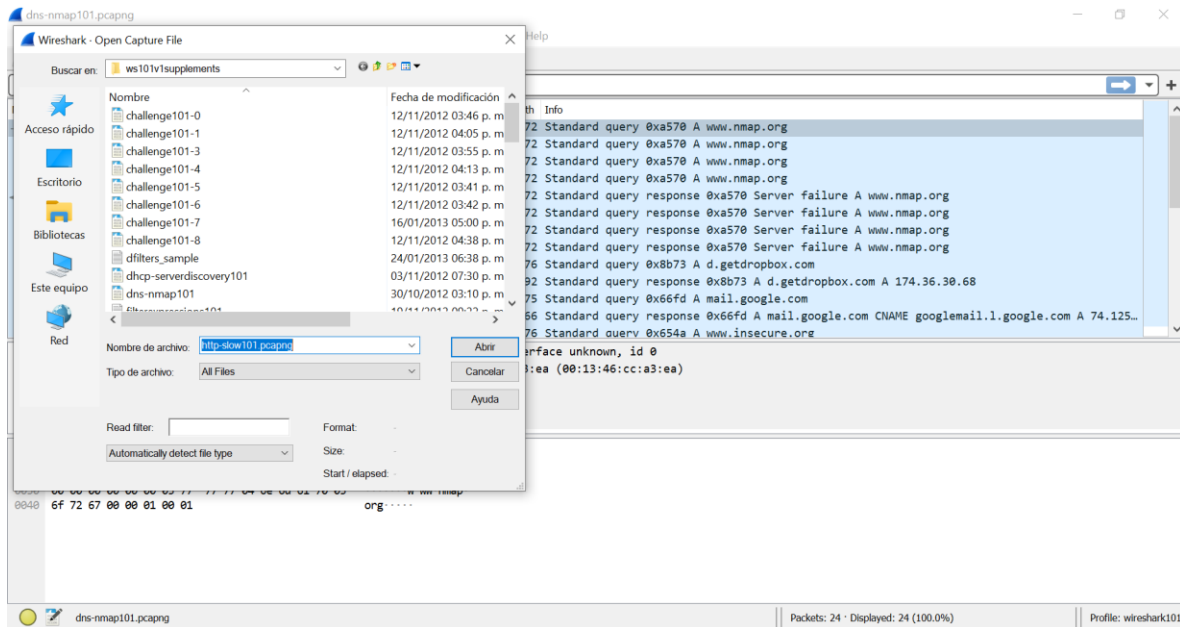
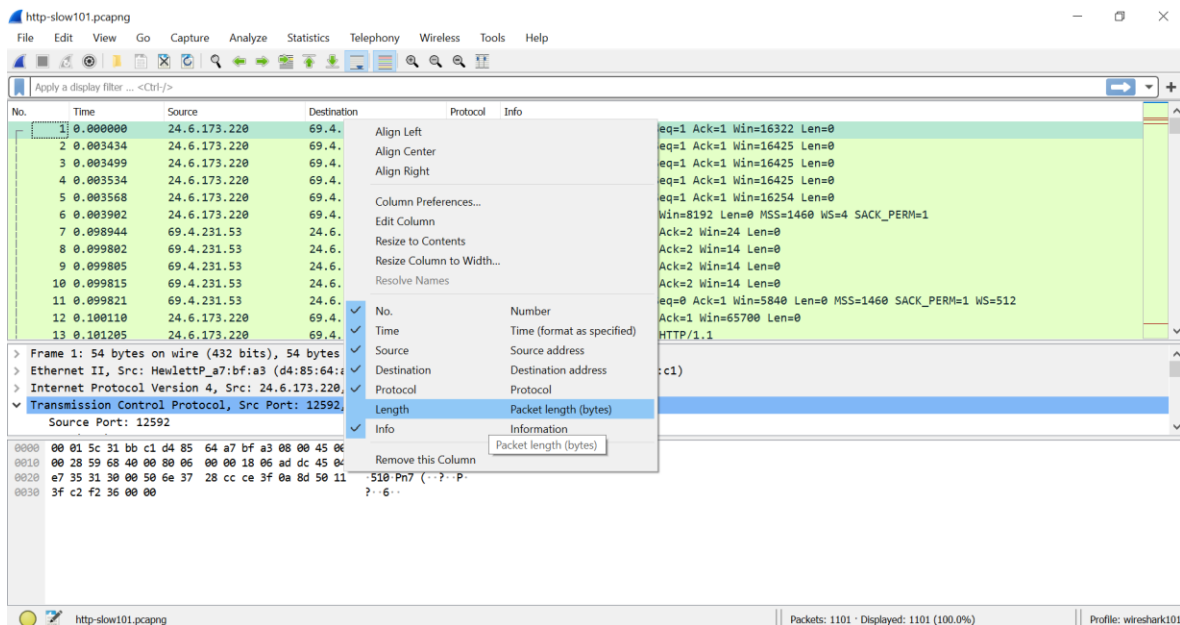


