Lab 2: Capture and Analyze IoT Device Traffic

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge to capture and analyze the traffic between IoT devices. Using various tools and techniques, you can capture the valuable data flowing between the IoT devices, analyze it to obtain information on the communication protocol used by the IoT devices, and acquire sensitive information such as credentials, device identification numbers, etc.

Lab Objectives

- Capture and analyze IoT traffic using Wireshark

Overview of IoT and OT Traffic

Many IoT devices such as security cameras host websites for controlling or configuring cameras from remote locations. These websites mostly implement the insecure HTTP protocol instead of the secure HTTPS protocol and are, hence, vulnerable to various attacks. If the cameras use the default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web applications and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi keys of the target network.

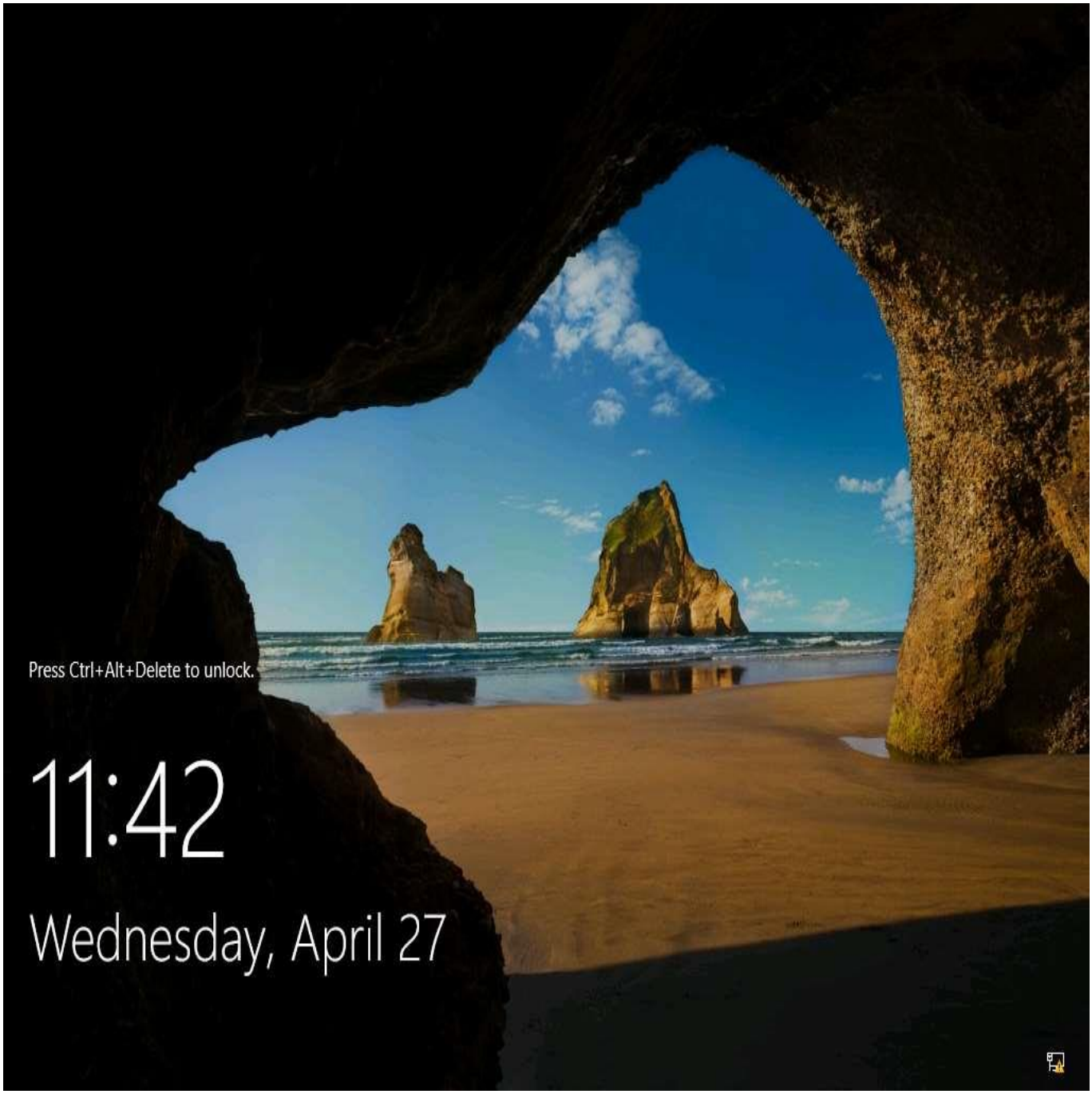
Task 1: Capture and Analyze IoT Traffic using Wireshark

Wireshark is a free and open-source packet analyzer. It facilitates network troubleshooting, analysis, software and communications protocol development, and education. It is used to identify the target OS and sniff/capture the response generated from the target machine to the machine from which a request originates.

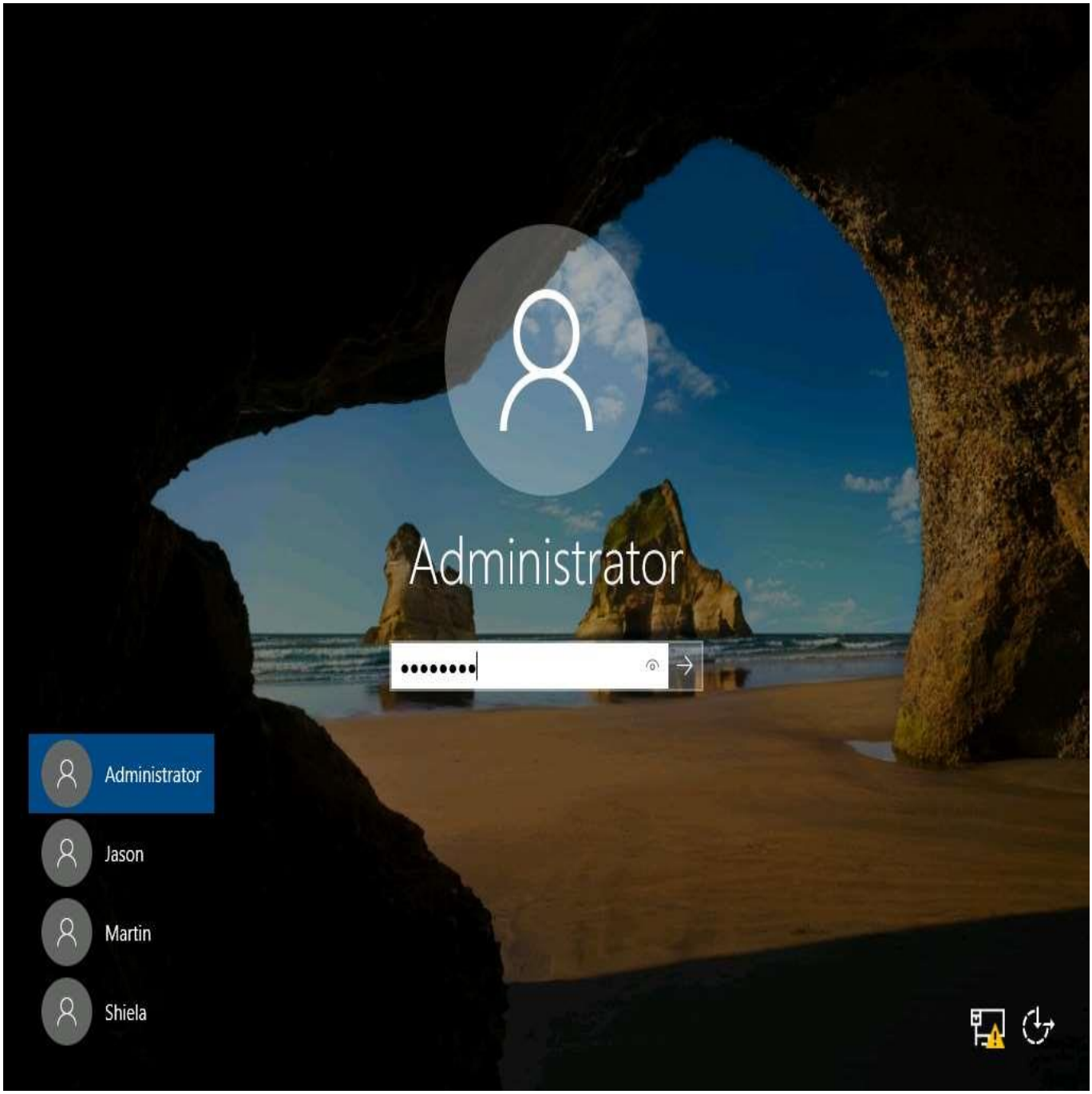
MQTT is a lightweight messaging protocol that uses a publish/subscribe communication pattern. Since the protocol is meant for devices with a low-bandwidth, it is considered ideal for machine-to-machine (M2M) communication or IoT applications. We can create virtual IoT devices over the virtual network using the Bevywise IoT simulator on the client side and communicate these devices to the server using the MQTT Broker web interface. This interface collects data and displays the status and messages of connected devices over the network.

Here, we use Wireshark to capture and analyze traffic between IoT devices.

