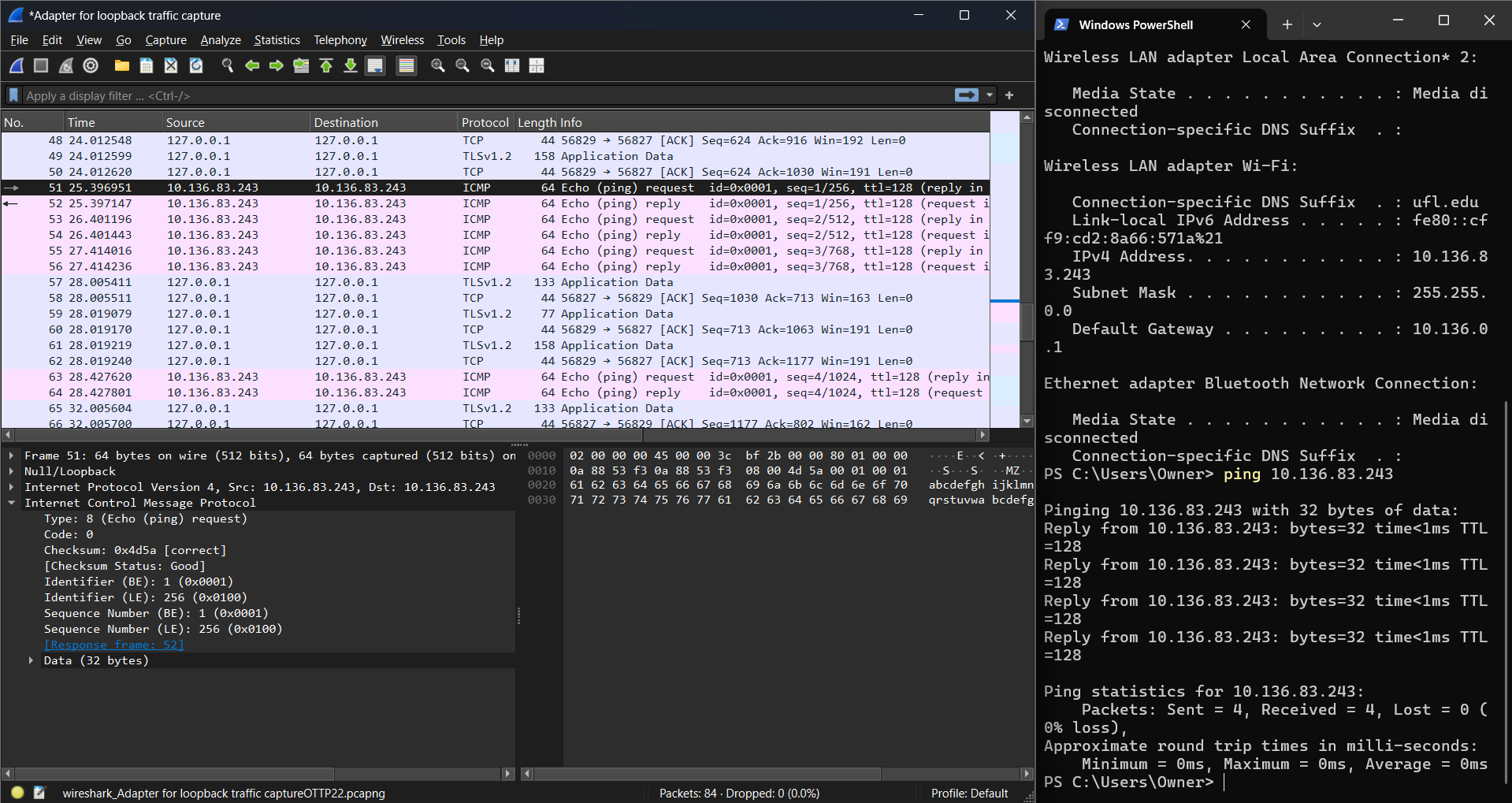
# Lab 4: Basic Network Security

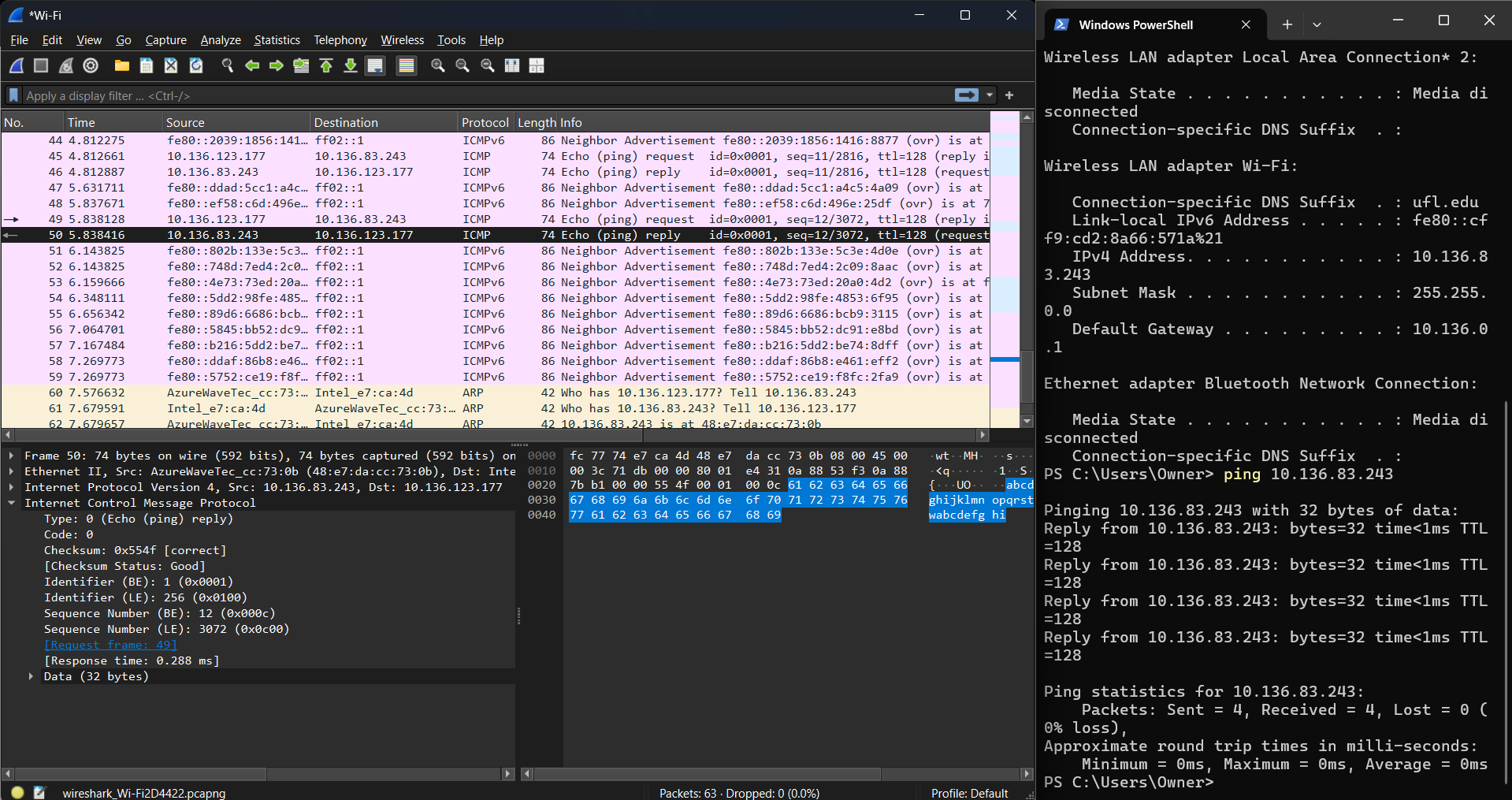
**(79 Points)**

## Wireshark:

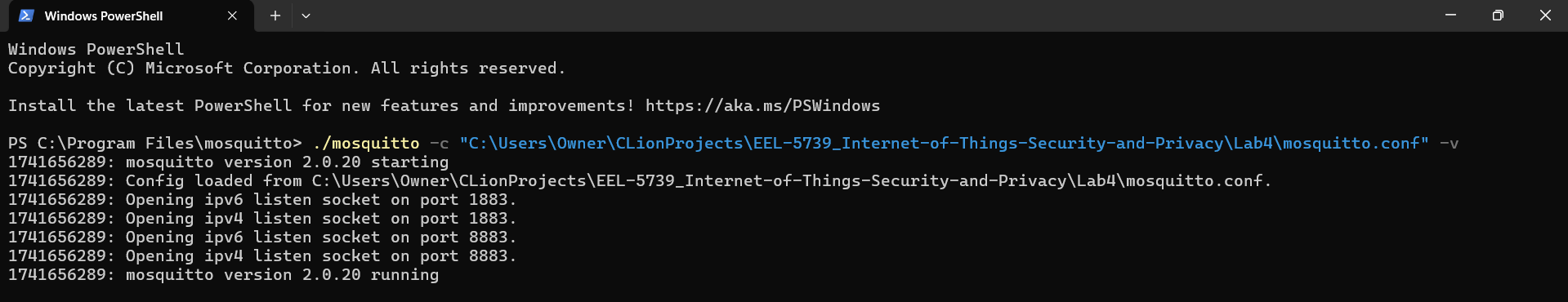