LAB 8

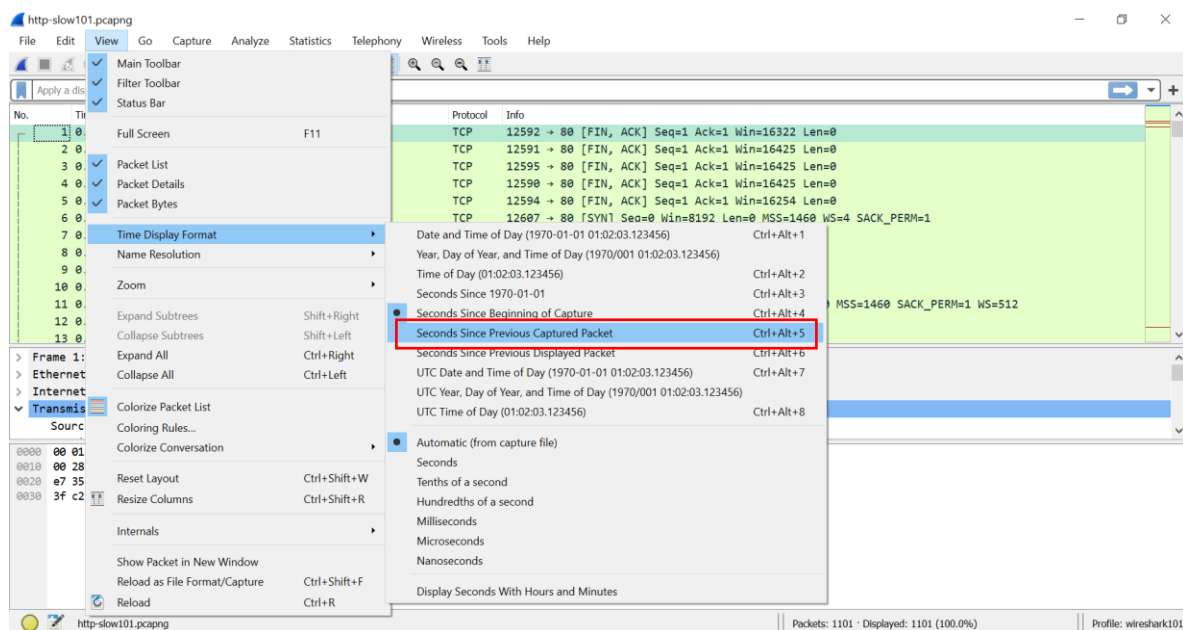
Abriremos un nuevo archivo llamado http-slow101.pcapng