1. To install the **MQTT Broker** on the **Windows Server 2019**, click Windows Server 2019 to launch **Windows Server 2019** machine, and then click Ctrl+Alt+Delete link to login.

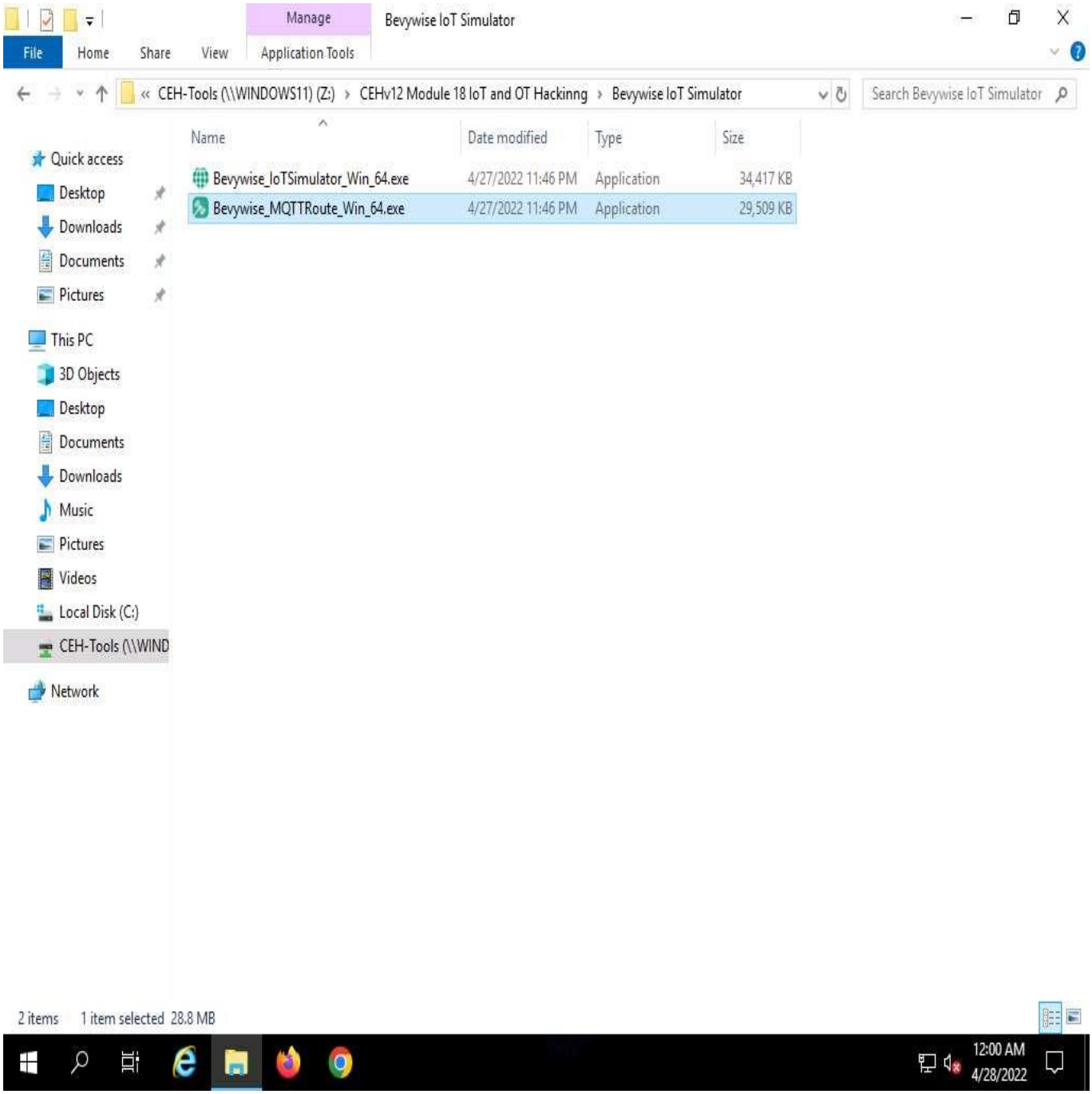


2. ☐ By default **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

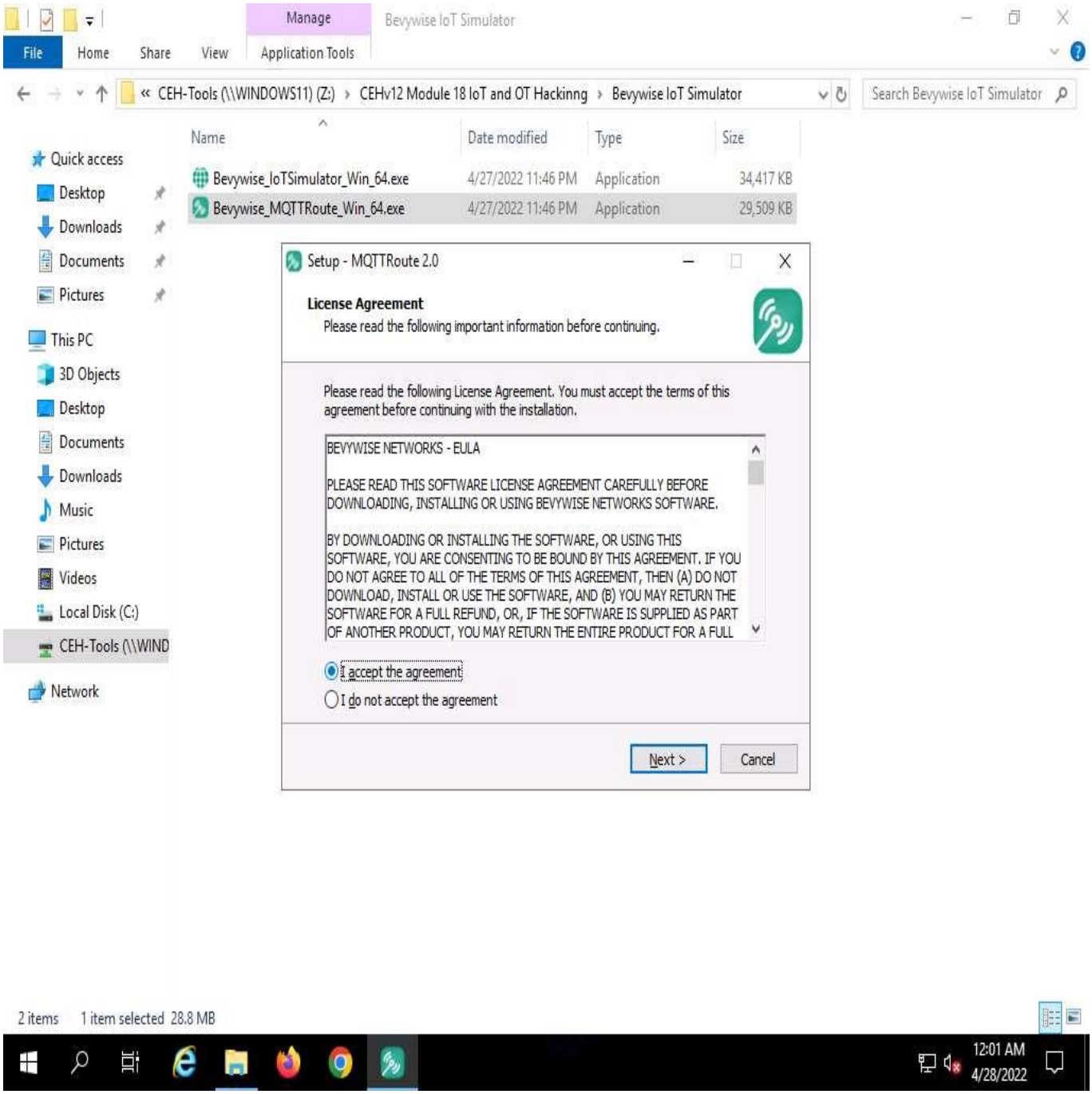


If the network screen appears, click **Yes**.