1. Install [wires.hark](https://www.wireshark.org/download.html) on Partner A’s computer
2. Select the wifi adapter to monitor
3. Partner A should ping Partner A’s address and screenshot the result in wireshark (5 point)



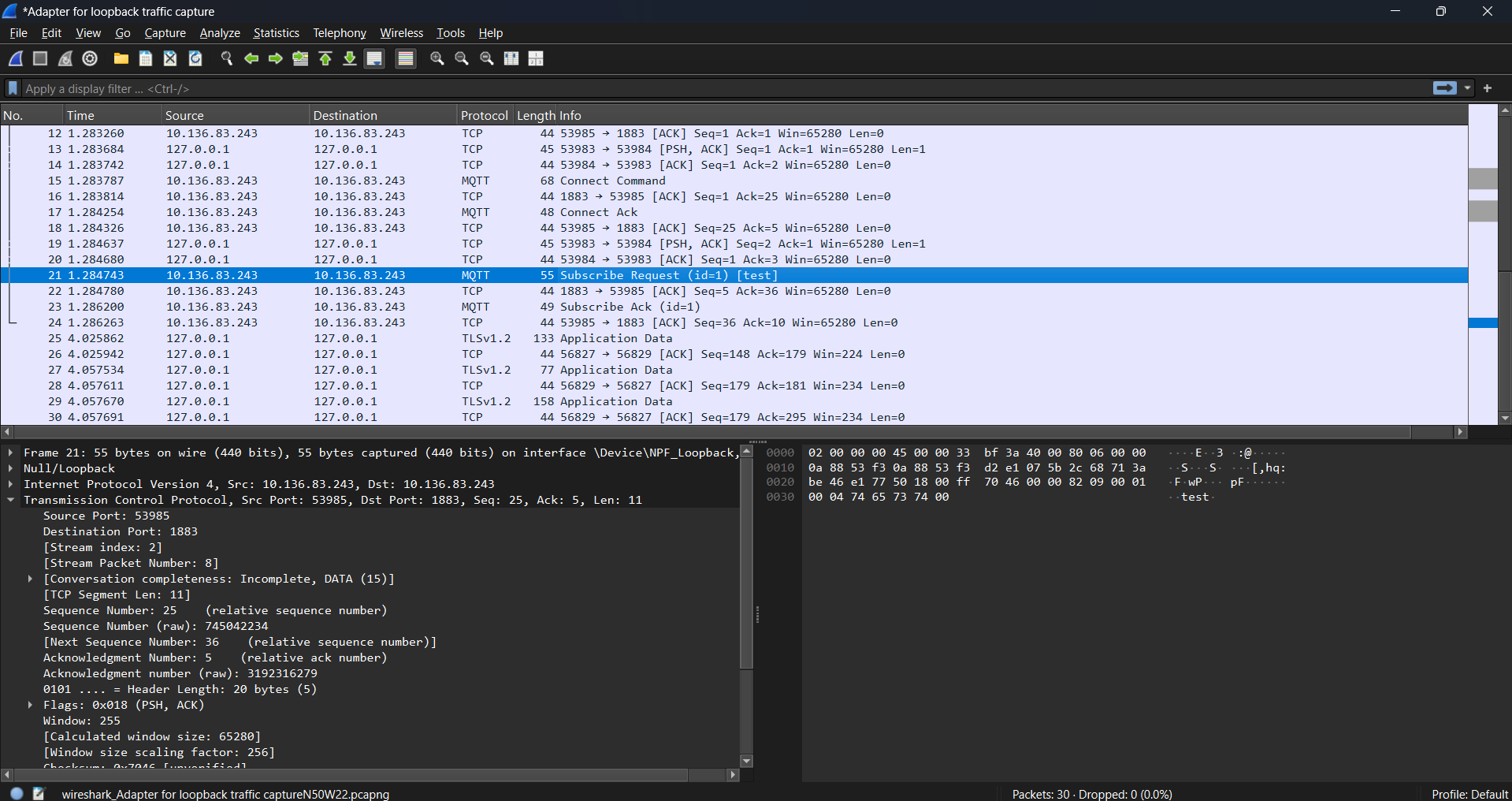
1. Partner B should ping Partner A’s address and screenshot the result in wireshark (5 point)