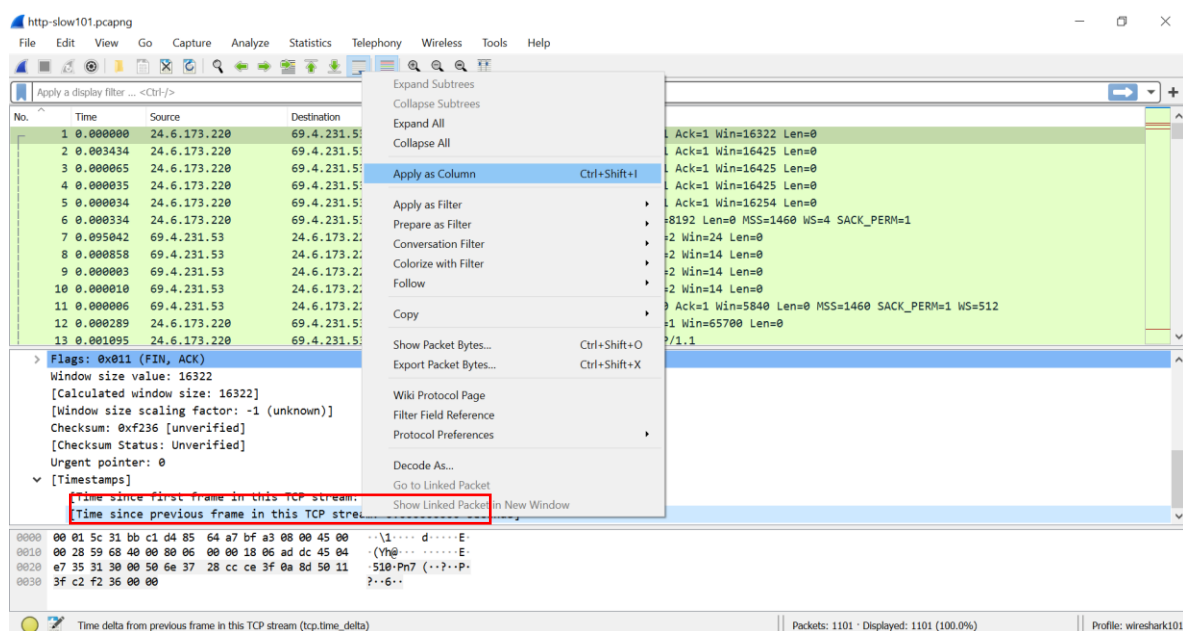
En la barra donde nos aparecen los nombres daremos click derecho y desmarcaremos la que se llama "LENGHT"



En la sección de *view* marcaremos la que se llama **SECONDS SINCE PREVIOUS CAPTURED PACKET**



Daremos click derecho y aplicaremos como una columna



Nos aparecerá como una nueva columna

http-slow101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Time since previous frame in this TCP stream	Info
1	0.000000	24.6.173.220	69.4.231.53	TCP	0.000000000	12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
2	0.003434	24.6.173.220	69.4.231.53	TCP	0.000000000	12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
3	0.000065	24.6.173.220	69.4.231.53	TCP	0.000000000	12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
4	0.000035	24.6.173.220	69.4.231.53	TCP	0.000000000	12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
5	0.000034	24.6.173.220	69.4.231.53	TCP	0.000000000	12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
6	0.000334	24.6.173.220	69.4.231.53	TCP	0.000000000	12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	0.095042	69.4.231.53	24.6.173.220	TCP	0.095410000	80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
8	0.000858	69.4.231.53	24.6.173.220	TCP	0.096300000	80 → 12595 [ACK] Seq=1 Ack=2 Win=14 Len=0
9	0.000003	69.4.231.53	24.6.173.220	TCP	0.096237000	80 → 12594 [ACK] Seq=1 Ack=2 Win=14 Len=0
10	0.000010	69.4.231.53	24.6.173.220	TCP	0.096381000	80 → 12591 [ACK] Seq=1 Ack=2 Win=14 Len=0
11	0.000006	69.4.231.53	24.6.173.220	TCP	0.095919000	80 → 12607 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
12	0.000289	24.6.173.220	69.4.231.53	TCP	0.000289000	12607 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
13	0.001095	24.6.173.220	69.4.231.53	HTTP	0.001095000	GET /viewvc/trunk-1.6/ HTTP/1.1

> Flags: 0x011 (FIN, ACK)
Window size value: 16322
[Calculated window size: 16322]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xf236 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1... d....E-
0010 00 28 59 68 40 00 00 06 00 00 18 06 ad dc 45 04 .(Yh@... ..E-
0020 e7 35 31 30 00 50 6e 37 28 cc ce 3f 0a 8d 50 11 .S10-Pn7 (...?..P-
0030 3f c2 f2 36 00 00 ..6..

