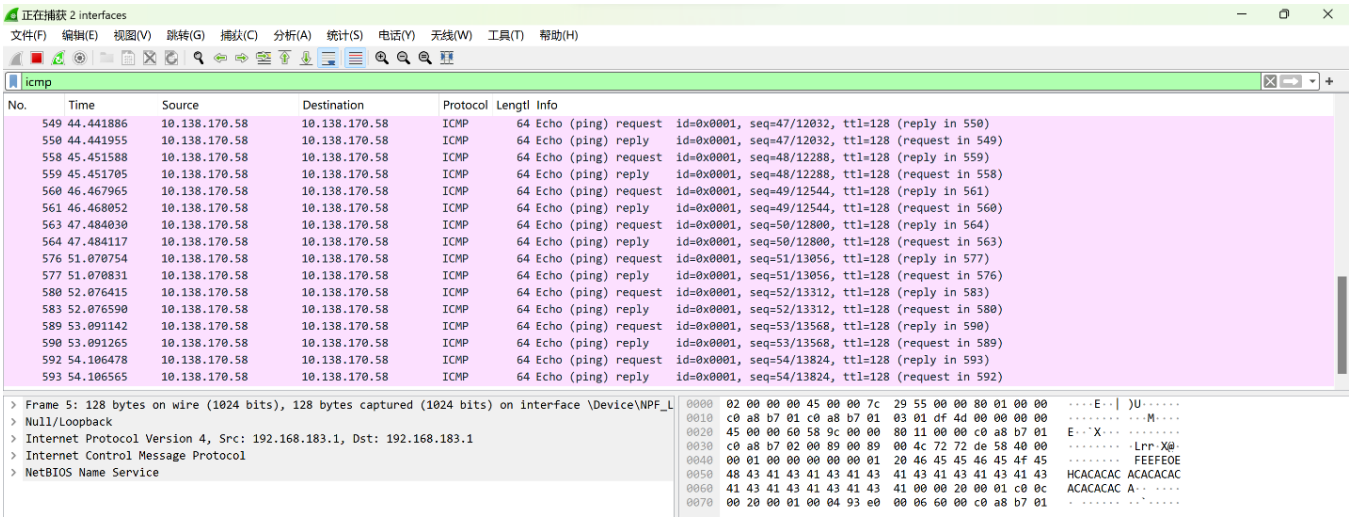
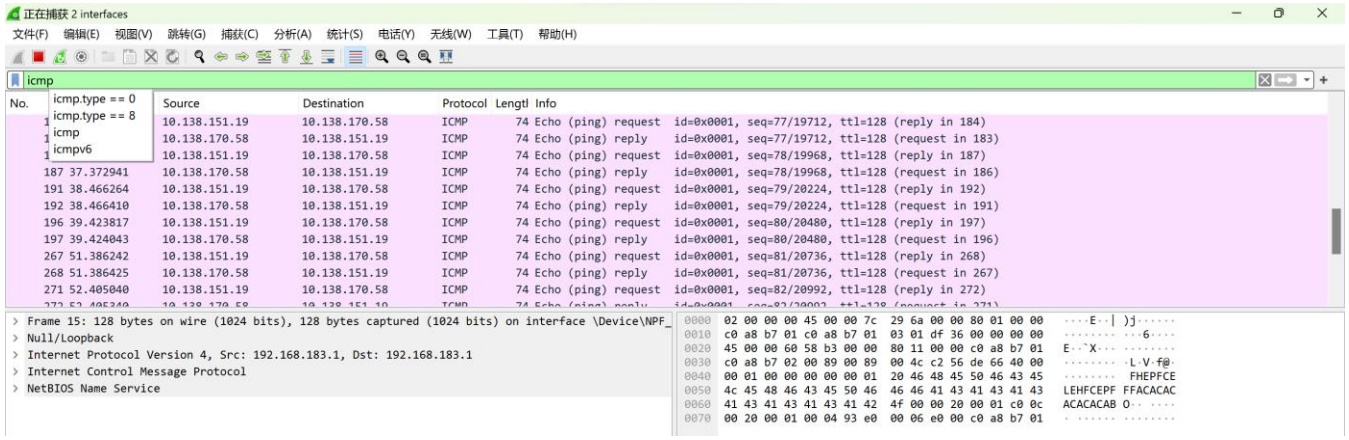
Lab 4: Basic Network Security

Wireshark:

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



2. B should ping A's address and screenshot the result in wireshark (5 point)



3. A and B should install mosquitto if you do not have it
4. A starts a mosquitto server capable of sending and receiving messages off A machine (not localhost) using both raw TCP (1883) and TLS/SSL (8883) (10 point)

```
C:\D\5739\lab\lab4>"C:\Program Files\mosquitto\mosquitto.exe" -v -c "C:\Program Files\mosquitto\mosquitto.conf"
1709927213: mosquitto version 2.0.18 starting
1709927213: Config loaded from C:\Program Files\mosquitto\mosquitto.conf.
1709927213: Opening ipv6 listen socket on port 1883.
1709927213: Opening ipv4 listen socket on port 1883.
1709927213: Opening ipv6 listen socket on port 8883.
1709927213: Opening ipv4 listen socket on port 8883.
1709927213: mosquitto version 2.0.18 running
```

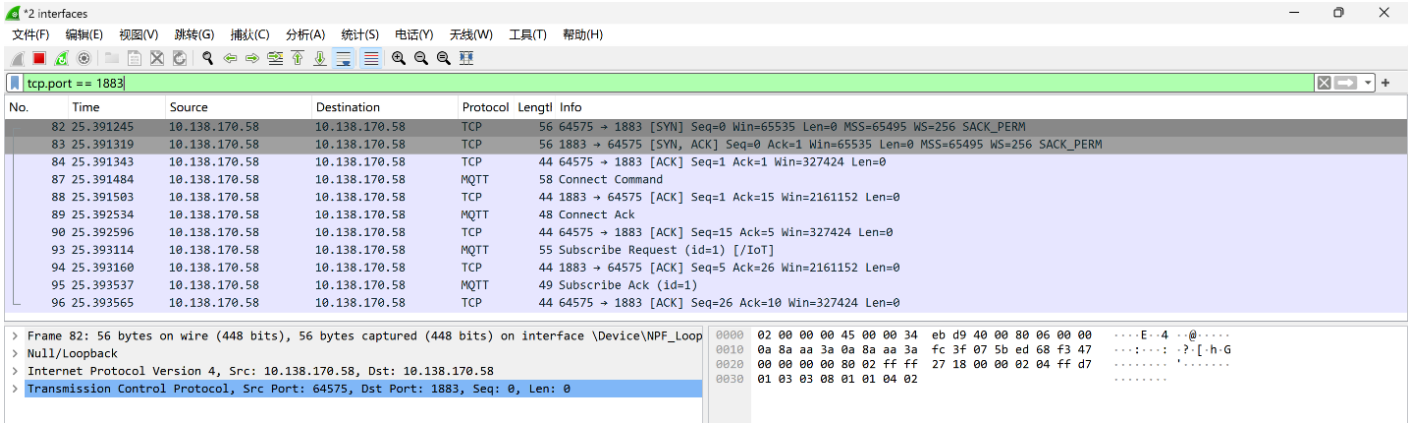
TEST(PORT 1883)

```
1709928492: New connection from 10.138.170.58:64548 on port 1883.
1709928492: New client connected from 10.138.170.58:64548 as auto-3C367550-3DF1-31D1-A039-022A250F9C12 (p2, c1, k60).
1709928492: No will message specified.
1709928492: Sending CONNACK to auto-3C367550-3DF1-31D1-A039-022A250F9C12 (0, 0)
1709928492: Received PUBLISH from auto-3C367550-3DF1-31D1-A039-022A250F9C12 (d0, q0, r0, m0, '/IoT', ... (7 bytes))
1709928492: Sending PUBLISH to auto-9B969BE9-011A-DE12-7045-4D79085093E8 (d0, q0, r0, m0, '/IoT', ... (7 bytes))
1709928492: Received DISCONNECT from auto-3C367550-3DF1-31D1-A039-022A250F9C12
```