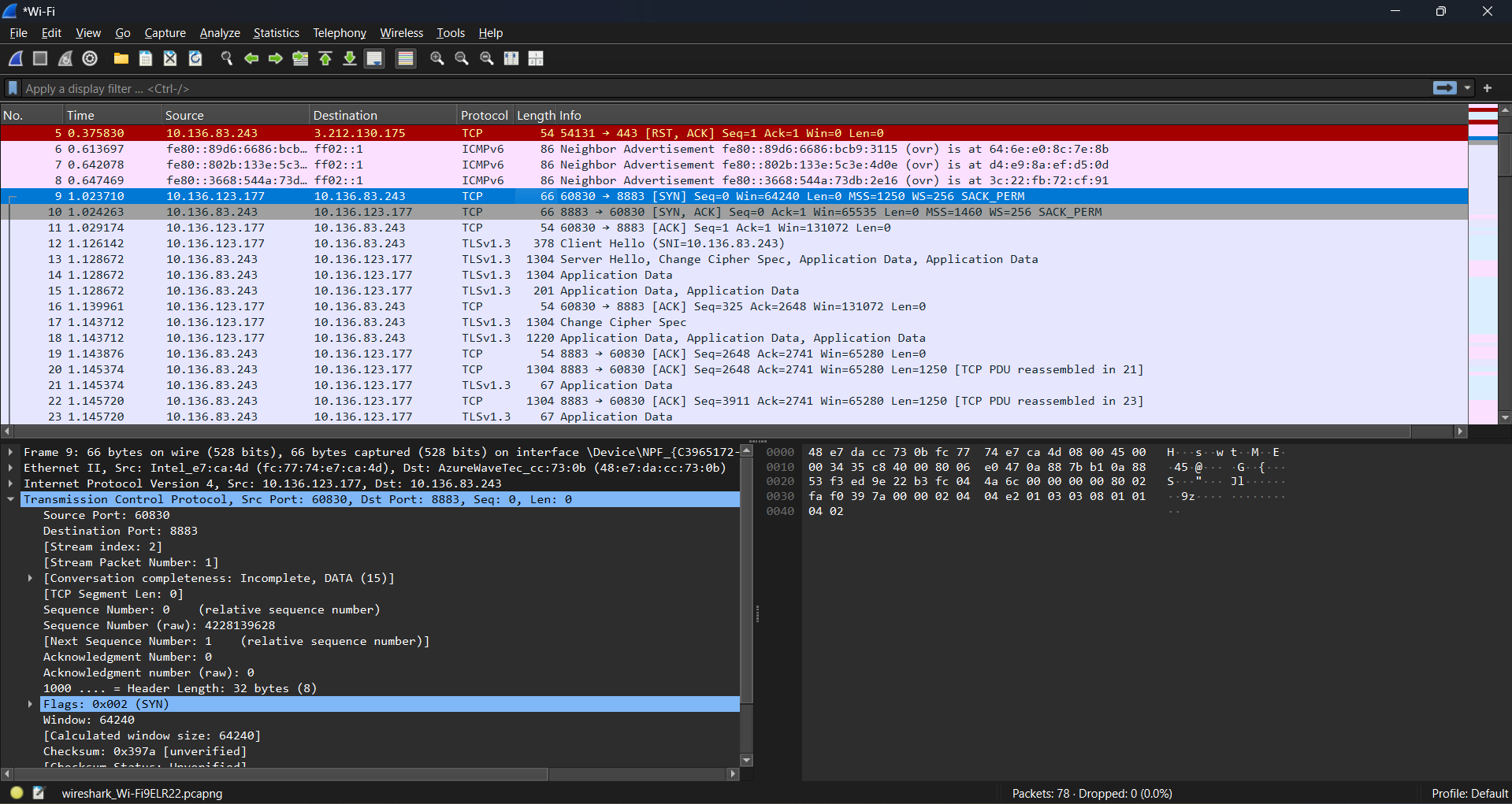
1. Partner A and Partner B should install [mosquitto](https://mosquitto.org/download/) if you do not have it
2. Partner A starts a mosquitto server capable of sending and receiving messages off Partner A machine (not localhost) using both raw TCP (1883) and TLS/SSL (8883) (10 point)



