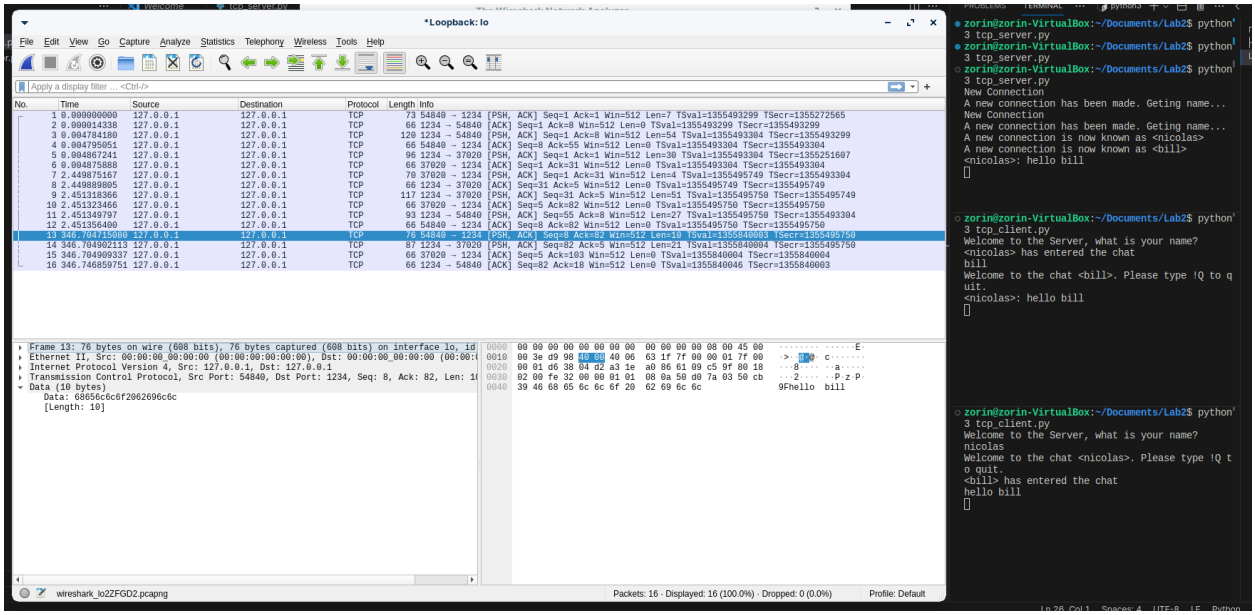
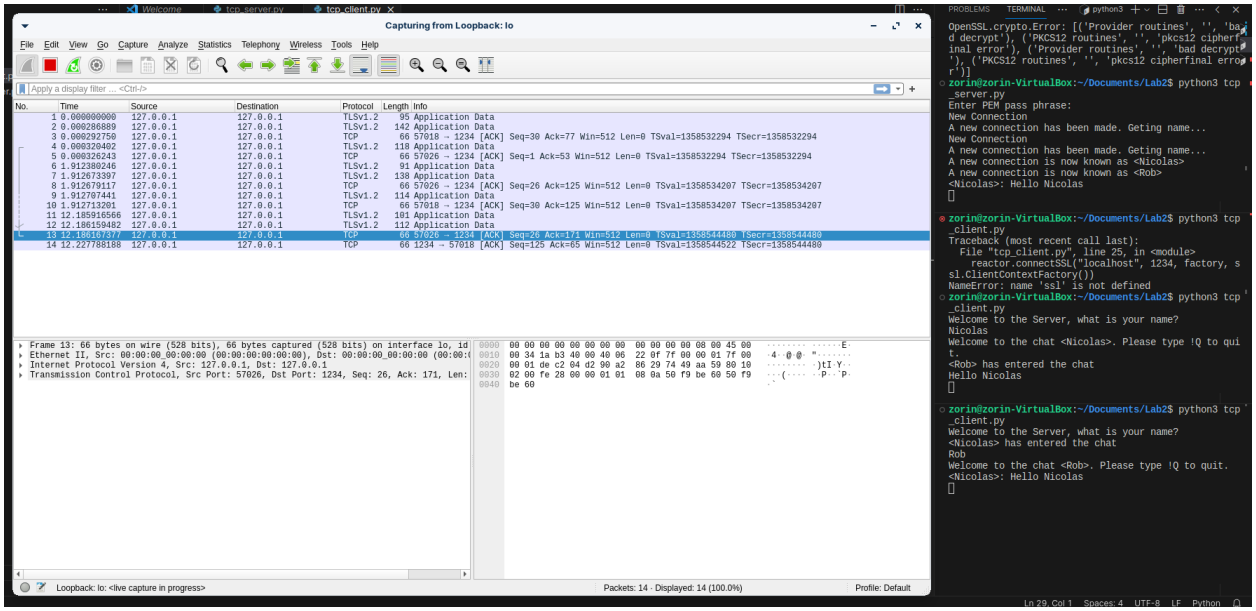
Nicolas Ansell, 200431074