Time delta from previous frame in this TCP stream (tcp.time_delta) | Packets: 1101 · Displayed: 1101 (100.0%) | Profile: wireshark101

Con click derecho en la sección de *edit column* podremos hacer diversos cambios

http-slow101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Time since previous frame in this TCP stream	Info
1	0.000000	24.6.173.220	69.4.231.53	TCP	0.000000000	12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
2	0.003434	24.6.173.220	69.4.231.53	TCP	0.000000000	12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
3	0.000065	24.6.173.220	69.4.231.53	TCP	0.000000000	12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
4	0.000035	24.6.173.220	69.4.231.53	TCP	0.000000000	12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
5	0.000034	24.6.173.220	69.4.231.53	TCP	0.000000000	12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
6	0.000334	24.6.173.220	69.4.231.53	TCP	0.000000000	12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	0.095042	69.4.231.53	24.6.173.220	TCP	0.095410000	80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
8	0.000858	69.4.231.53	24.6.173.220	TCP	0.096300000	80 → 12595 [ACK] Seq=1 Ack=2 Win=14 Len=0
9	0.000003	69.4.231.53	24.6.173.220	TCP	0.096237000	80 → 12594 [ACK] Seq=1 Ack=2 Win=14 Len=0
10	0.000010	69.4.231.53	24.6.173.220	TCP	0.096381000	80 → 12591 [ACK] Seq=1 Ack=2 Win=14 Len=0
11	0.000006	69.4.231.53	24.6.173.220	TCP	0.095919000	80 → 12607 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
12	0.000289	24.6.173.220	69.4.231.53	TCP	0.000289000	12607 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
13	0.001095	24.6.173.220	69.4.231.53	HTTP	0.001095000	GET /viewvc/trunk-1.6/ HTTP/1.1

> Flags: 0x011 (FIN, ACK)
Window size value: 16322
[Calculated window size: 16322]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xf236 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1... d....E-
0010 00 28 59 68 40 00 00 06 00 00 18 06 ad dc 45 04 .(Yh@... ..E-
0020 e7 35 31 30 00 50 6e 37 28 cc ce 3f 0a 8d 50 11 .S10-Pn7 (...?..P-
0030 3f c2 f2 36 00 00 ..6..

Time delta from previous frame in this TCP stream (tcp.time_delta) | Packets: 1101 · Displayed: 1101 (100.0%) | Profile: wireshark101

Cambiaremos el nombre que tiene por defecto a “TCP DELTA”

The screenshot shows the Wireshark interface with the display filter set to `tcp.time_delta`. The packet list shows 11 items, all of which are TCP segments. The packet details pane shows the flags and window size for a FIN, ACK packet.

No.	Time	Source	Destination	Protocol	Time since previous frame in this TCP stream	Info
1	0.000000	24.6.173.220	69.4.231.53	TCP	0.000000000	12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
2	0.003434	24.6.173.220	69.4.231.53	TCP	0.000000000	12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
3	0.000065	24.6.173.220	69.4.231.53	TCP	0.000000000	12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
4	0.000035	24.6.173.220	69.4.231.53	TCP	0.000000000	12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
5	0.000034	24.6.173.220	69.4.231.53	TCP	0.000000000	12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
6	0.000334	24.6.173.220	69.4.231.53	TCP	0.000000000	12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	0.095042	69.4.231.53	24.6.173.220	TCP	0.095410000	80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
8	0.000858	69.4.231.53	24.6.173.220	TCP	0.096303000	80 → 12595 [ACK] Seq=1 Ack=2 Win=14 Len=0
9	0.000003	69.4.231.53	24.6.173.220	TCP	0.096237000	80 → 12594 [ACK] Seq=1 Ack=2 Win=14 Len=0
10	0.000010	69.4.231.53	24.6.173.220	TCP	0.096381000	80 → 12591 [ACK] Seq=1 Ack=2 Win=14 Len=0
11	0.000006	69.4.231.53	24.6.173.220	TCP	0.095919000	80 → 12607 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_F

