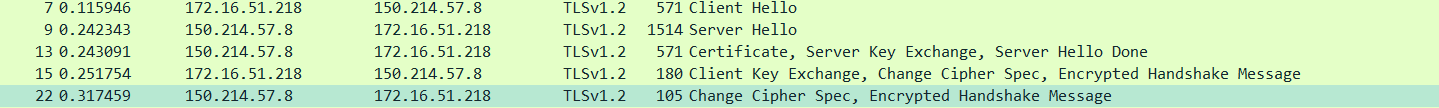
1 ¿Cuándo se procede con el handshake y la fase de conexión?

Hanshake

meneame



Tlsv13\_test

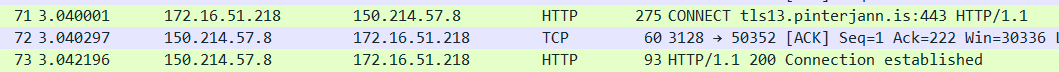


Fase de conexión

meneame



Tlsv13\_test



2 ¿Qué versión de TLS se utiliza?

Mename: TLSv1.2

TLSv13\_test: TLSv1.3

3 En la parte del cliente, ¿en qué trama se puede ver las suites de cifrado que soporta el cliente?

mename



Tlsv13\_test



4 ¿Qué suite de cifrado se acepta finalmente para el proceso de conexión?



5 ¿En qué trama se envía el certificado digital del servidor? NOTA: No responder esta pregunta para la web (b)



6 ¿El servidor se autentica al cliente? ¿Y el cliente al servidor?

Meneame: El servidor al cliente se autentica pero al revés no.

TLSv13\_test: Los dos se auntentican.