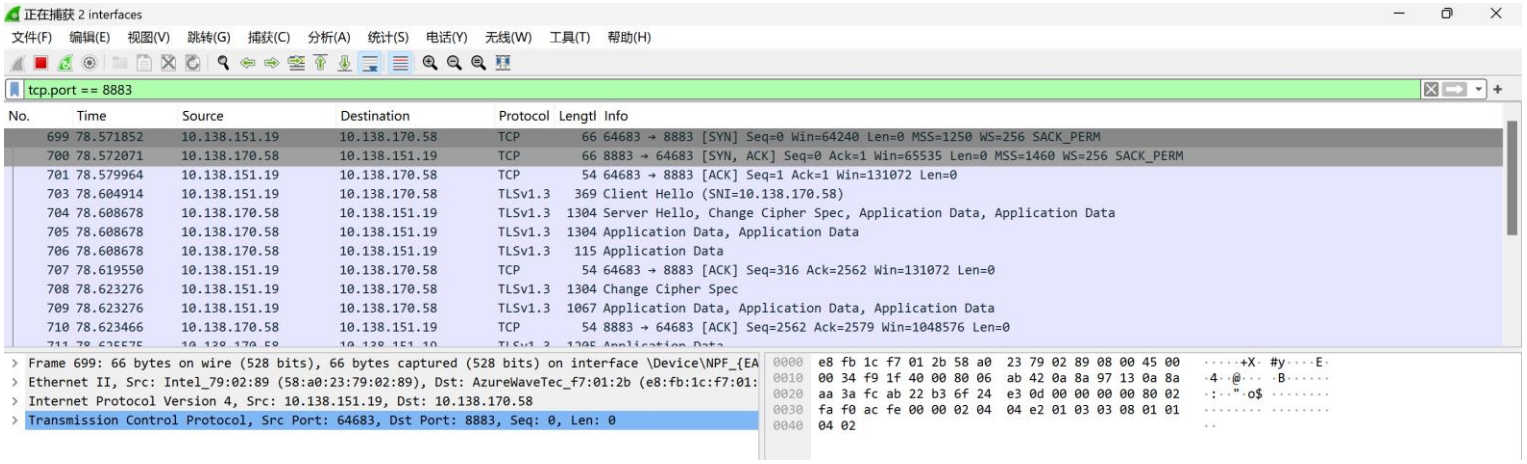
TEST(PORT 8883)

```
1709928355: New connection from 10.138.170.58:64537 on port 8883.
1709928355: New client connected from 10.138.170.58:64537 as auto-E0CC15CA-148D-D7C7-5F8D-7AC21F5AB82A (p2, c1, k60).
1709928355: No will message specified.
1709928355: Sending CONNACK to auto-E0CC15CA-148D-D7C7-5F8D-7AC21F5AB82A (0, 0)
1709928355: Received PUBLISH from auto-E0CC15CA-148D-D7C7-5F8D-7AC21F5AB82A (d0, q0, r0, m0, '/IoT_secure', ... (7 bytes
))
1709928355: Received DISCONNECT from auto-E0CC15CA-148D-D7C7-5F8D-7AC21F5AB82A
```

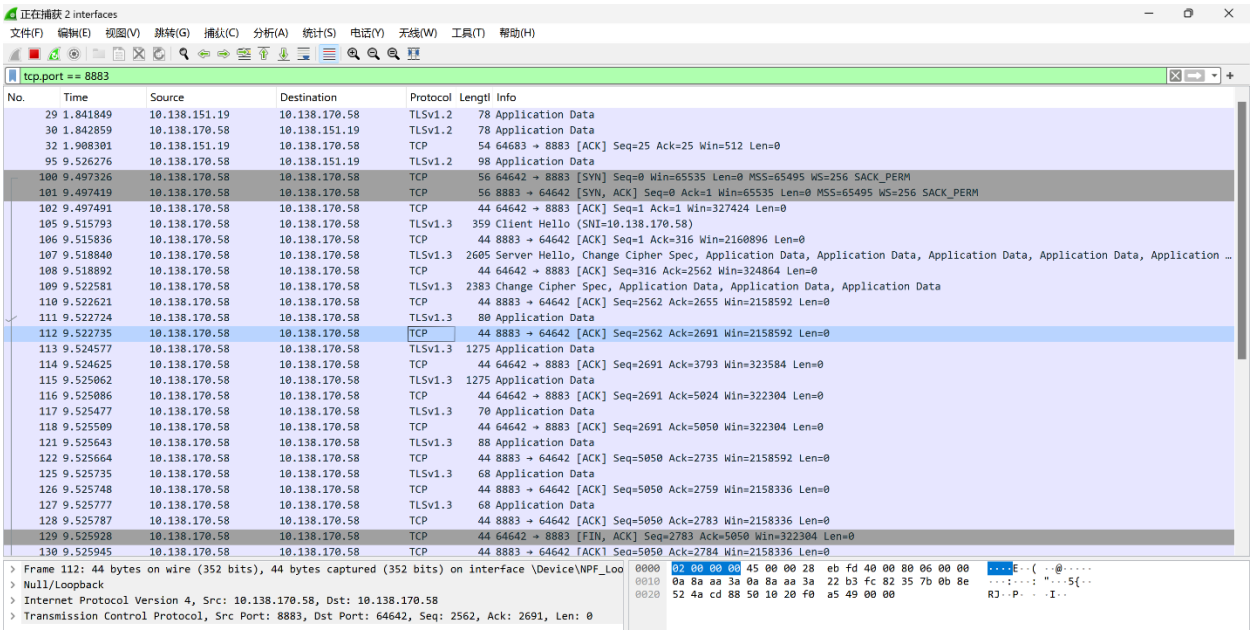
5. A subscribes to /IoT on raw TCP, screen shot any packets in wireshark (10 point)