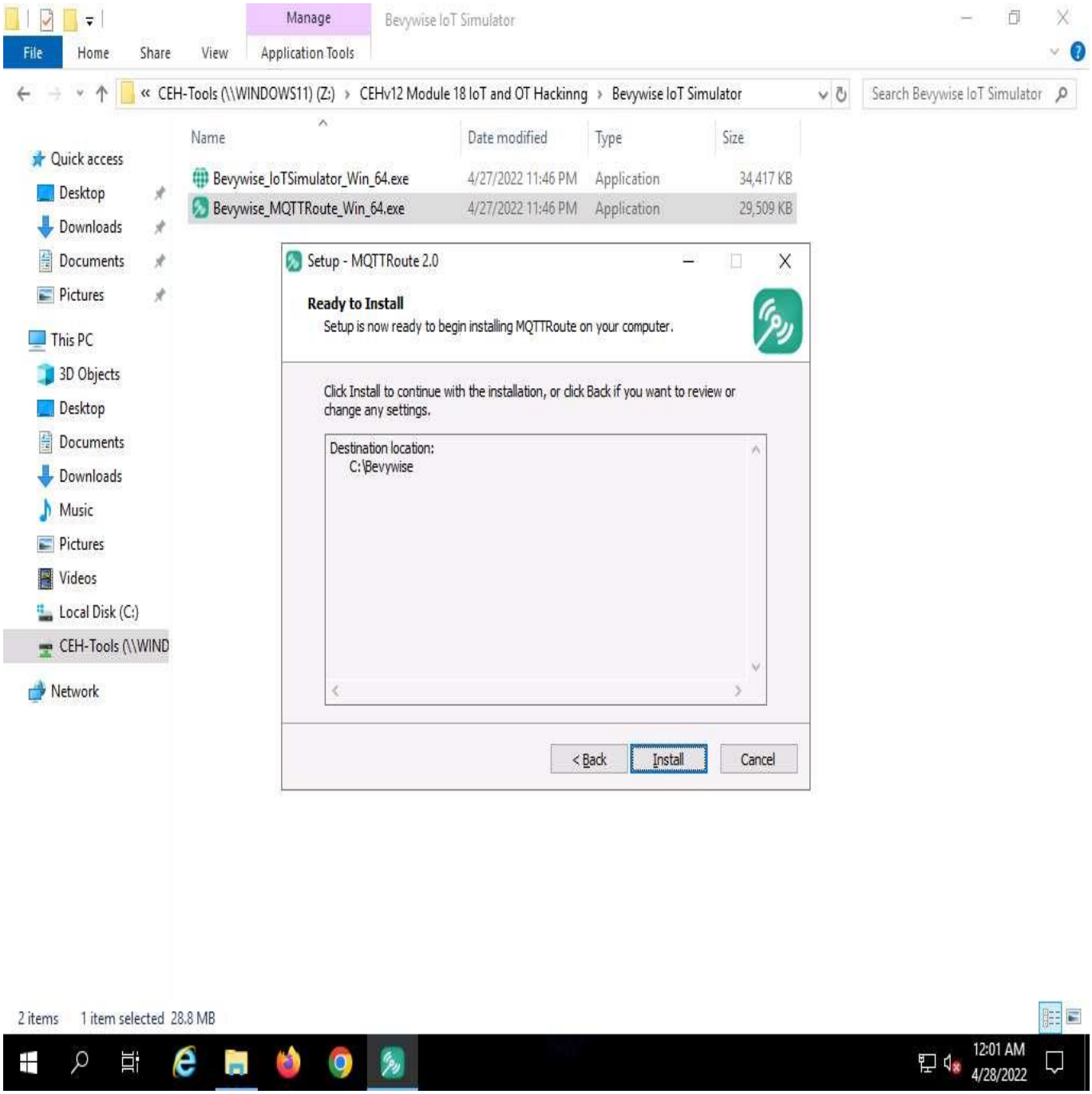
3. Navigate to **Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator** folder and double-click on the **Bevywise_MQTTRoute_Win_64.exe** file.



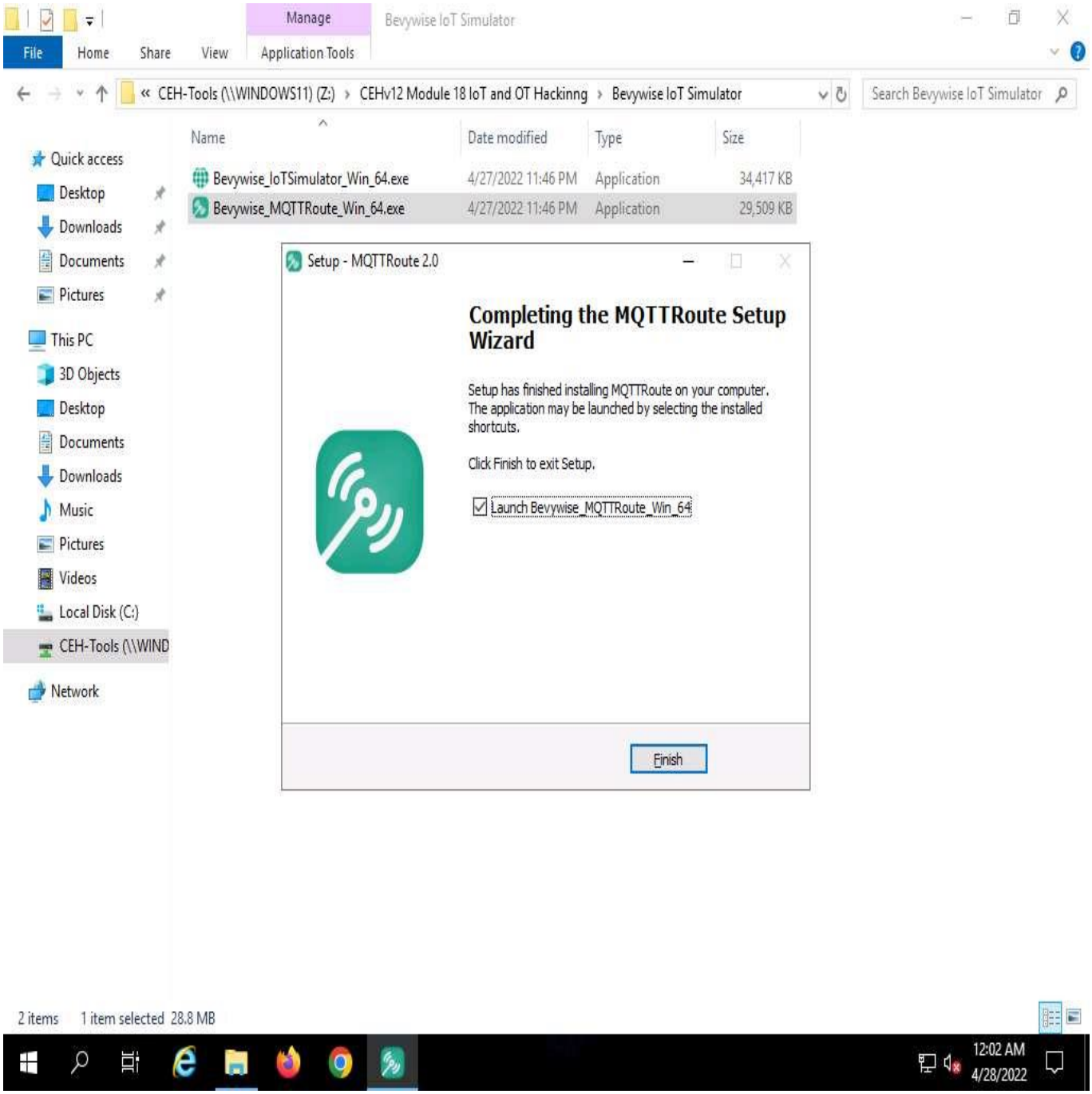
4. ☐ The **Open File - Security Warning** popup appears. Click **Run**.
5. ☐ The **Setup – MQTTRoute 2.0** window opens. Select **I accept the agreement** and click on **Next**.



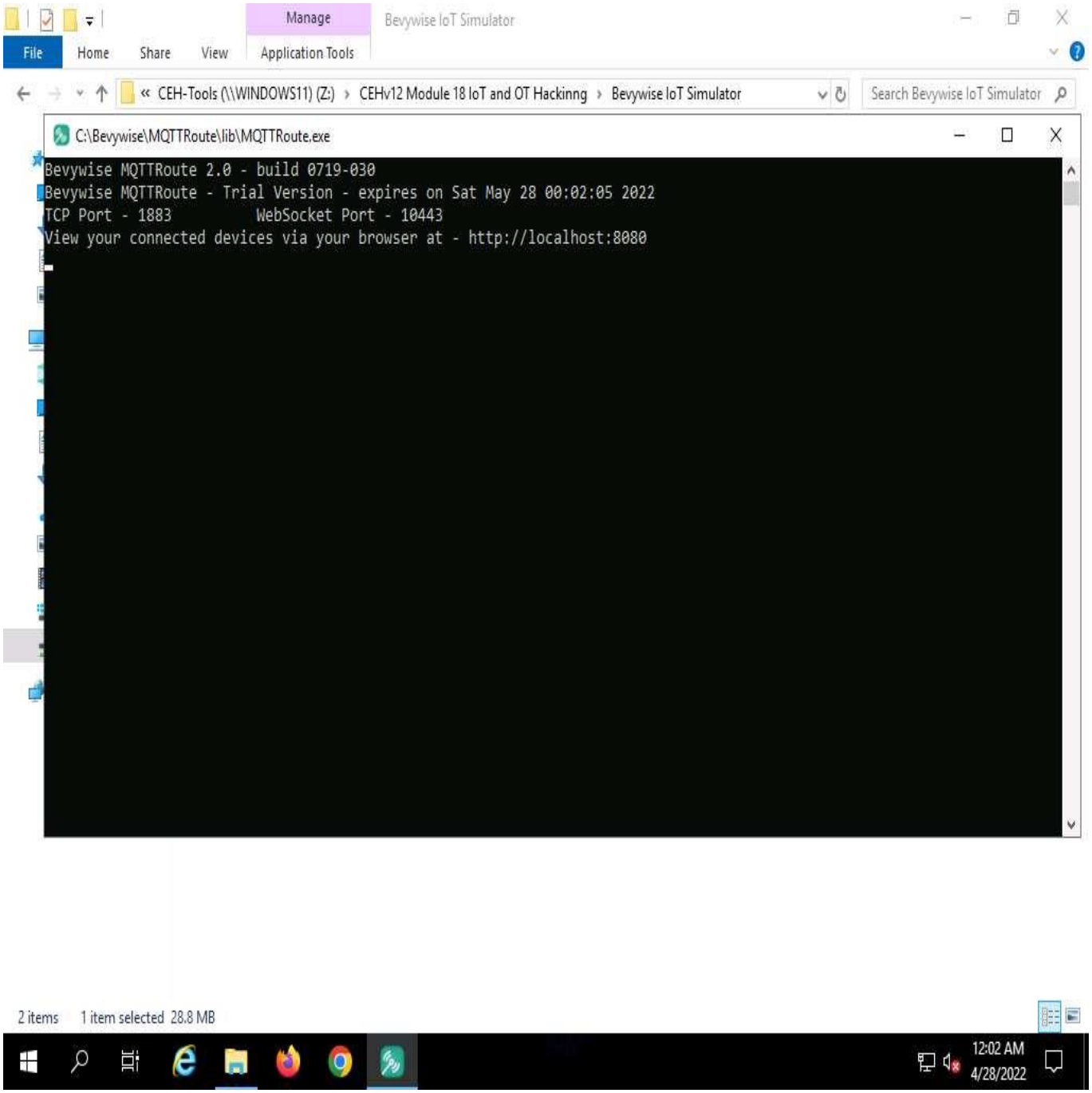
6. ☐ **Select Destination Location** page appears, without making any changes to the default installation location, click on **Next**.
7. ☐ In the next window, click **Install** to complete the installation.