Flags: 0x011 (FIN, ACK)
Window size value: 16322
[Calculated window size: 16322]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xf236 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]

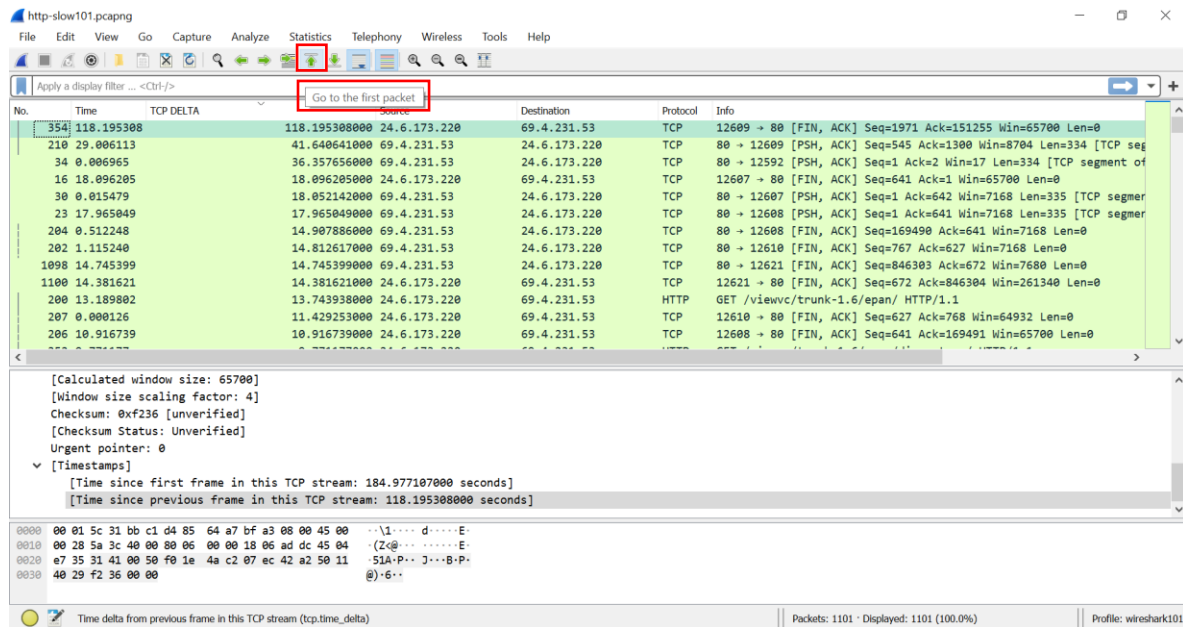
Con dos clics derechos en TCP DELTA podremos volver al no.1

The screenshot shows the Wireshark interface with the display filter set to `tcp.time_delta`. The packet list shows 11 items, all of which are TCP segments. The packet details pane shows the flags and window size for a FIN, ACK packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	24.6.173.220	69.4.231.53	TCP	12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
2	0.003434	24.6.173.220	69.4.231.53	TCP	12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
3	0.000065	24.6.173.220	69.4.231.53	TCP	12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
4	0.000035	24.6.173.220	69.4.231.53	TCP	12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
5	0.000034	24.6.173.220	69.4.231.53	TCP	12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
6	0.000334	24.6.173.220	69.4.231.53	TCP	12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
17	0.008281	24.6.173.220	69.4.231.53	TCP	12608 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
26	0.007718	24.6.173.220	69.4.231.53	TCP	80 → 12593 [PSH, ACK] Seq=1 Ack=1 Win=17 Len=334 [TCP segment of
44	0.009983	24.6.173.220	69.4.231.53	TCP	12609 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
62	0.020614	24.6.173.220	69.4.231.53	TCP	12610 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
355	0.003224	24.6.173.220	69.4.231.53	TCP	12621 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
557	0.000001	69.4.231.53	24.6.173.220	TCP	80 → 12621 [ACK] Seq=210600 Ack=672 Win=7680 Len=1460 [TCP segme
580	0.000001	69.4.231.53	24.6.173.220	TCP	80 → 12621 [ACK] Seq=238340 Ack=672 Win=7680 Len=1460 [TCP segme