Phase 1



Wireshark is able to see the messages being transmitted by the clients and the server

Adding SSL



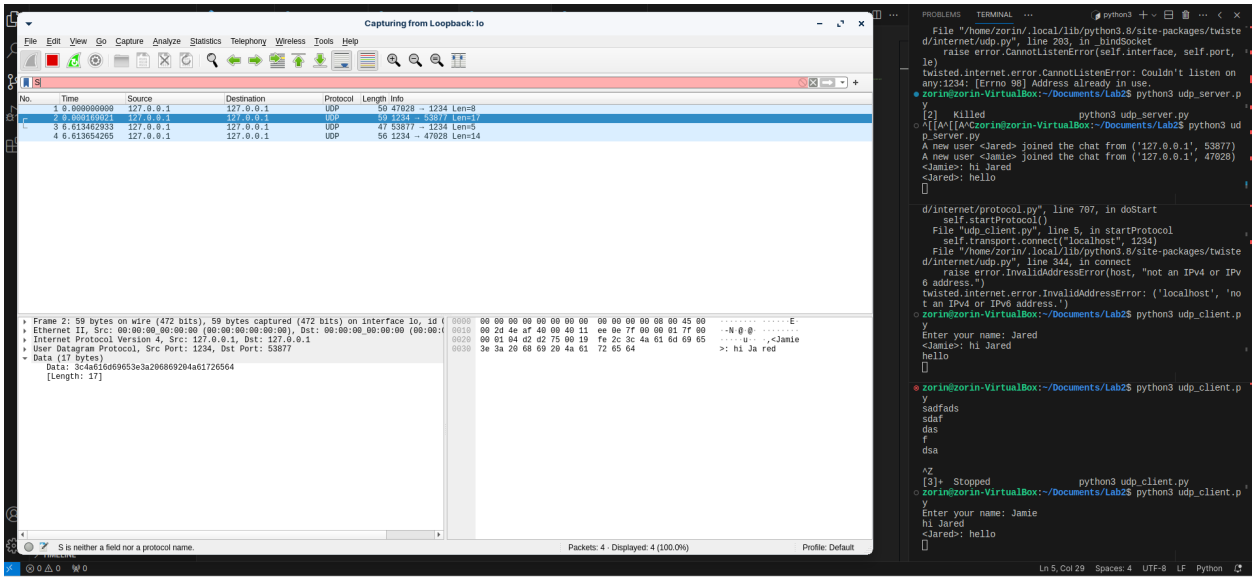
The protocol being used now is SSL on top of TCP. TLS in its updated versions.

trying to capture packets now, you will not see the actual content of the messages being sent. Instead, you'll see encrypted data. Using wireshark we see that this is the case

From the user's perspective, the application functions the same as before. They will not notice that the messages are being encrypted unless they are aware of the upgrade or use wireshort

If you capture the packets, you will observe the SSL/TLS handshake process at the start of the connection. Here you'll see the "Client Hello" and "Server Hello" messages.
Certificates being exchanged: During the TLS handshake, the server will send its certificate to the client for verification. This is visible in the captured packets as part of the handshake process

Changing to UDP



The protocol in use is now UDP instead of TCP.
There's no connection establishment or termination, so you won't see any SYN, SYN-ACK, or FIN packets that you would with TCP.
Each packet is independent; there's no guaranteed order, and no automatic retransmission for lost packets.
there absence of many of the features TCP provides, which can either be a benefit or a drawback depending on the use case. In a chat application, you may notice that messages can arrive out of order or not at all if there are any network disruptions.
Im not sure if we were supposed to use SSL with udp or something but i wasn’t sure how.