Ejercicio 1

a.
Gracias al filtro `tcp.flags.syn == 1`, podemos observar la existencia de tres paquetes. El primer paquete contiene el SYN, el segundo el SYN/ACK, y el tercero el ACK.

b.
En la trama 203 se devuelve un "200 OK". Por lo tanto, el primer segmento que realiza la petición HTTP POST es el número 206.

c.
Usando el filtro `http.request.method == POST`, puedo identificar que la petición POST se encuentra en la línea 199. Por tanto, las tramas que siguen desde la 200 hasta la 203 son las relacionadas con esta petición.

La conexión TCP se cierra en la trama 213.

Ejercicio 2

a.
Puerto de origen: 1161
Puerto de destino: 80 (reservado para TCP)

b.
Se emplean 2 bytes, es decir, 16 bits.

c.
Se pueden emplear un total de 2162^{16}216 puertos, desde 0 hasta 216−12^{16} - 1216−1.

Ejercicio 3

a.
La dirección IP es: 128.119.245.12.

b.
Envía desde el puerto 80 (reservado para TCP) hacia el puerto 1161.

Ejercicio 4

a.
El número de secuencia relativo es 0, y el número de secuencia en formato raw (puro) es 232129012.

b.
A partir de las flags, la secuencia de bits 0x002 en el campo de flags corresponde a un paquete SYN. Esto es lógico porque todos los bits están en cero, excepto el penúltimo, que corresponde al setter del SYN.

Ejercicio 5

a.
El número de secuencia relativo es 1, y el número de secuencia en formato raw (puro) es 883061786.

b.
Contamos con el campo relativo y el campo raw del número de reconocimiento (acknowledgement number).

- Relativo del número de reconocimiento (AN): 0
- Raw del número de reconocimiento (AN): 883061785

c.
Para el valor del AN, se toma el número de secuencia anterior menos 1. El número de secuencia (SN) puede ser cualquier valor en su primera instancia: 232129013.

d.
A partir de las flags, podemos observar que están activados los bits correspondientes al SYN y al ACK.

Ejercicio 6

Número de secuencia: 232293053

Ejercicio 7

Número de secuencia (raw): 232129012
Número de reconocimiento (AN): 0 (lógicamente).

Observamos que el número de secuencia es menor de lo esperado.

En las sesiones teóricas no vimos la diferencia entre AN relativo y AN absoluto (raw). El número absoluto corresponde al valor real del campo en la cabecera TCP del segmento, el cual es establecido de manera aleatoria al inicio de la conexión. Para facilitar la visualización del intercambio de información, se utiliza el AN relativo, que comienza en 0 al inicio de la conexión.

Ejercicio 8

Casilla marcada:

- Raw: 232129012
- Relativo: 0 (al inicio de la conexión).

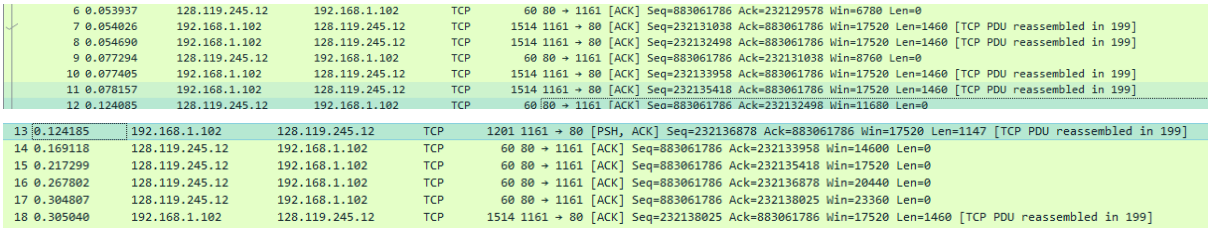
Casilla desmarcada:
Solo se muestra el valor raw, es decir, no aparece el AN relativo, tal como se mostró en clase.

Ejercicio 9

a.
El número de secuencia del primer paquete PUSH/ACK es 232136878.
Los siguientes cinco números de secuencia son:

- 883061786
- 883061786
- 883061786
- 883061786
- 232138025

b.



6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232129578 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=232131038 Ack=883061786 Win=17520 Len=1460 [TCP PDU reassembled in 199]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=232132498 Ack=883061786 Win=17520 Len=1460 [TCP PDU reassembled in 199]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232131038 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=232133958 Ack=883061786 Win=17520 Len=1460 [TCP PDU reassembled in 199]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=232135418 Ack=883061786 Win=17520 Len=1460 [TCP PDU reassembled in 199]
12	0.124085	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201 1161 → 80 [PSH, ACK] Seq=232136878 Ack=883061786 Win=17520 Len=1147 [TCP PDU reassembled in 199]
14	0.169118	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232133958 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232135418 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232136878 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=883061786 Ack=232138025 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [ACK] Seq=232138025 Ack=883061786 Win=17520 Len=1460 [TCP PDU reassembled in 199]

