Criptografia - SSL/TLS
Trabalho Prático

Autor:
Vasco Barnabé - nº42819

Setembro de 2021

1 Introdução

Como exercício prático relativamente ao trabalho teórico realizado, será efetuada uma pequena análise de tráfego na rede utilizando o **Wireshark**, programa que analisa este tráfego e o organiza por protocolos. Deste modo, será apresentado um exemplo do processo de **Handshake com TLS**.

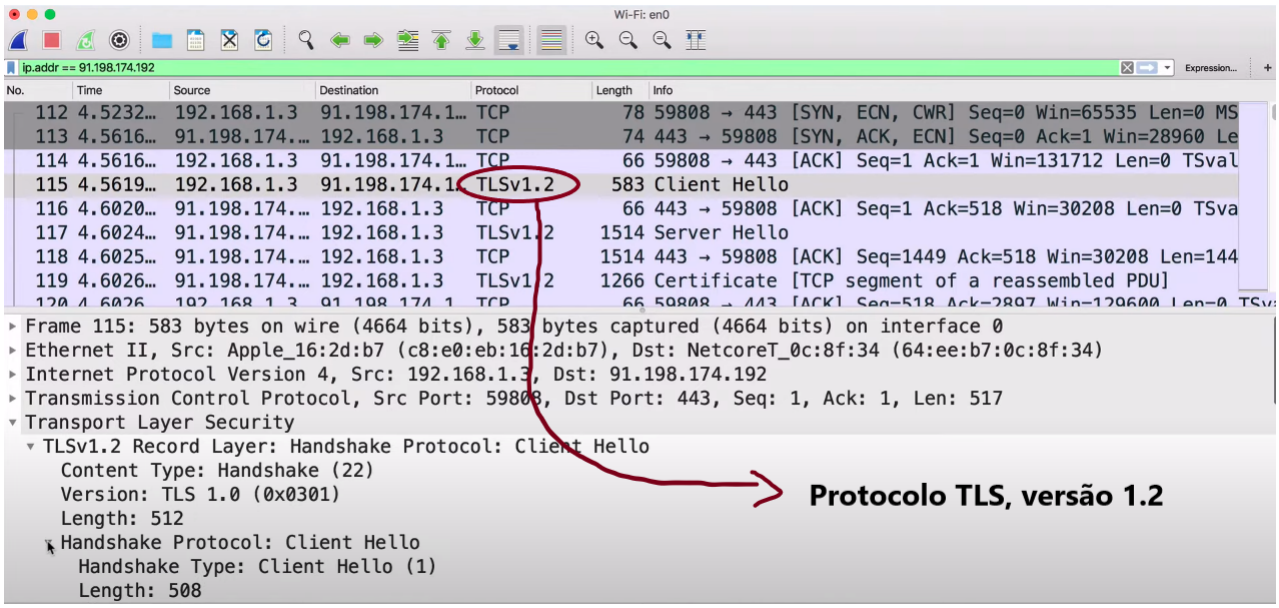
2 Requisitos

Para a realização deste exercício basta o uso do programa Wireshark. A sua instalação pode ser feita a partir de um terminal, em Linux, do seguinte modo:

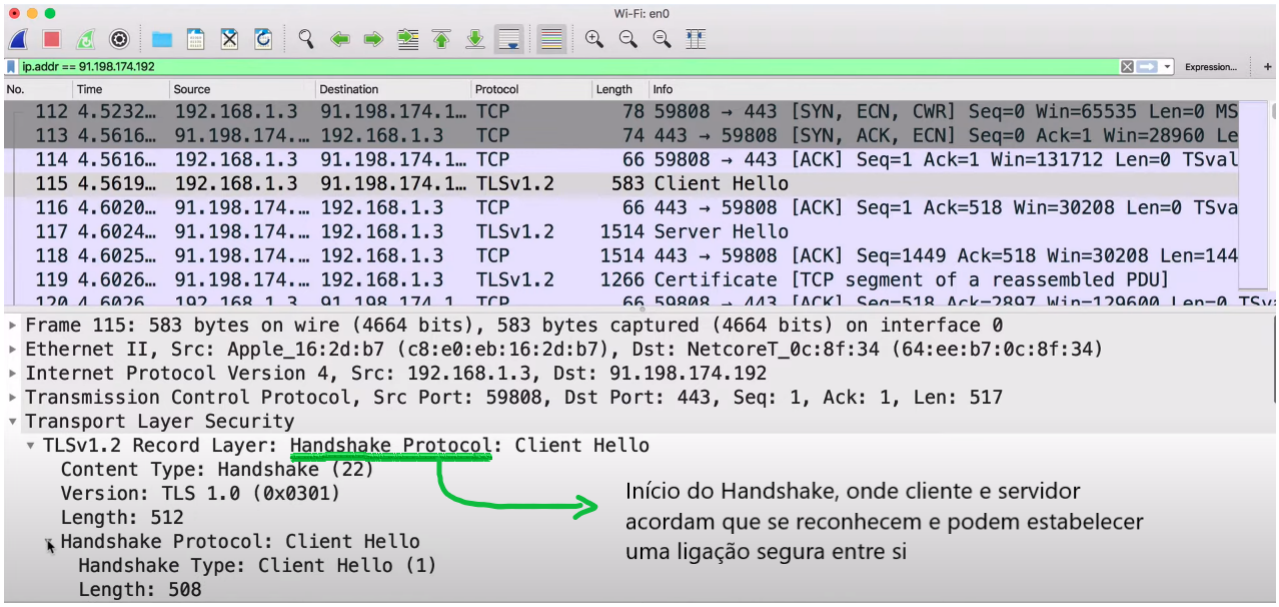
$ sudo apt install wireshark.

3 Análise de Tráfego utilizando o WireShark

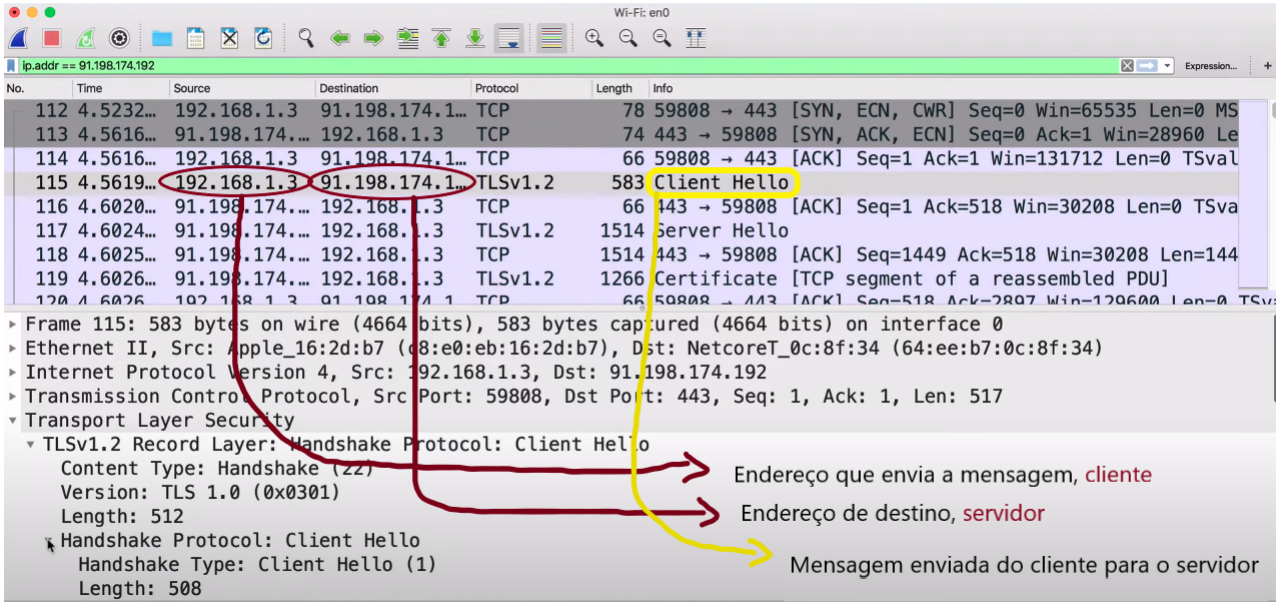
Como é possível verificar na imagem seguinte, a versão do protocolo TLS em execução neste exemplo é a **versão 1.2**:



