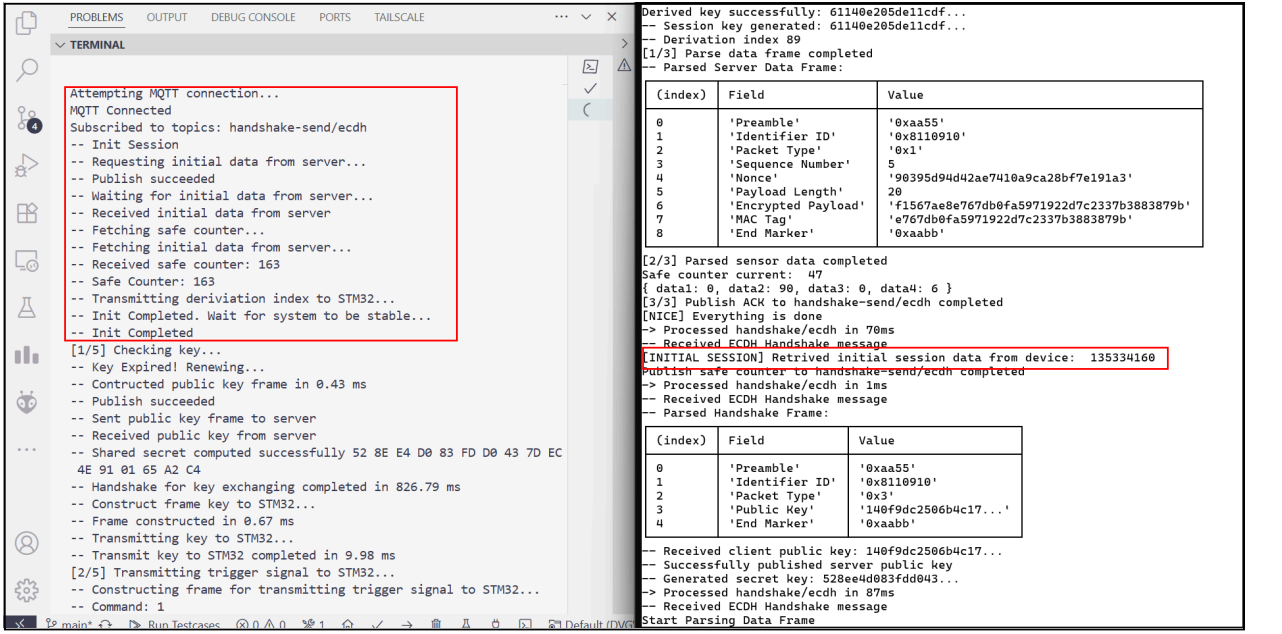
PROBLEMS
OUTPUT
DEBUG CONSOLE
PORTS
TAILSCALE
TERMINAL
Attempting MQTT connection...
MQTT Connected
Subscribed to topics: handshake-send/ecdh
-- Init Session
-- Requesting initial data from server...
-- Publish succeeded
-- Waiting for initial data from server...
-- Received initial data from server
-- Fetching safe counter...
-- Fetching initial data from server...
-- Received safe counter: 163
-- Safe Counter: 163
-- Transmitting deriviation index to STM32...
-- Init Completed. Wait for system to be stable...
-- Init Completed
[1/5] Checking key...
-- Key Expired! Renewing...
-- Contructed public key frame in 0.43 ms
-- Publish succeeded
-- Sent public key frame to server
-- Received public key from server
-- Shared secret computed successfully 52 8E E4 D0 83 FD D0 43 7D EC 4E 91 01 65 A2 C4
-- Handshake for key exchanging completed in 826.79 ms
-- Construct frame key to STM32...
-- Frame constructed in 0.67 ms
-- Transmitting key to STM32...
-- Transmit key to STM32 completed in 9.98 ms
[2/5] Transmitting trigger signal to STM32...
-- Constructing frame for transmitting trigger signal to STM32...
-- Command: 1
main*
Run Testcases
Derived key successfully: 61140e205de11cdf...
-- Session key generated: 61140e205de11cdf...
-- Derivation index 89
[1/3] Parse data frame completed
-- Parsed Server Data Frame:
(index) Field Value
0 'Preamble' '0xaa55'
1 'Identifier ID' '0x8110910'
2 'Packet Type' '0x1'
3 'Sequence Number' 5
4 'Nonce' '90395d94d42ae7410a9ca28bf7e191a3'
5 'Payload Length' 20
6 'Encrypted Payload' 'f1567ae8e767db0fa5971922d7c2337b3883879b'
7 'MAC Tag' 'e767db0fa5971922d7c2337b3883879b'
8 'End Marker' '0xaabb'
[2/3] Parsed sensor data completed
Safe counter current: 47
{ data1: 0, data2: 90, data3: 0, data4: 6 }
[3/3] Publish ACK to handshake-send/ecdh completed
[NICE] Everything is done
-> Processed handshake/ecdh in 70ms
-- Received ECDH Handshake message
[INITIAL SESSION] Retrived initial session data from device: 135334160
Publish safe counter to handshake-send/ecdh completed
-> Processed handshake/ecdh in 1ms
-- Received ECDH Handshake message
-- Parsed Handshake Frame:
(index) Field Value
0 'Preamble' '0xaa55'
1 'Identifier ID' '0x8110910'
2 'Packet Type' '0x3'
3 'Public Key' '140f9dc2506b4c17...'
4 'End Marker' '0xaabb'
-- Received client public key: 140f9dc2506b4c17...
-- Successfully published server public key
-- Generated secret key: 528ee4d083fdd043...
-> Processed handshake/ecdh in 87ms
-- Received ECDH Handshake message
Start Parsing Data Frame