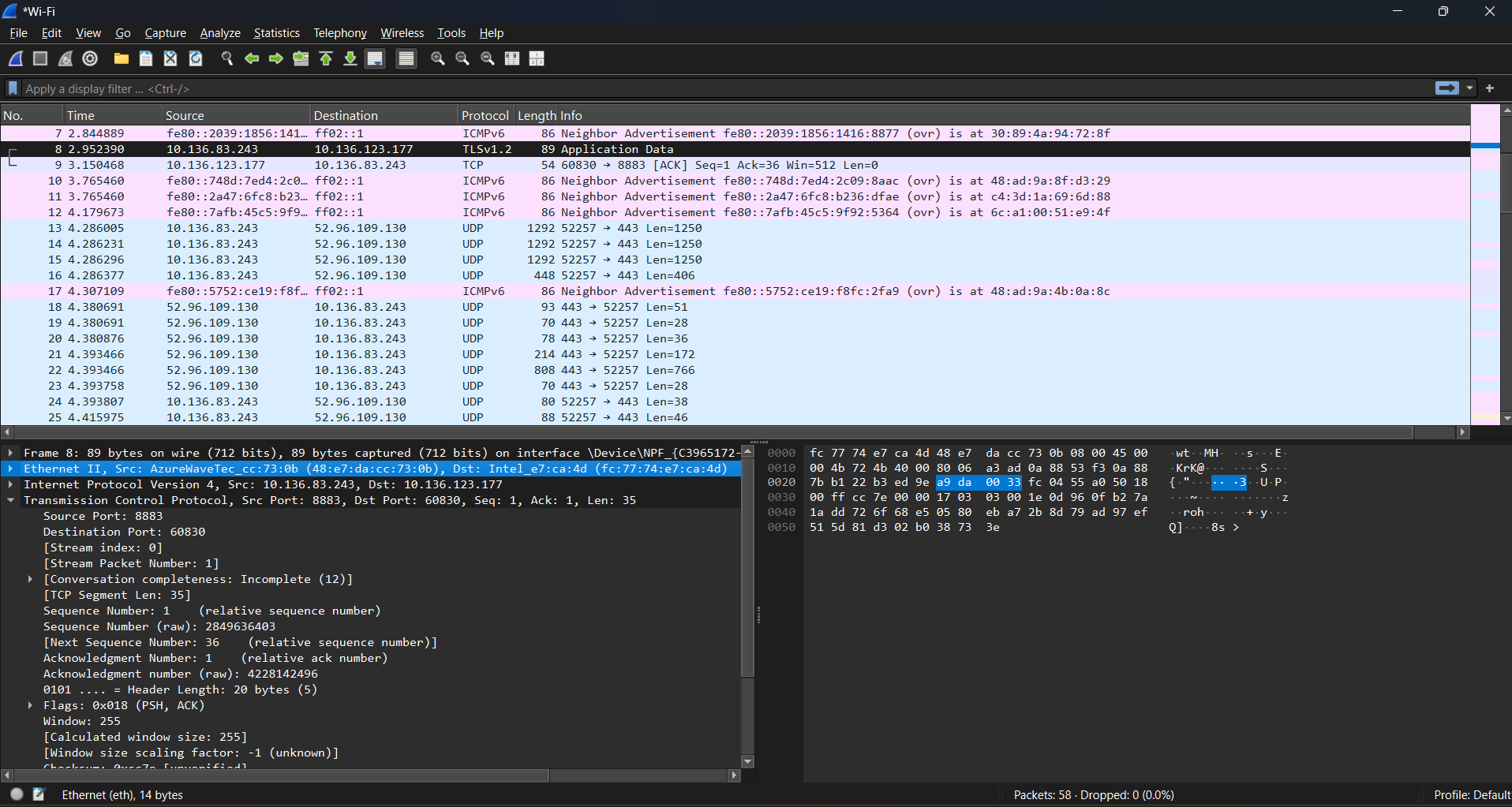
1. Partner A subscribes to /IoT on raw TCP, screen shot any packets in wireshark (10 point)