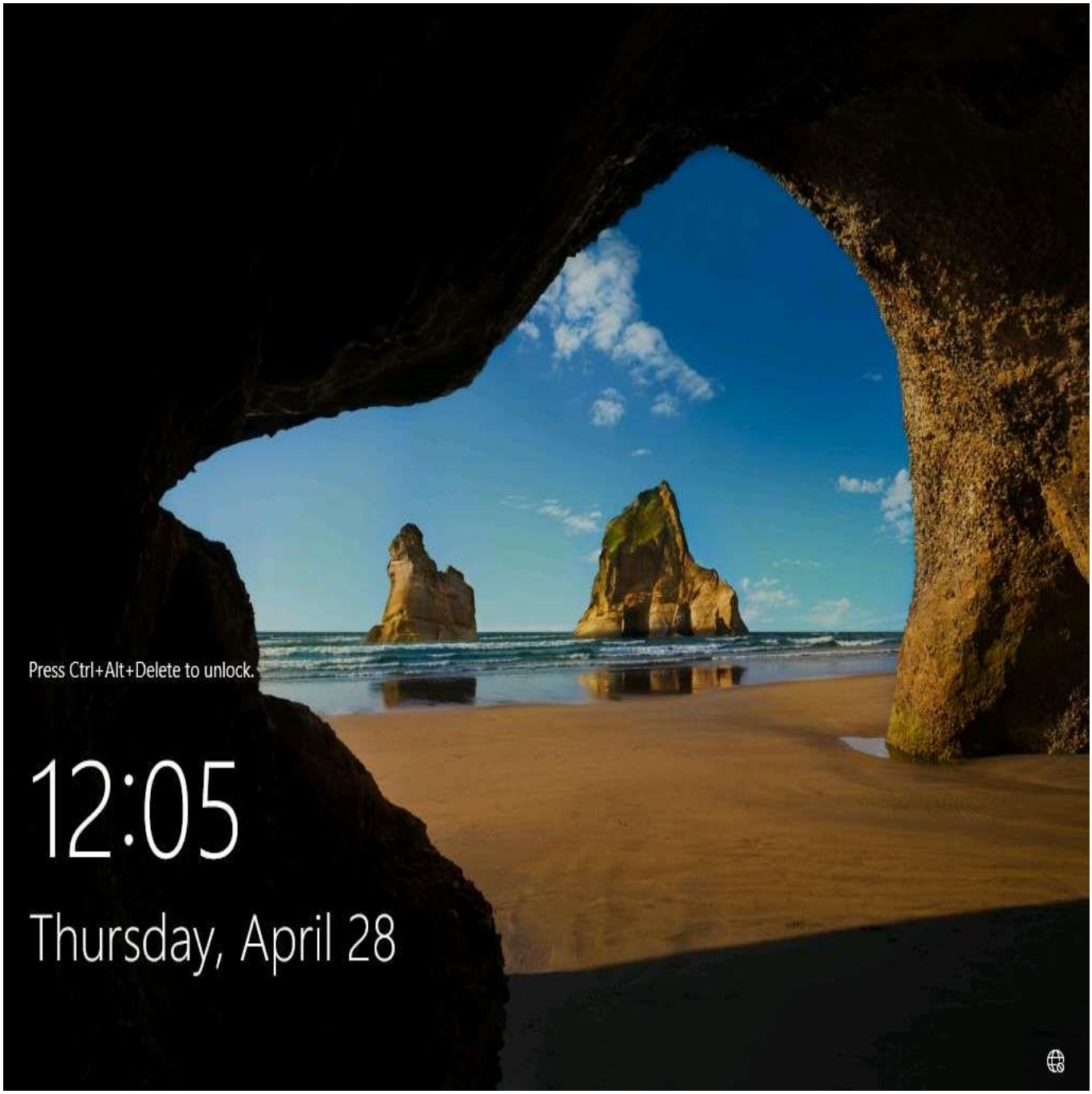
8. ☐ The installation completes, click on **Finish**. Ensure that **Launch Bevywise_MQTTRoute_Win_64** is checked.



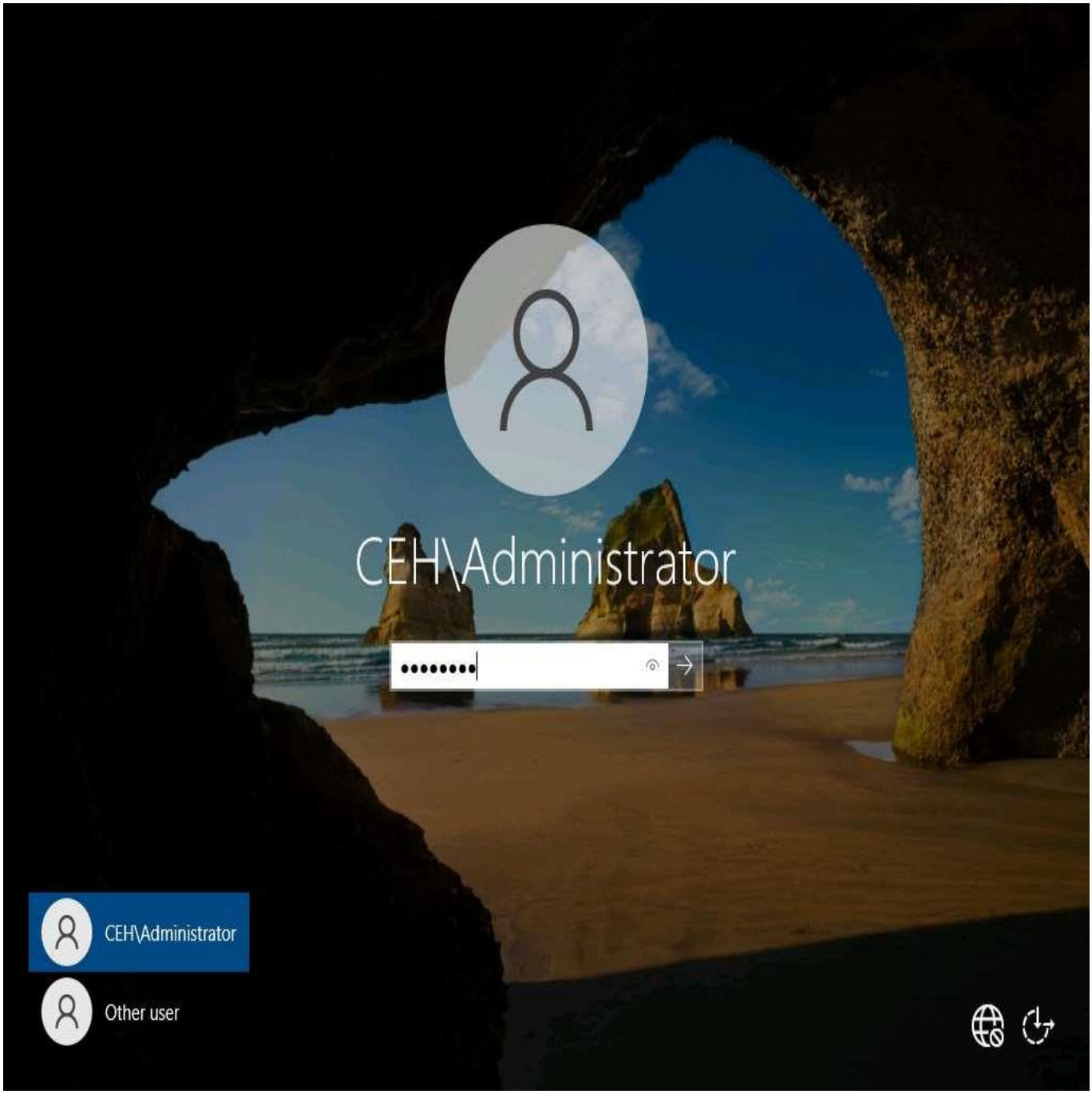
9. ☐ The MQTTRoute will execute and the command prompt will appear. You can see the **TCP** port using **1883**.



