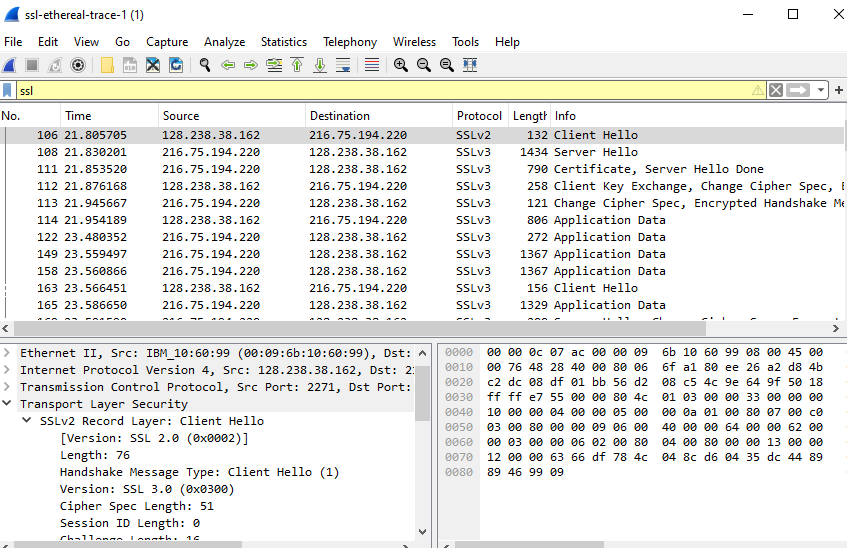
Task 3: Investigating the Secure Sockets Layer (SSL) protocol

SSL is a mechanism for securing the Internet that is based on encryption. The Secure Sockets Layer (SSL) protocol initiates a process of authentication known as a handshake between two communicating devices in order to verify that both devices are in fact indeed who they claim to be. In addition, SSL digitally signs data in order to ensure the integrity of the data. This ensures that the data has not been altered in any way before it is delivered to the person who is supposed to receive it.

1: Capturing packets in an SSL Session



2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Time | Source | Destination | Info |
| 106 | 21.80571 | 128.238.38.162 | 216.75.194.220 | Client Hello |
| 108 | 21.8302 | 216.75.194.220 | 128.238.38.162 | Server Hello |
| 111 | 21.85352 | 216.75.194.220 | 128.238.38.162 | Certificate, Server Hello Done |
| 112 | 21.87617 | 128.238.38.162 | 216.75.194.220 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 113 | 21.94567 | 216.75.194.220 | 128.238.38.162 | Change Cipher Spec, Encrypted Handshake Message |
| 114 | 21.95419 | 128.238.38.162 | 216.75.194.220 | Application Data |
| 122 | 23.48035 | 216.75.194.220 | 128.238.38.162 | Application Data |
| 149 | 23.5595 | 216.75.194.220 | 128.238.38.162 | SSLv3 |