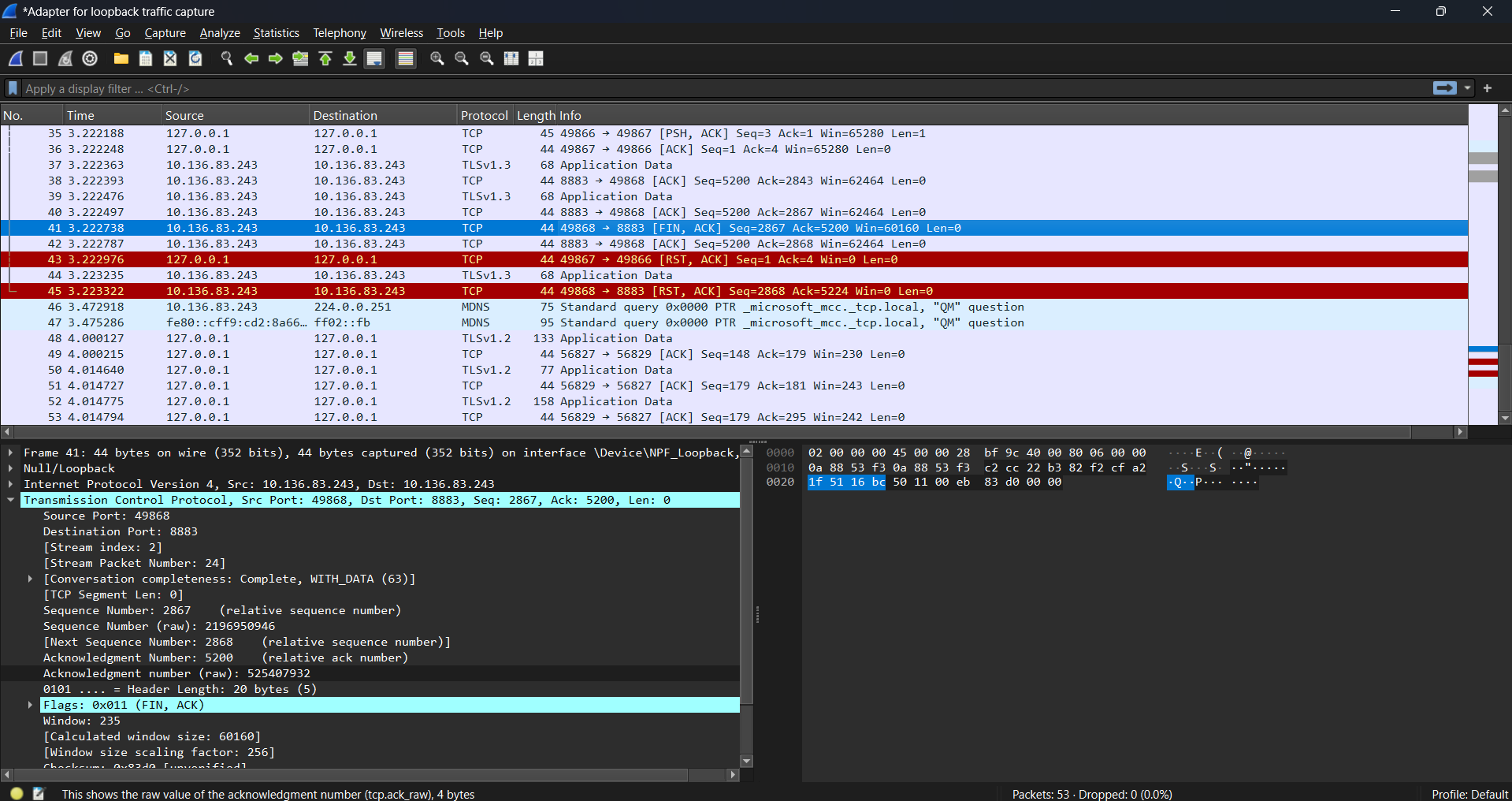


1. Partner B subscribes to /IoT\_secure on TLS/SSL, screenshot any packets in wireshark (10 point)

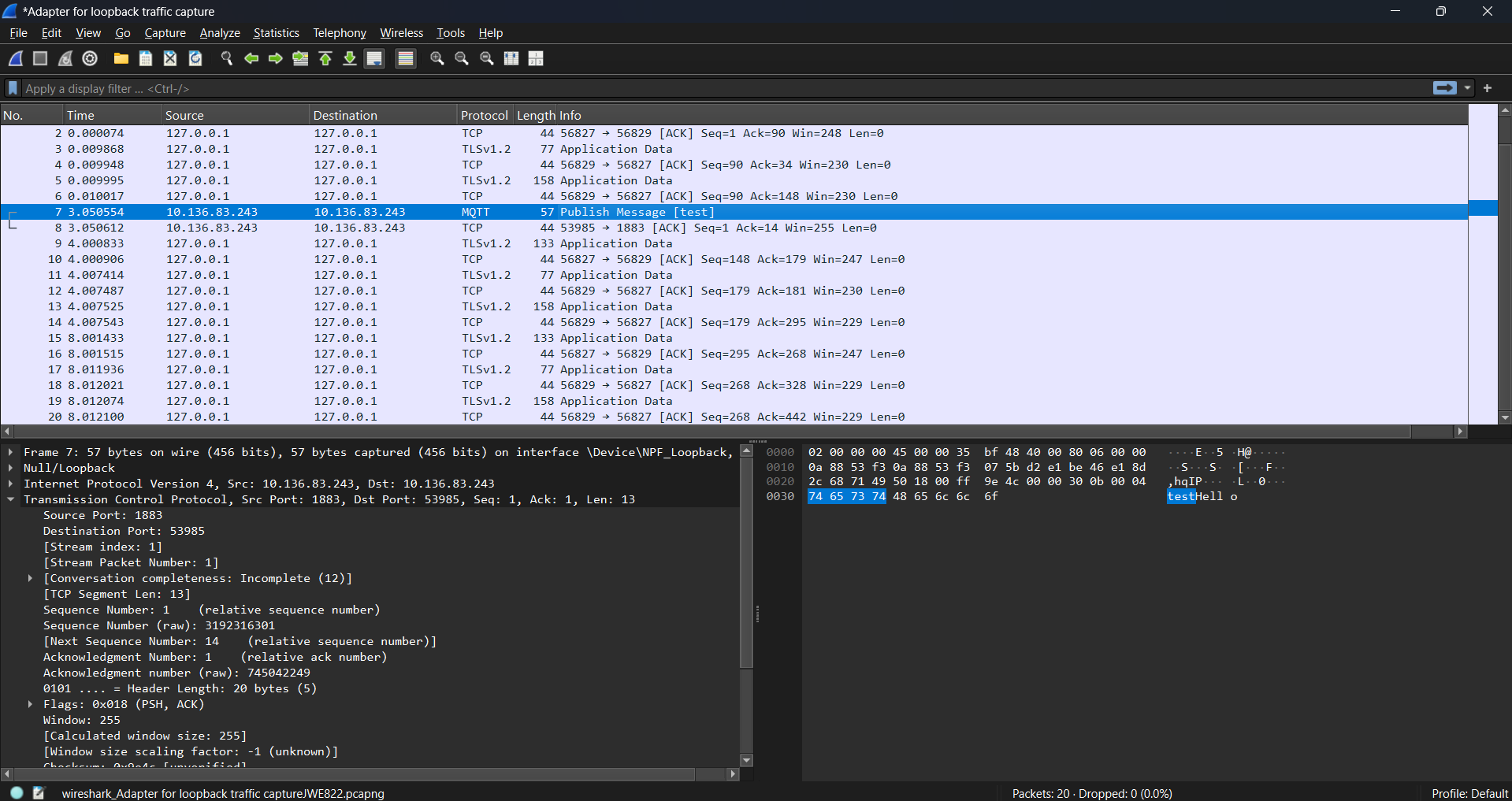


1. Partner A publishes to /IoT\_secure on TLS/SSL, screenshot any packets in wireshark (10 point)





1. Partner B publishes /IoT on raw TCP, screenshot any packets in wireshark (10 point)



1. List three ways wireshark may present a Threat to an IoT system. (9 point)
2. Wireshark can allow for eavesdropping on sensitive data as it can capture and inspect the traffic passing through the network. If an IoT system sends sensitive data, like user credentials, device commands, and/or personal information, it can be eavesdropped on using Wireshark. Generally, the information from HTTP servers indicates it is MQTT without TLS, so the messages are unencrypted for public viewing. Whole HTTPS connections indicate TLS/SSL, which uses encryption protocols to protect data.
3. Man-in-the-Middle Attacks are also possible with Wireshark, as an attacker can intercept communication between the IoT device and the server, modify the message, or inject commands.