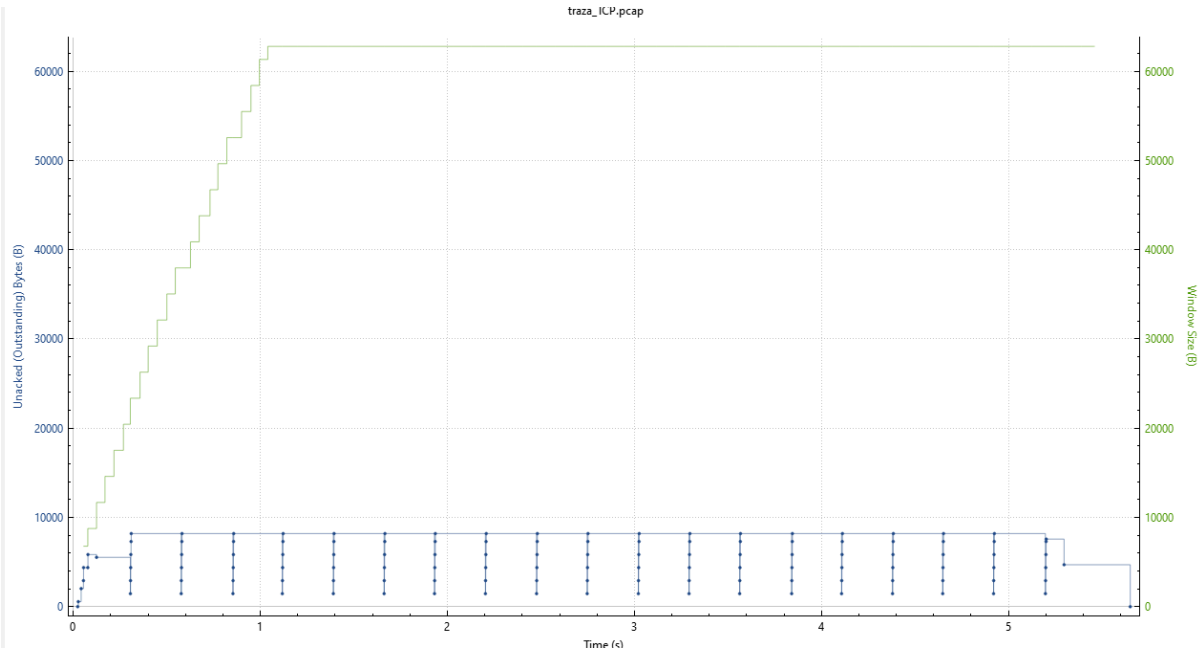
c.

- 12 0.124085 128.119.245.12 192.168.1.102 TCP 60 80 → 1161 [ACK] Seq=883061786 Ack=232132498 Win=11680 Len=0

d.
1514
60

Ejercicio 10

a.

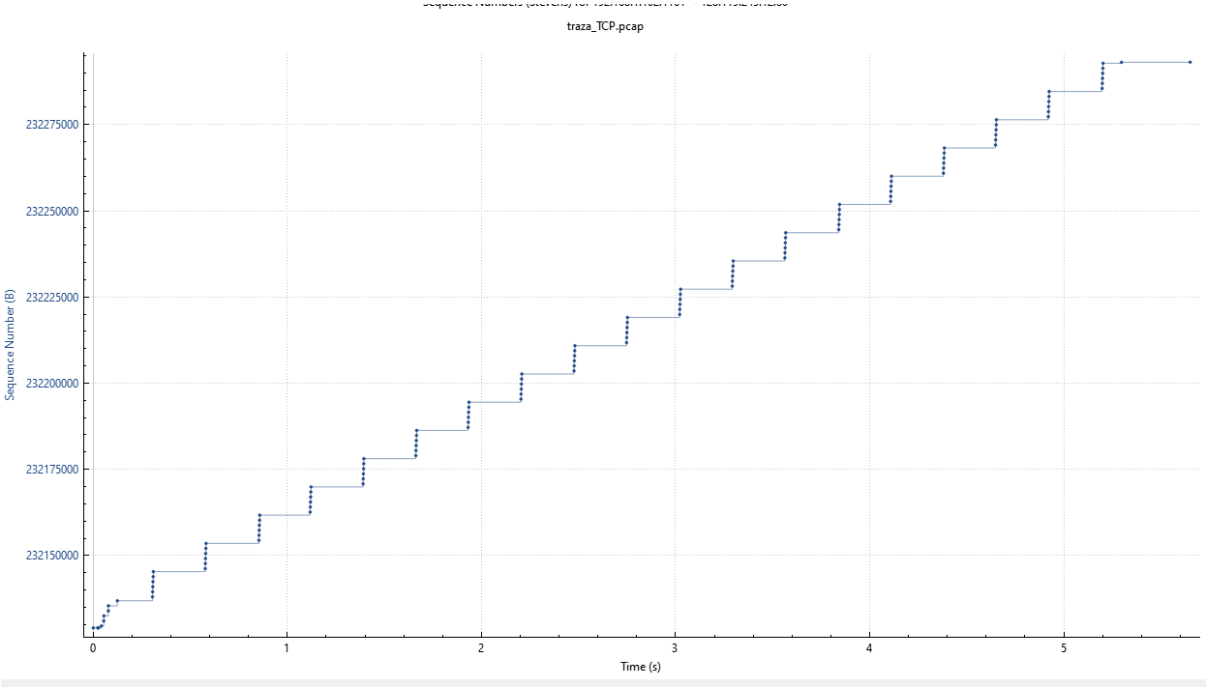


b.

17520

Ejercicio 11

a.



Ejercicio 12

A partir del comando `tcp.analysis.duplicate_ack`, no aparece ningún ACK duplicado.

Ejercicio 13

Primer número de secuencia: 232129013
Octavo número de secuencia: 883061786

Ejercicio 14

Procesado - Final / Tiempo

- Número inicial de secuencia: 232129013
- Número final de secuencia: 883062516

- Tiempo inicial: 0.023172
- Tiempo final: 5.6561141
- Caudal: 115,070,257.6 bytes/segundo = 112,345.5 KB/s = 115 MB/s