

CHALLENGE 4



Open **challenge101-4.pcapng** and use the techniques covered in this chapter to answer these Challenge questions. The answer key is located in **Appendix A**.

Question 4-1.

What coloring rules does frame 170 match?

Bad TCP

Question 4-2.

Temporarily color TCP stream 5 with a light blue background and apply a filter on this traffic. How many packets match your filter?

The screenshot shows the Wireshark interface with the file 'challenge101-4.pcapng' open. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	TCP DELTA	Info
20	0.000434	24.6.173.220	184.30.240.170	TCP	66		0.000000000 29360 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
42	0.000005	184.30.240.170	24.6.173.220	TCP	66		0.031452000 80 → 29360 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=4
44	0.000014	24.6.173.220	184.30.240.170	TCP	54		0.000122000 29360 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
46	0.000307	24.6.173.220	184.30.240.170	HTTP	650		0.000693000 GET /swa/c/sitecopy_setup_L3.css HTTP/1.1
81	0.000001	184.30.240.170	24.6.173.220	TCP	60		0.037860000 80 → 29360 [ACK] Seq=1 Ack=597 Win=15792 Len=0
83	0.011776	184.30.240.170	24.6.173.220	HTTP	670		0.011776000 HTTP/1.1 200 OK (text/css)
166	0.090470	24.6.173.220	184.30.240.170	TCP	54		0.194656000 29360 → 80 [ACK] Seq=597 Ack=617 Win=65804 Len=0
298	0.001726	24.6.173.220	184.30.240.170	HTTP	1242		1.304084000 GET /web/fw/4/mtagconfig-2011-08.js HTTP/1.1

The details pane for the selected packet (No. 20) shows the following information:

- Arrival Time: Aug 31, 2012 15:51:38.130390000 Hora estándar del Este (México)
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1346446298.130390000 seconds
- [Time delta from previous captured frame: 0.000434000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.196955000 seconds]
- Frame Number: 20
- Frame Length: 66 bytes (528 bits)
- Capture Length: 66 bytes (528 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]
- [Coloring Rule Name: HTTP]

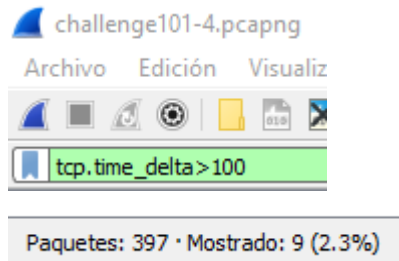
The packet bytes pane shows the raw data of the packet:

```
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 00 00 45 00  ..1....d....E-
0010 00 34 71 83 40 00 00 06 00 00 18 06 ad dc b8 1e  4q @.....
0020 f0 aa 72 b0 00 50 8b 0c 60 ee 00 00 00 00 00 02  -P.....
0030 20 00 6e d2 00 00 02 04 05 b4 01 03 03 02 01 01  n.....
0040 04 02 ..
```

Pasamos a colorear la conversación y luego TCP y color seleccionado 6. Esta secuencia TCP contiene 13 paquetes

Question 4-3.

Create and apply a coloring rule for TCP delta delays greater than 100 seconds. How many frames match this coloring rule?



Usamos la misma cadena como filtro de visualización y encontramos 9 cuadros que coinciden con los filtros. Un paquete aún conservaba nuestra regla de coloración temporal de la pregunta anterior

373	0.000109	24.6.173.220	184.30.240.170	TCP	54	114.879991000	29360	→ 80 [FIN, ACK] Seq=1785 Ack=1956 Win=65700 Len=0
374	0.000058	24.6.173.220	184.30.240.170	TCP	54	114.879991000	29360	→ 80 [FIN, ACK] Seq=1785 Ack=1956 Win=65700 Len=0

Question 4-4.

Export this filtered TCP delta information in CSV format? Using a spreadsheet program, what is the average TCP delta time?

Seleccionamos exportar los paquetes capturados y solo la línea de resumen de paquetes.

Después de crear una columna TCP Delta, seleccionamos Archivo | Exportar disecciones de paquetes | como formato "CSV". Seleccionamos exportar los paquetes capturados y solo la línea de resumen del paquete, abrimos el archivo .csv en Excel y determinamos el valor promedio de las columnas TCP Delta exportadas 115.2703762