10. ☐ We have installed MQTT Broker successfully and leave the Bevywise MQTT **running**.
11. ☐ To create IoT devices, we must install the **IoT simulator** on the client machine.
12. ☐ Click Windows Server 2022 to launch **Windows Server 2022** machine. Click Ctrl+Alt+Delete.

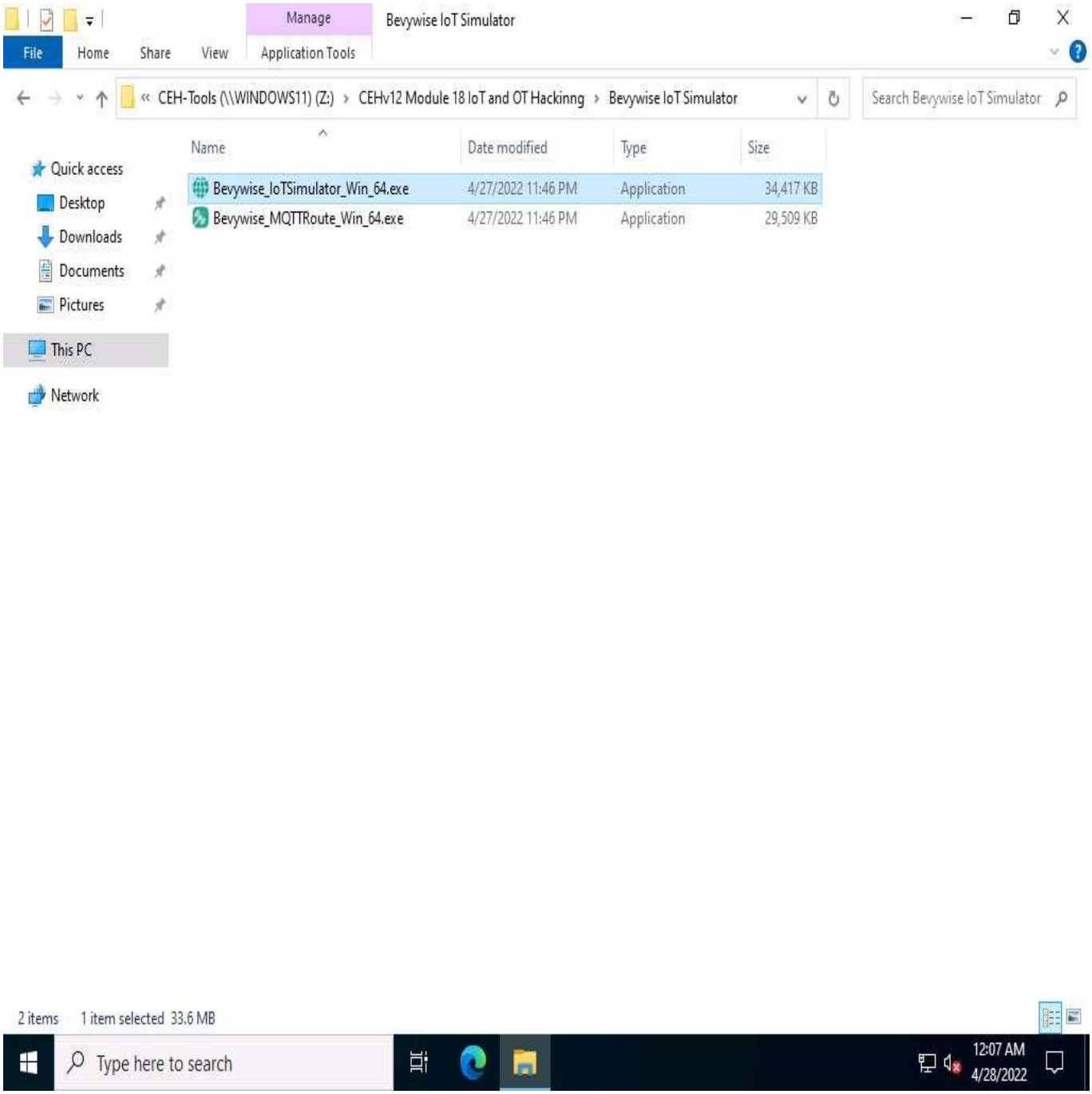


13. ☐ By default **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

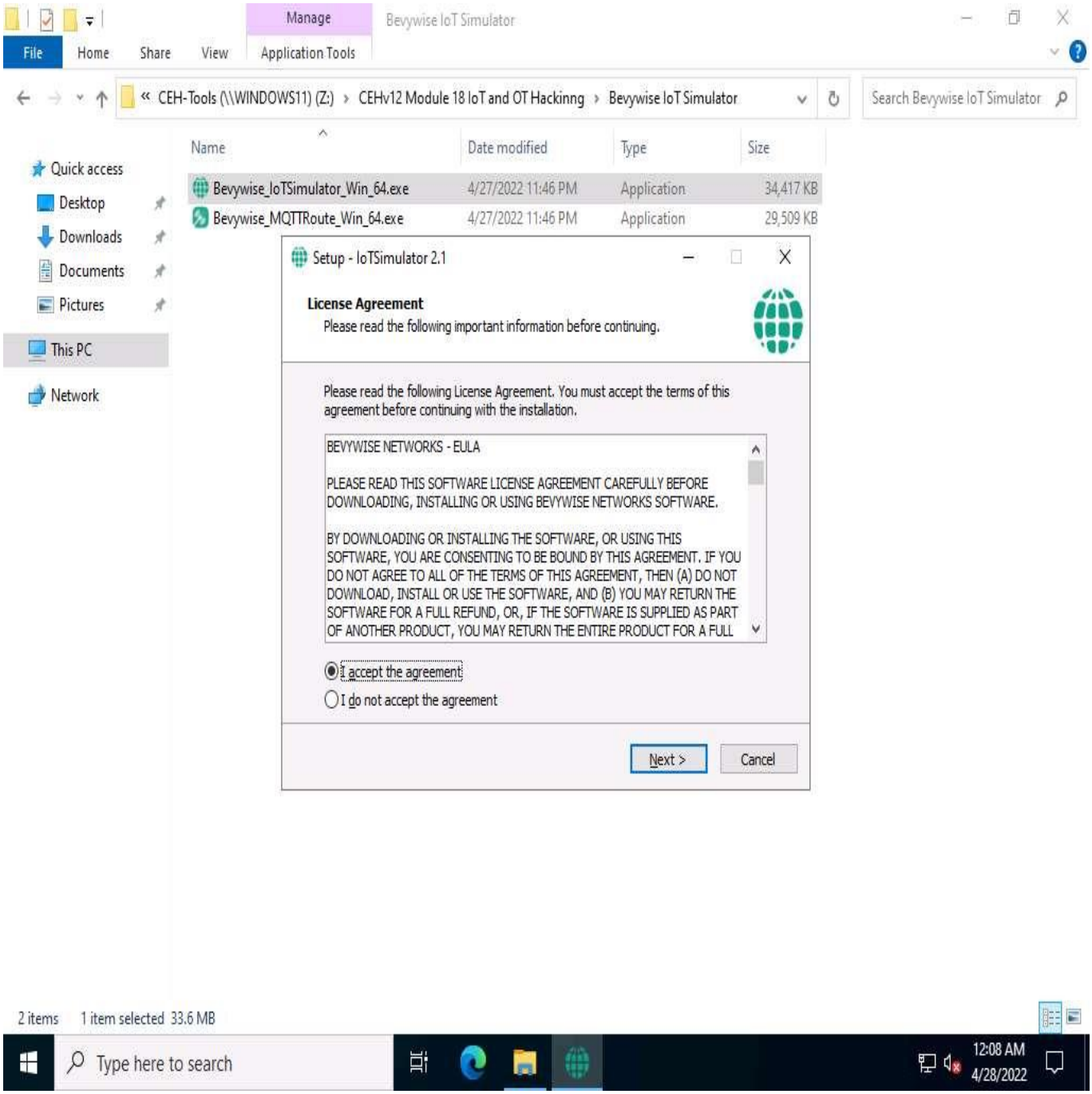


If the network screen appears, click **Yes**.

