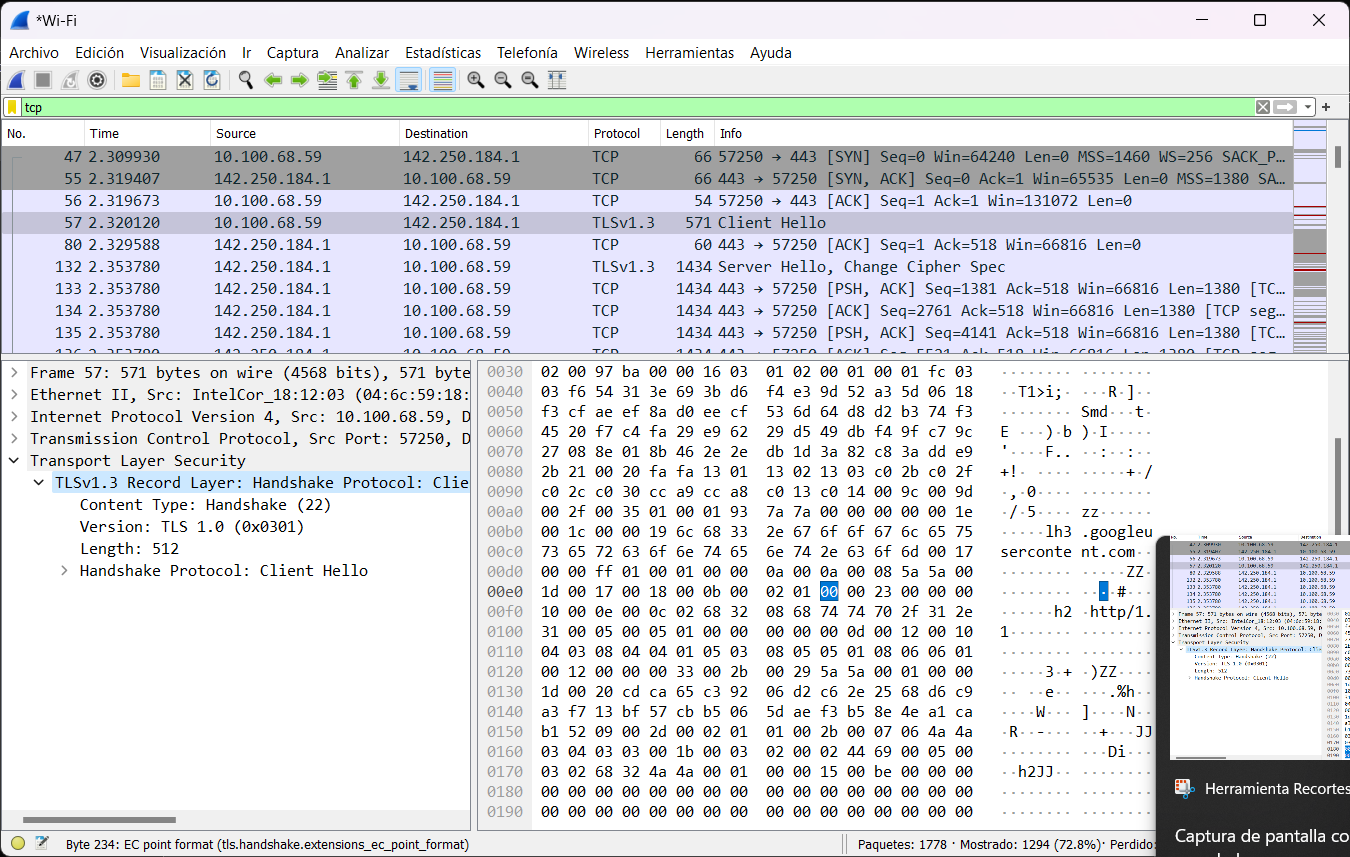
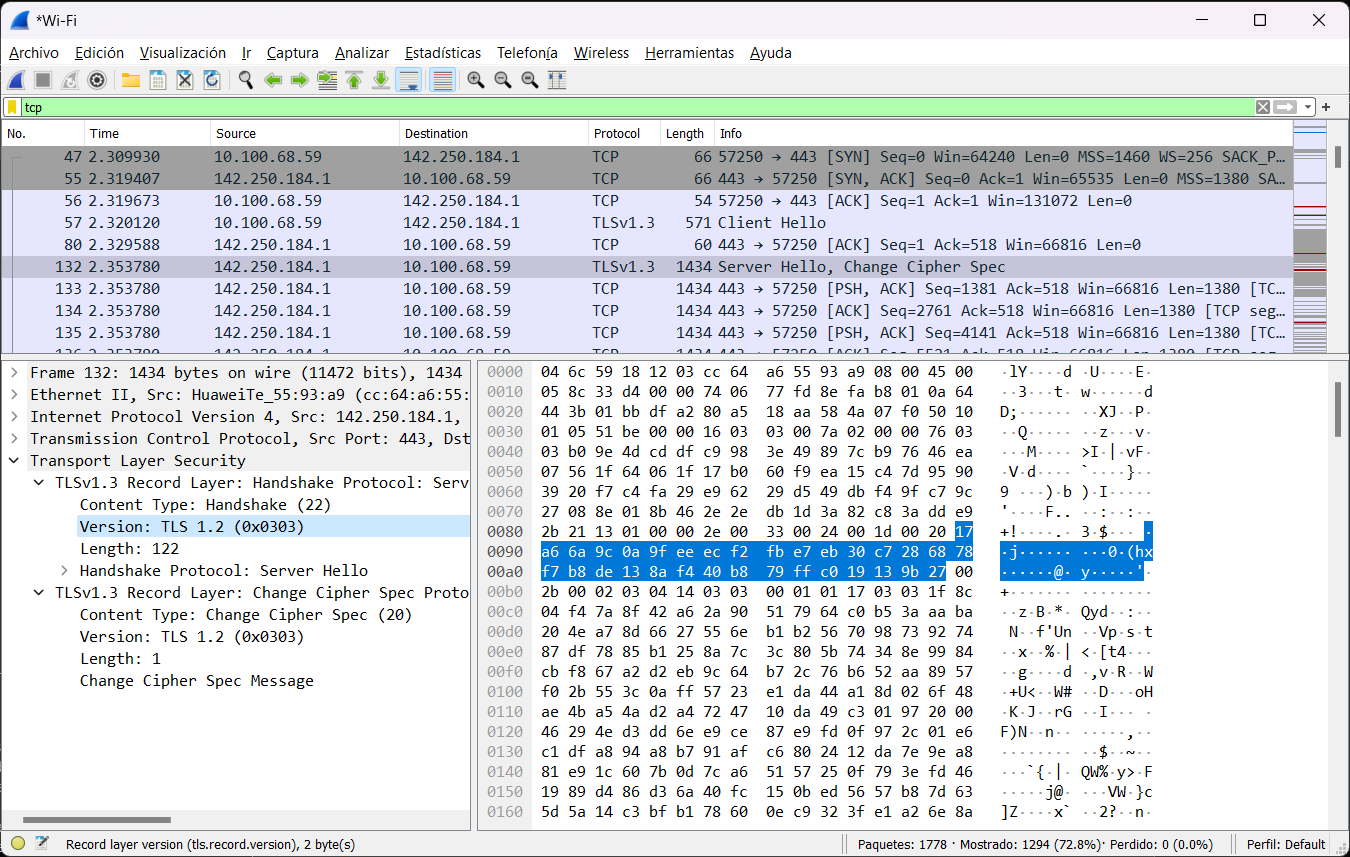
Debido a las múltiples vulnerabilidades que se han identificado en las implementaciones de SSL y TLS en los últimos años (BEAST, CRIME, BREACH, HEARTBLEED, POODLE, FREAK, Logjam), una de las principales recomendaciones (adicional a la de actualizar los componentes asociados a estos protocolos) es la de emplear algoritmos de encriptación con longitudes de claves robustas. Para configurarlo, se hace uso de un “conjunto de cifrado” (“cipher suite”), que por lo general involucra cadenas como estas:

Client Hello:



Server Hello:



Aplication data:

Se ve que esta encriptado.