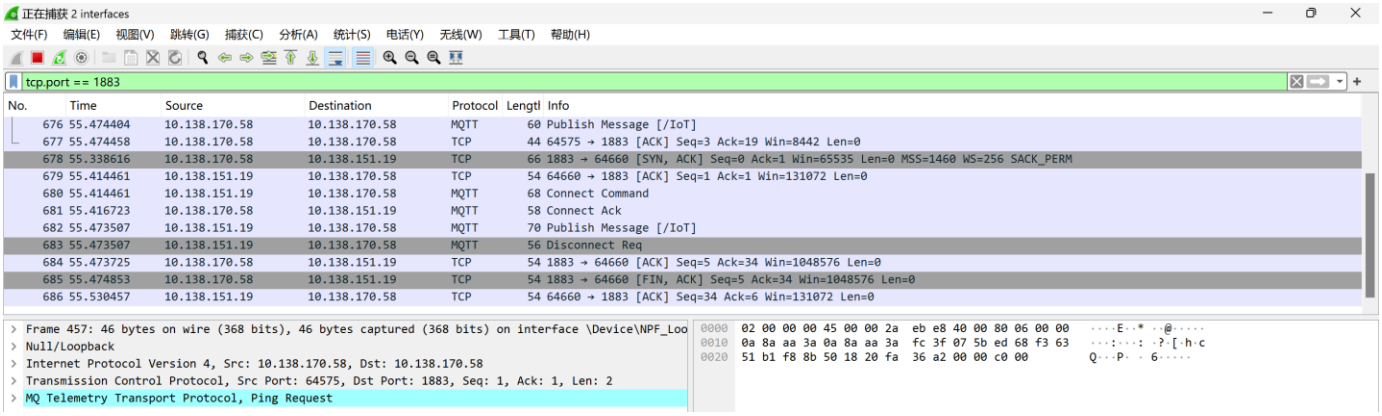
6. B subscribes to /IoT_secure on TLS/SSL, screenshot any packets in wireshark (10 point)



7. A publishes to /IoT_secure on TLS/SSL, screenshot any packets in wireshark (10 point)



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



9. List three ways wireshark may present a Threat to an IoT system. (9 point)

1.Data Interception and Eavesdropping: Wireshark can capture packets of data transmitted over a network, which includes IoT systems. If these IoT devices transmit sensitive information over unencrypted or weakly encrypted protocols, an attacker could use Wireshark to intercept and read this information. This could lead to the exposure of sensitive data such as personal information, login credentials, or proprietary data.

2.Network Traffic Analysis: By analyzing the traffic flow and patterns with Wireshark, an attacker could infer the behavior of IoT devices, identify when devices are communicating, and determine the nature of the communications. This could lead to a variety of attacks, including timing attacks where an attacker learns when systems are most vulnerable or when certain operations are being performed, allowing for more targeted intrusions.

3.Vulnerability Identification: Wireshark can be used to examine the details of protocols used by IoT devices. A malicious user could analyze this data to identify vulnerabilities in the implementation of these protocols. The attacker could then exploit these vulnerabilities to launch attacks against the device, such as man-in-the-middle attacks or denial of service attacks.

4.Disruption of Service: By analyzing traffic with Wireshark, an attacker could identify patterns or weaknesses in the communication protocols used by IoT devices. This knowledge could be used to craft and inject malicious packets into the network, potentially disrupting the normal operation of IoT devices. Such disruptions could range from degrading device performance to completely disabling devices, leading to a denial of service for users depending on those IoT systems for critical functions.

5.Device Fingerprinting and Enumeration: Wireshark can be used to capture packets that help in fingerprinting devices on the network. By analyzing specific characteristics of the captured traffic, an attacker can enumerate devices on a network. This information can be used to identify vulnerable or high-value targets for more focused attacks.

10. How can wireshark be used to better secure a system? (10 point)

1. Detection of Malicious Activity: By monitoring network traffic, Wireshark can help identify unusual patterns that may indicate malicious activity, such as constant high traffic volumes (potential DoS attacks), unrecognized protocols which might be used by malware, or unexpected communication between devices.

2. Network Health and Performance Monitoring: Regular monitoring with Wireshark can provide insights into the network's performance and health, enabling the identification and troubleshooting of issues before they become significant problems. This can include detecting packet losses, unusual latency, or bandwidth issues that could indicate a security problem or compromise.

3. Verification of Network Encryption: Wireshark can be used to verify that data transmitted by IoT devices and other systems is appropriately encrypted. By inspecting the encrypted communication, administrators can ensure that sensitive information is protected in transit, adhering to best practices for data privacy and security.

4. Policy Enforcement and Compliance: Wireshark can audit network traffic to ensure compliance with organizational or industry-specific security policies and standards. This includes verifying that only allowed protocols and ports are in use, ensuring that devices are communicating as expected, and that no policy violations are occurring which could compromise security.

5. Identification and Analysis of Unknown Protocols: In an IoT ecosystem, devices might use proprietary or less common protocols. Wireshark, with its extensive protocol dissectors, can be used to understand these protocols better, analyze their security features, and identify potential vulnerabilities or misconfigurations that could be exploited.