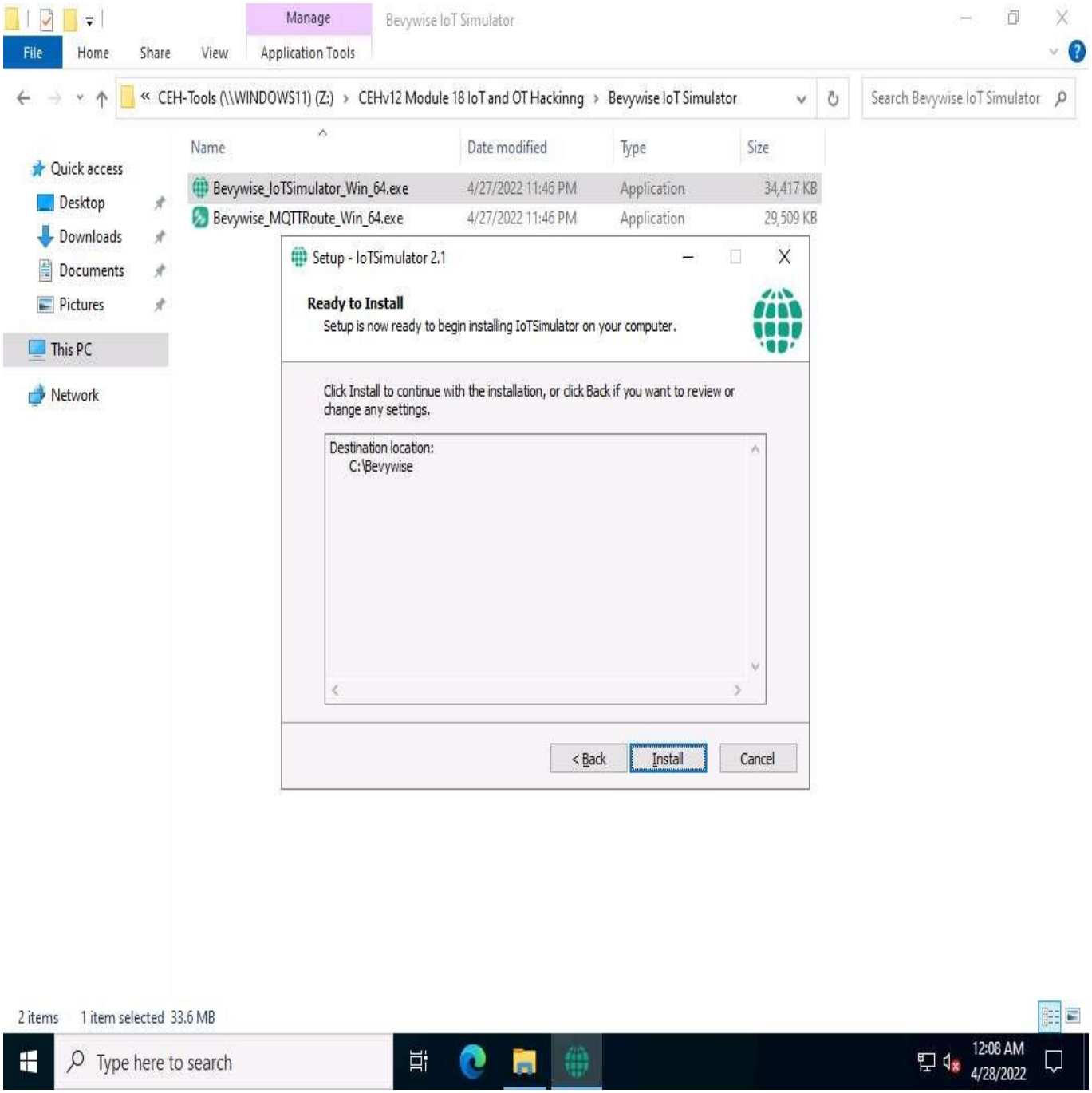
14. Navigate to **Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator** folder and double-click on the **Bevywise_IoTSimulator_Win_64.exe** file.



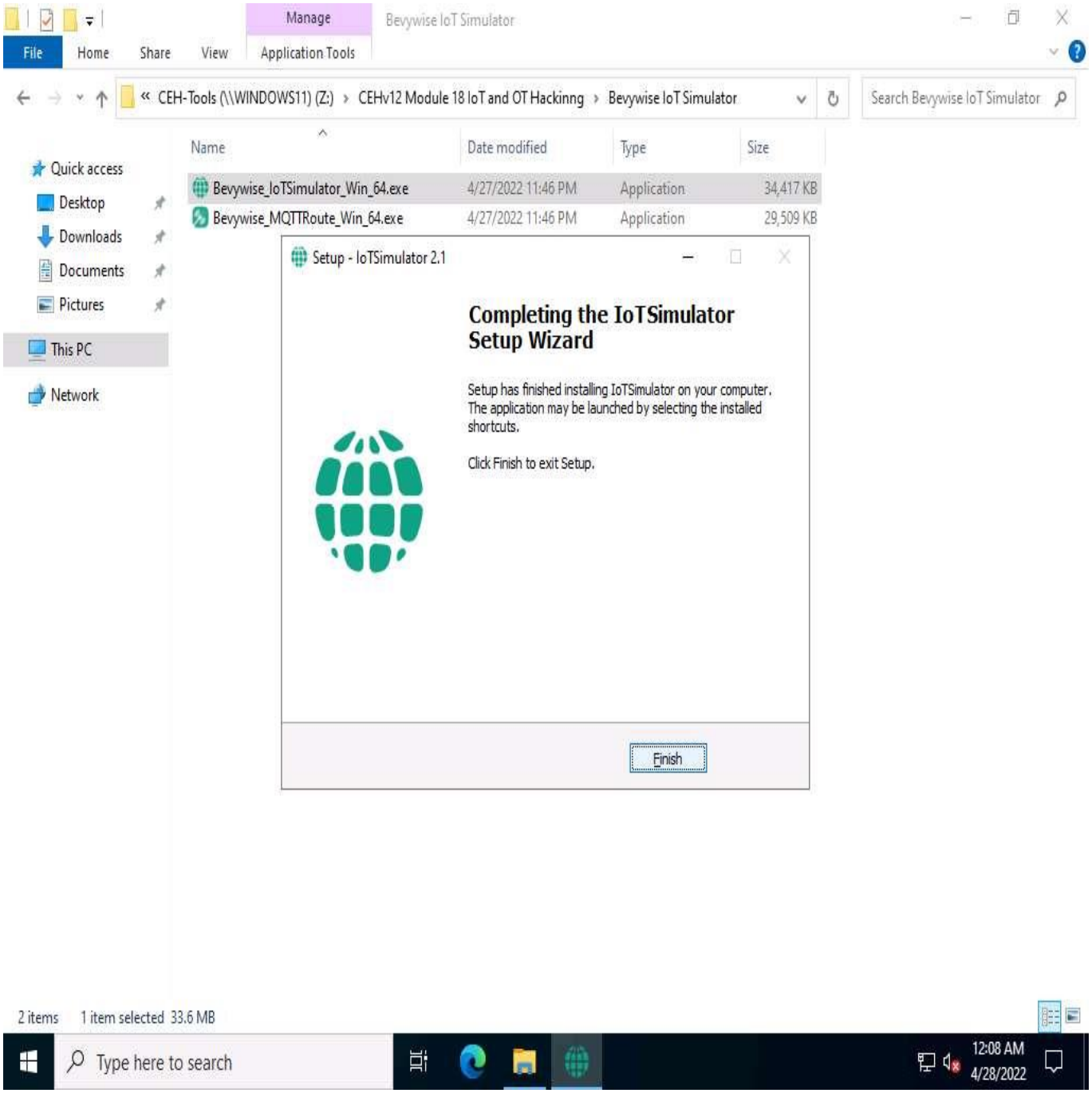
15. ☐ The **Open File - Security Warning** popup appears. Click **Run**..
16. ☐ The **Setup-IoTSimulator 2.1** setup wizard opens. Select **I accept the agreement** and click on **Next** to continue.