4. Wireshark can allow for device fingerprinting where attackers can analyze patterns of network traffic. By doing so, they can learn things like device types by inspecting the protocols and communication patterns, firmware versions by analyzing traffic or identifying vulnerabilities in specific protocol versions, and IP addresses. With this information, they can target specific vulnerabilities based on the device type of firmware.
5. How can wireshark be used to better secure a system? (10 point)

With Wireshark it is possible to analyze packets on the network and identify unusual traffic patterns like unauthorized data transmission, unexpected protocol use, or large amounts of outgoing data that might indicate a breach or attempt. It can help identify common attack techniques when starting out for breach attempts. It also helps identify vulnerabilities where certain data is being sent unencrypted to change them to encrypted channels.

Only partner A comes up with certificate authority and their own certificates as well as partner B certificates, and then email partner B's certificates to partner B.

Look at port: netstat -an | findstr "1883"

Ping: ping <IP Addresss>

Find IP for Window: ipconfig

./mosquitto -c "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\mosquitto.conf" -v

Over TLS - 8883:

./mosquitto\_sub -h 10.136.83.243 -i "testSubTLS" -t "test" -p 8883 --cafile "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\PartnerACertifications\_ICreated\CA.crt.pem" --cert "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\PartnerACertifications\_ICreated\sub.crt.pem" --key "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\PartnerACertifications\_ICreated\sub.key.pem" -d

./mosquitto\_pub -h 10.136.83.243 -p 8883 -i "testPubTLS" -t "test" -m "Hello" --cafile "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\PartnerACertifications\_ICreated\CA.crt.pem" --cert "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\PartnerACertifications\_ICreated\pub.crt.pem"--key "C:\Users\Owner\CLionProjects\EEL-5739\_Internet-of-Things-Security-and-Privacy\Lab4\PartnerACertifications\_ICreated\pub.key.pem" -d

Over TCP – 1883:

./mosquitto\_sub -h 10.136.83.243 -p 1883 -i "testSubTCP" -t "test" -d

./mosquitto\_pub -h 10.136.83.243 -p 1883 -i "testPubTCP" -t "test" -m "Hello" -d