	Protocol	Length	Info
6	0.291963	74.85.18.172	24.6.173.220	TCP	66	80 → 61520 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
37	4.844445	72.14.213.82	24.6.173.220	TCP	66	80 → 61533 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
40	4.845420	72.14.213.82	24.6.173.220	TCP	66	80 → 61534 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
43	4.846242	72.14.213.82	24.6.173.220	TCP	66	80 → 61530 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
44	4.846244	72.14.213.82	24.6.173.220	TCP	66	80 → 61529 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
45	4.846245	72.14.213.82	24.6.173.220	TCP	66	80 → 61532 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
46	4.846246	72.14.213.82	24.6.173.220	TCP	66	80 → 61531 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
59	4.871543	74.125.127.82	24.6.173.220	TCP	66	80 → 61535 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
60	4.871545	74.125.127.82	24.6.173.220	TCP	66	80 → 61536 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
103	4.976453	74.85.18.172	24.6.173.220	TCP	66	80 → 61537 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
131	5.079682	74.125.224.100	24.6.173.220	TCP	66	80 → 61538 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=
151	5.129748	184.85.97.107	24.6.173.220	TCP	66	80 → 61539 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
192	5.278696	199.59.148.10	24.6.173.220	TCP	66	80 → 61540 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=

> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
> Internet Protocol Version 4, Src: 74.85.18.172, Dst: 24.6.173.220
> Transmission Control Protocol, Src Port: 80, Dst Port: 61520, Seq: 0, Ack: 1, Len: 0

0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20 ..d....\1...E
0010 00 34 00 00 40 00 37 06 20 c1 4a 55 12 ac 18 06 -4-@7-3U...
0020 ad dc 00 50 f0 50 43 c1 ce fb a2 19 95 62 80 12 ...P.C....b..
0030 16 d0 fa 77 00 00 02 04 05 b4 01 01 04 02 01 03 ...w-.....
0040 03 03 ..

http-slowboat (1).pcapng Paquetes: 890 · Mostrado: 46 (5.2%) · Comentarios: 3 Perfil: Default

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.

The background is a solid dark blue. In the top right corner, there is a pink geometric shape that looks like a triangle pointing downwards. In the bottom left corner, there is an orange geometric shape that looks like a triangle pointing upwards.

**¡Gracias por
su atención!**