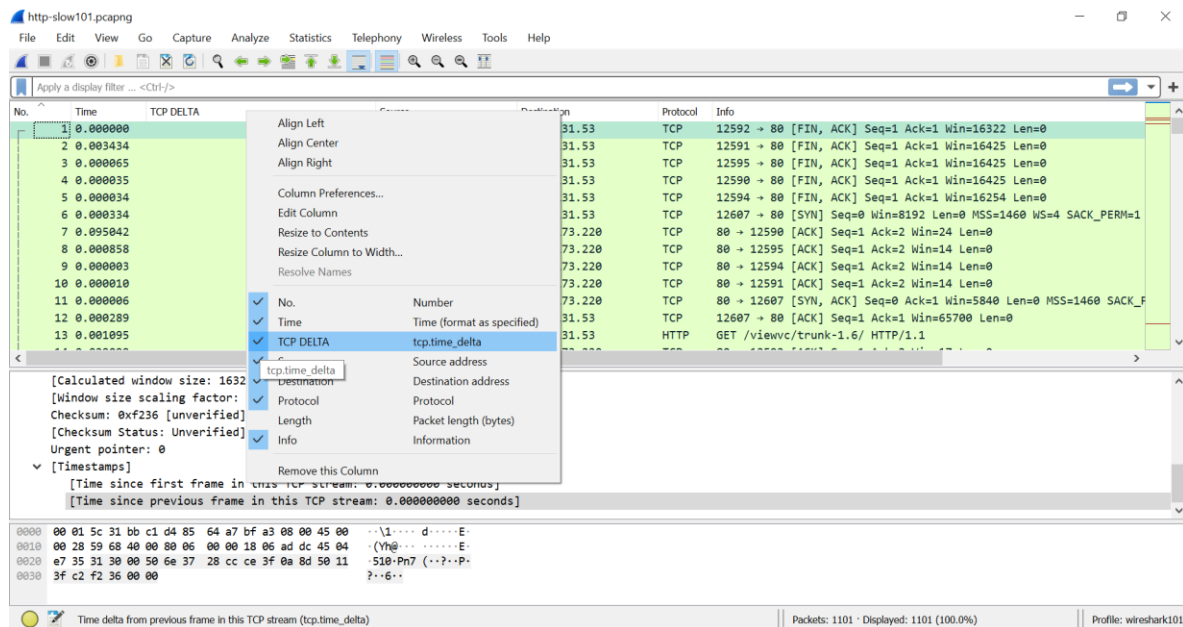
Flags: 0x011 (FIN, ACK)
Window size value: 16322
[Calculated window size: 16322]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xf236 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]

Con la flechita nos dirigiremos al número 354 que es el ultimo



The screenshot shows the Wireshark interface with the 'Go to the first packet' button highlighted in the display filter bar. The packet list shows packet 354 selected, which is a TCP segment. The packet details pane shows the TCP segment's structure, including the window size and scaling factor. The packet bytes pane shows the raw data of the packet.

Volvemos al número 1 y ahora desmarcaremos la columna de TCP DELTA dando click derecho en la barra, con eso desaparecerá de ahí.



The screenshot shows the Wireshark interface with the context menu open for the TCP DELTA column. The 'TCP DELTA' option is checked, and the 'Remove this Column' option is visible. The packet list shows packet 1 selected, which is a TCP segment. The packet details pane shows the TCP segment's structure, including the window size and scaling factor. The packet bytes pane shows the raw data of the packet.