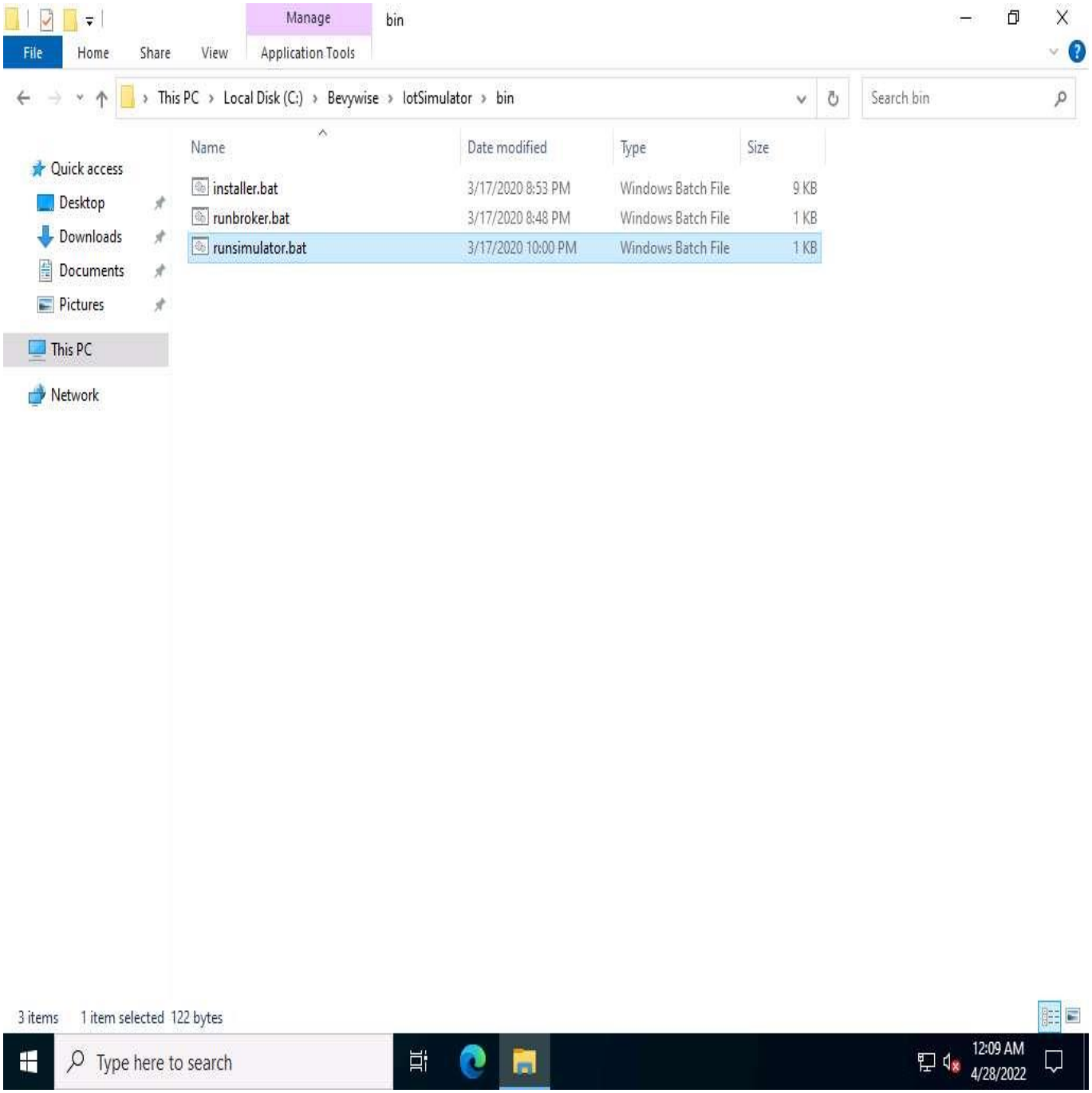
17. ☐ Keeping the default destination unchanged, click on **Next**.
18. ☐ The Ready to install screen appears, click on **Install**



19. ☐ Click on **Finish** to complete the installation.



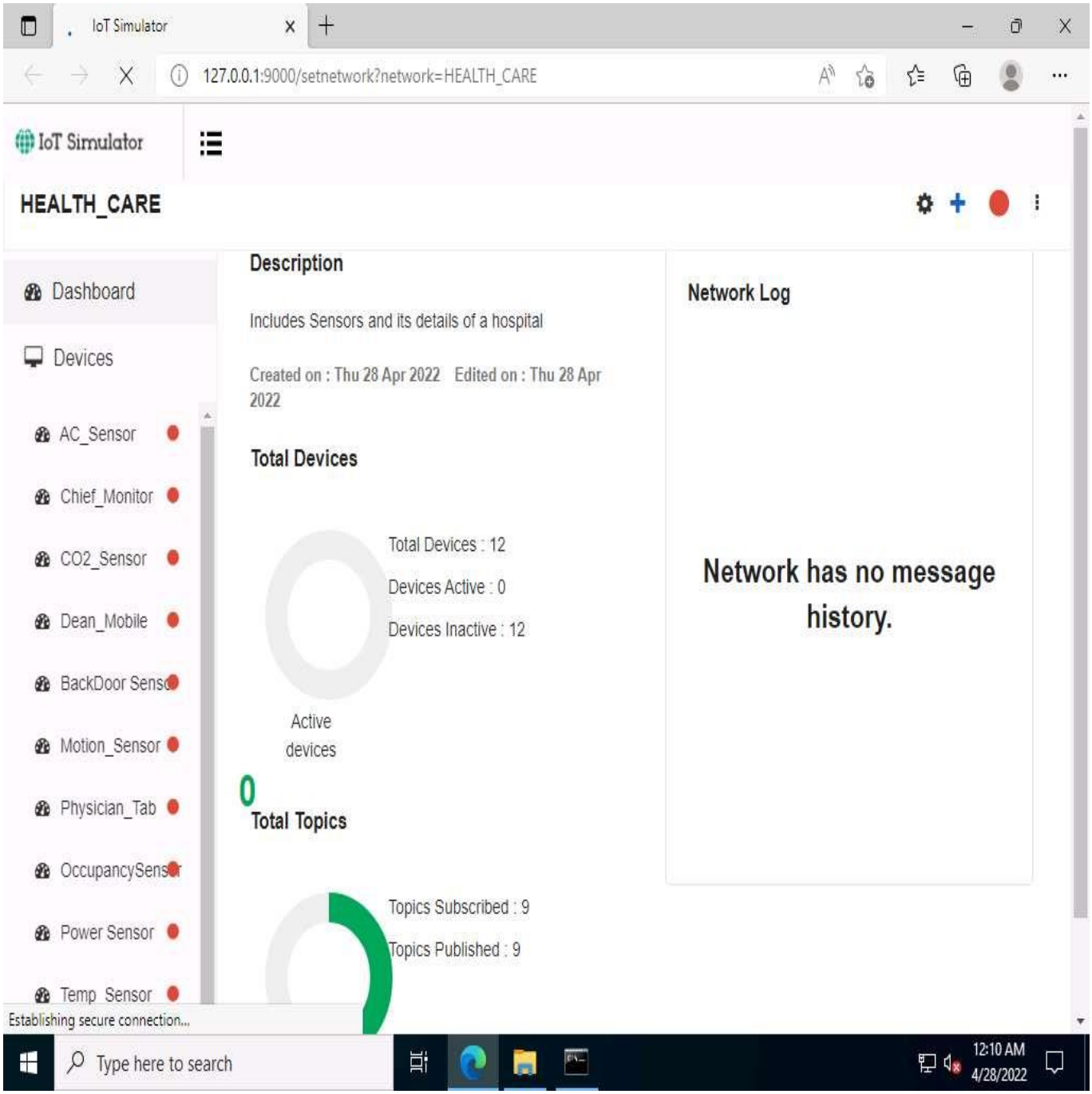
20. ☐ Bevywise IoT Simulator is installed successfully. To launch the **IoT simulator**, navigate to the **C:\Bevywise\IotSimulator\bin** directory and double-click on the **runsimulator.bat** file.



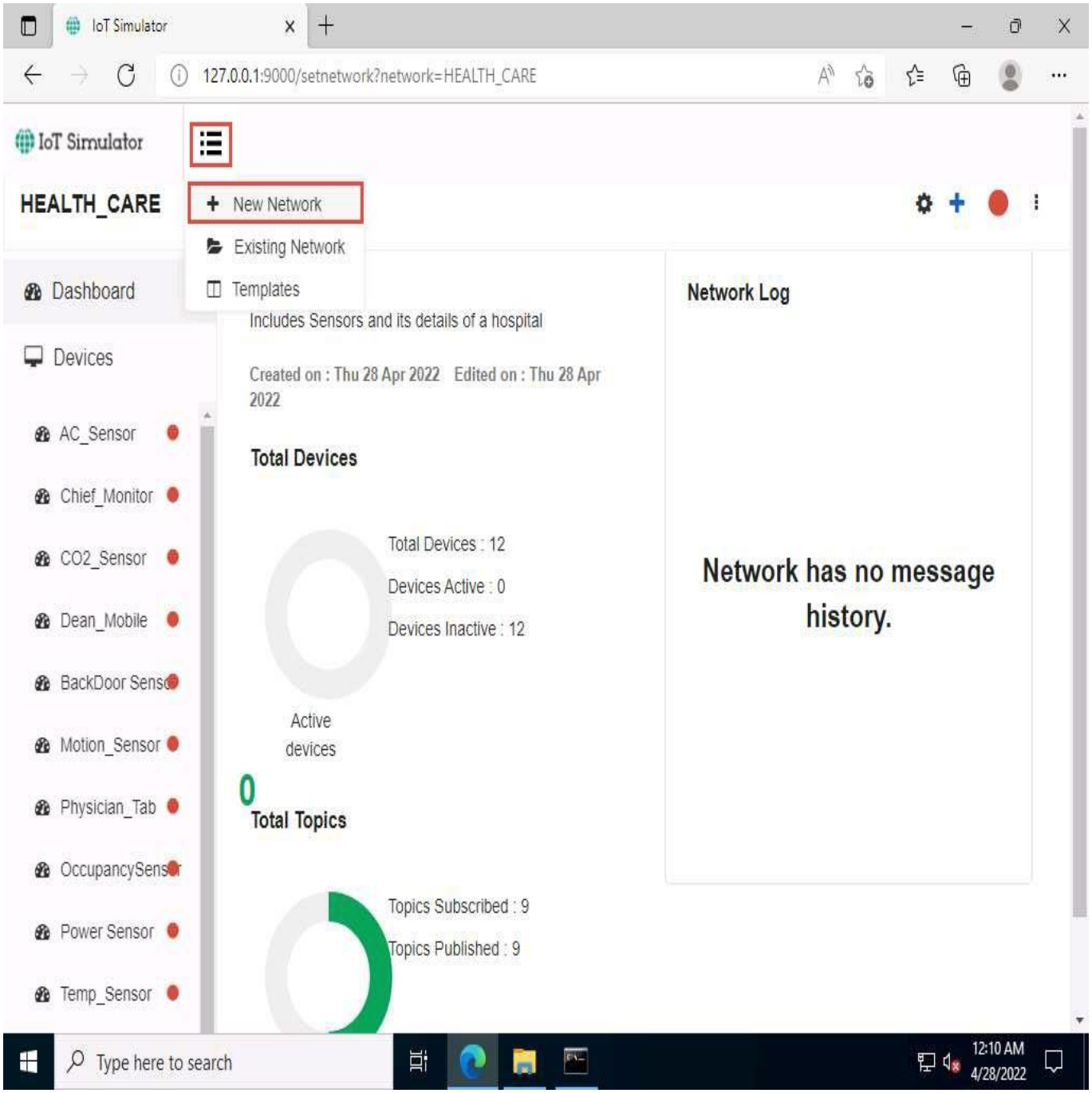
21. ☐ Upon double-clicking the **runsimulator.bat** file opens in the command prompt. If **How do you want to open this?** pop-up appears, select **Microsoft Edge** browser and click **OK** to open the URL **http://127.0.0.1:9000/setnetwork?network=HEALTH_CARE**.