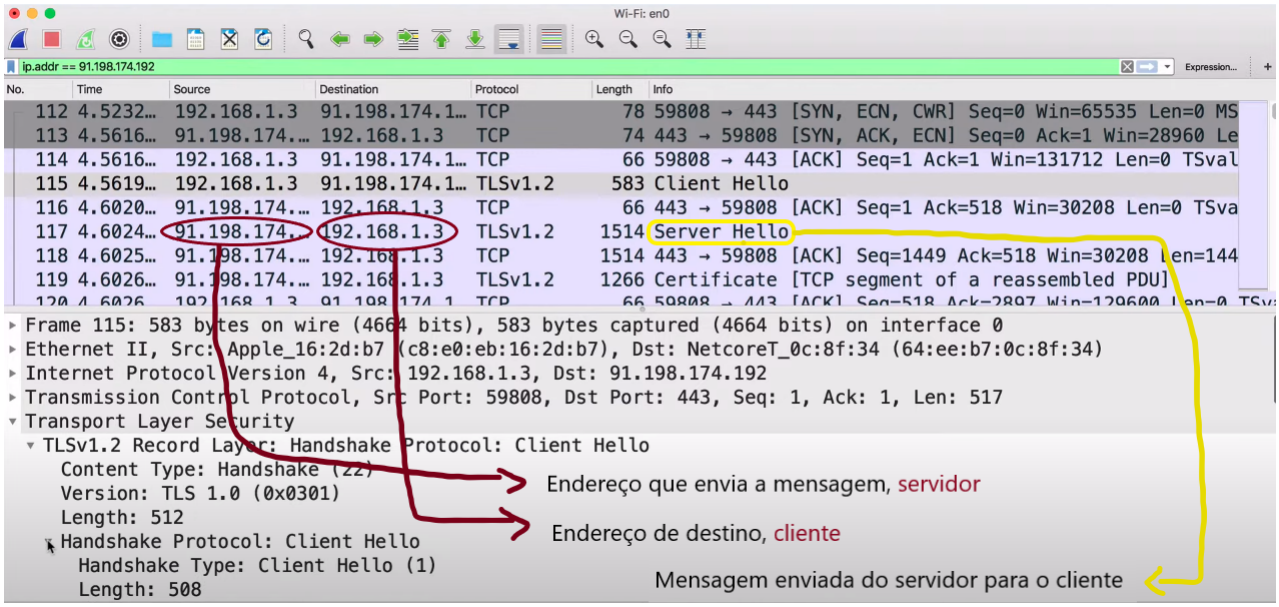
Início do processo de **Handshake** entre cliente e servidor:



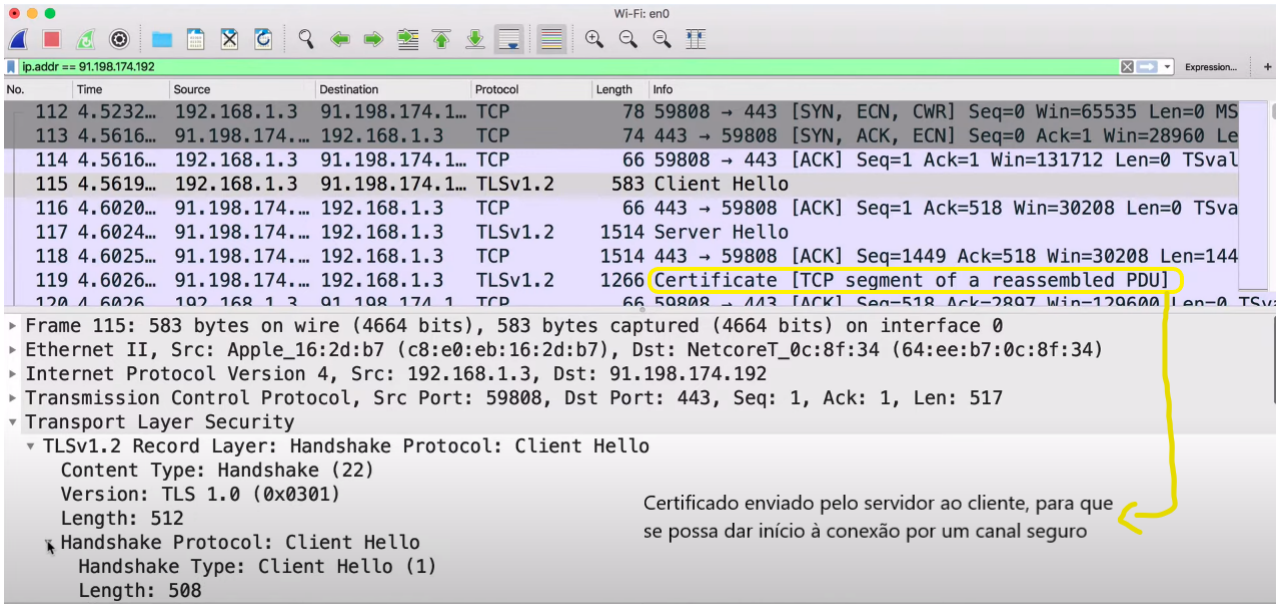
O cliente é o primeiro a enviar uma mensagem. Envia uma mensagem "olá"para o servidor, por um canal inseguro, de modo a dar a conhecer a este que quer estabelecer ligação segura:



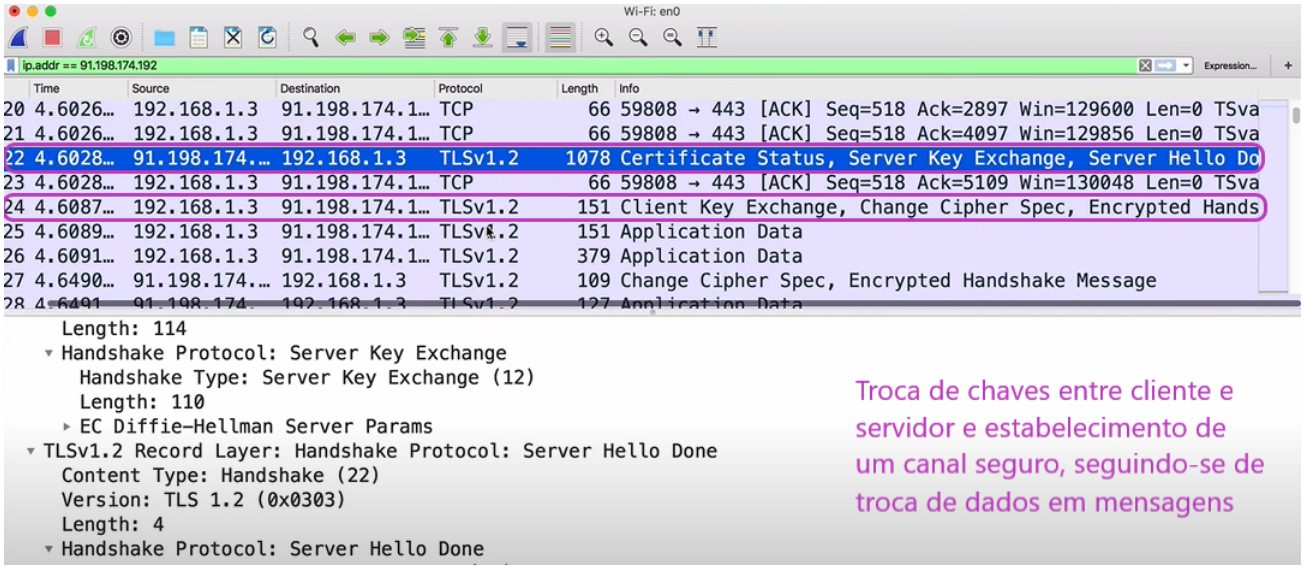
De seguida, é o servidor a mandar a mensagem "olá"ao cliente, como se pode verificar comparando com a imagem anterior, houve uma troca dos endereços de envio e de destino, pois agora a mensagem vai no sentido servidor ⇒ *cliente* :



Após as primeiras mensagens de reconhecimento entre cliente e servidor, é altura do servidor enviar o certificado SSL ao cliente, para que se possa dar início à ligação entre ambos por um canal seguro, protegido de possíveis ataques e roubo de dados em tráfego:



O último passo deste Handshake entre cliente e servidor, é então a troca de chaves públicas e privadas de forma a ser criada uma chave de sessão para o canal seguro por onde será feita a transferência de dados. Esta chave será utilizada para encriptar e desencriptar os dados transferidos nesta ligação.



Após a criação de um canal seguro, dá-se início à troca de dados entre cliente e servidor, como se pode ver na imagem anterior, "Application Data".