If the URL directly opens in Microsoft Edge browser, then continue.

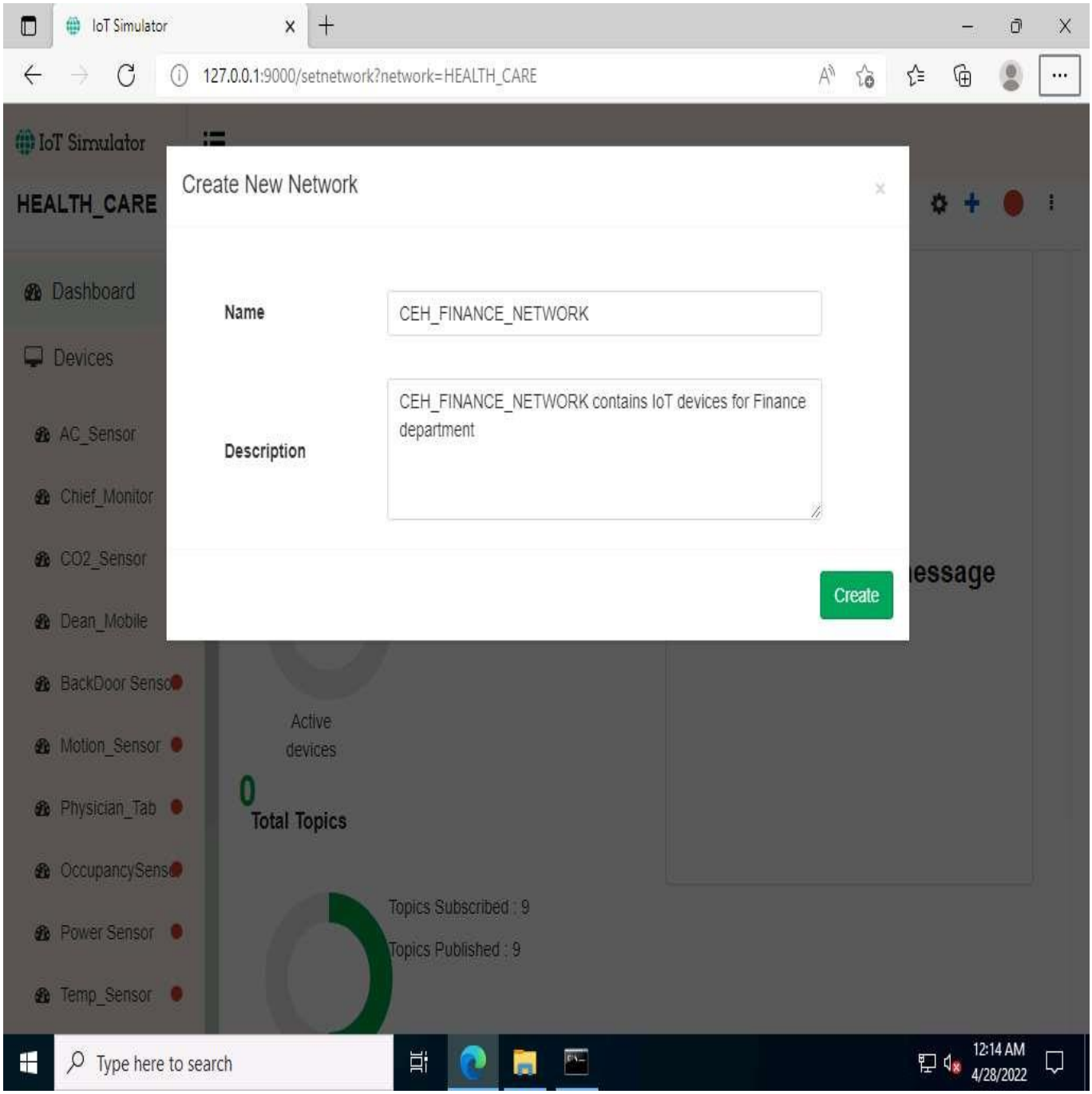
22. ☐ The web interface of the IoT Simulator opens in Edge browser. In the IoT Simulator, you can view the default network named **HEALTH_CARE** and several devices.



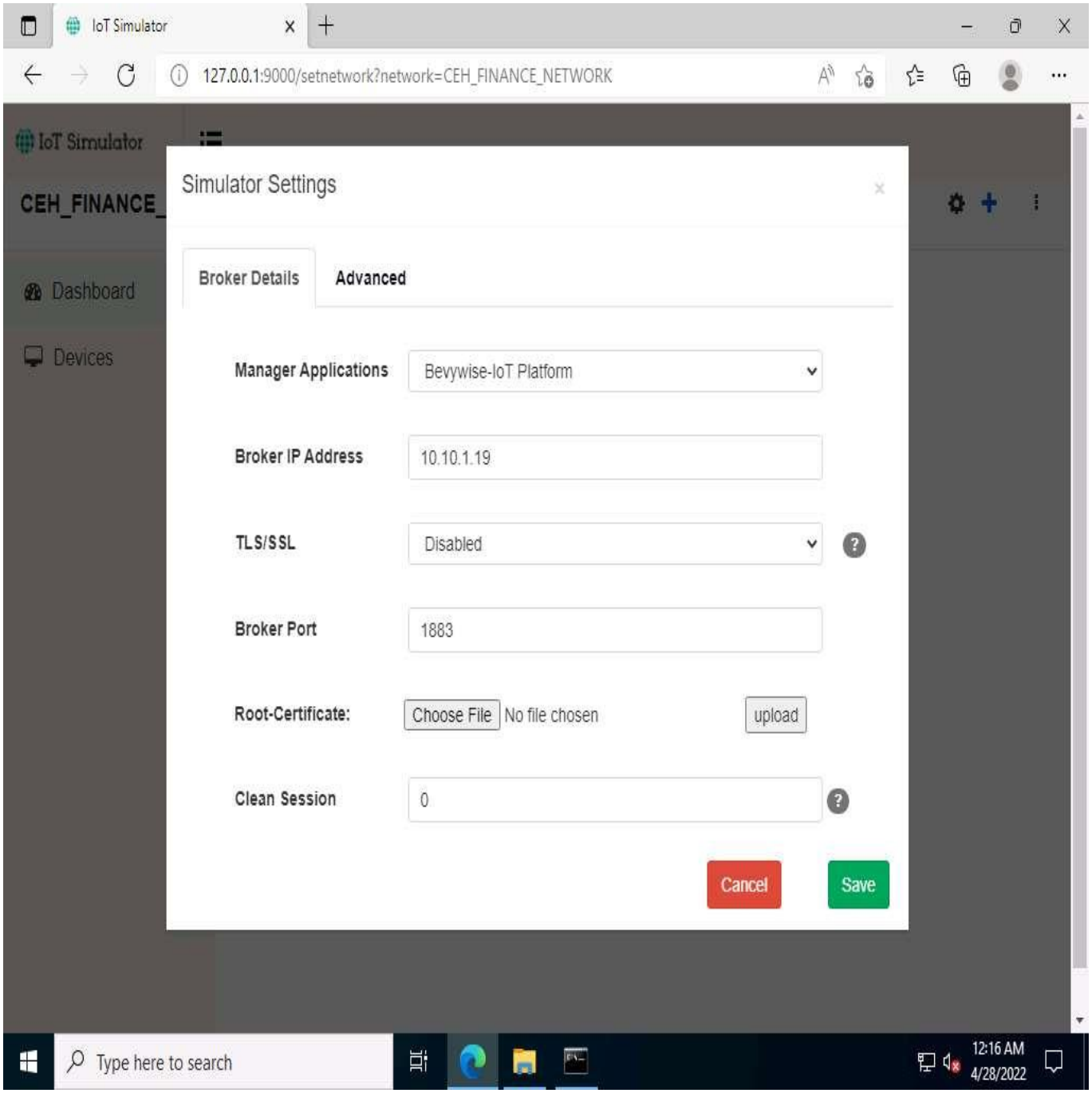
23. ☐ Next, we will create a **virtual IoT network** and **virtual IoT devices**. Click on the **menu** icon and select the **+New Network** option.



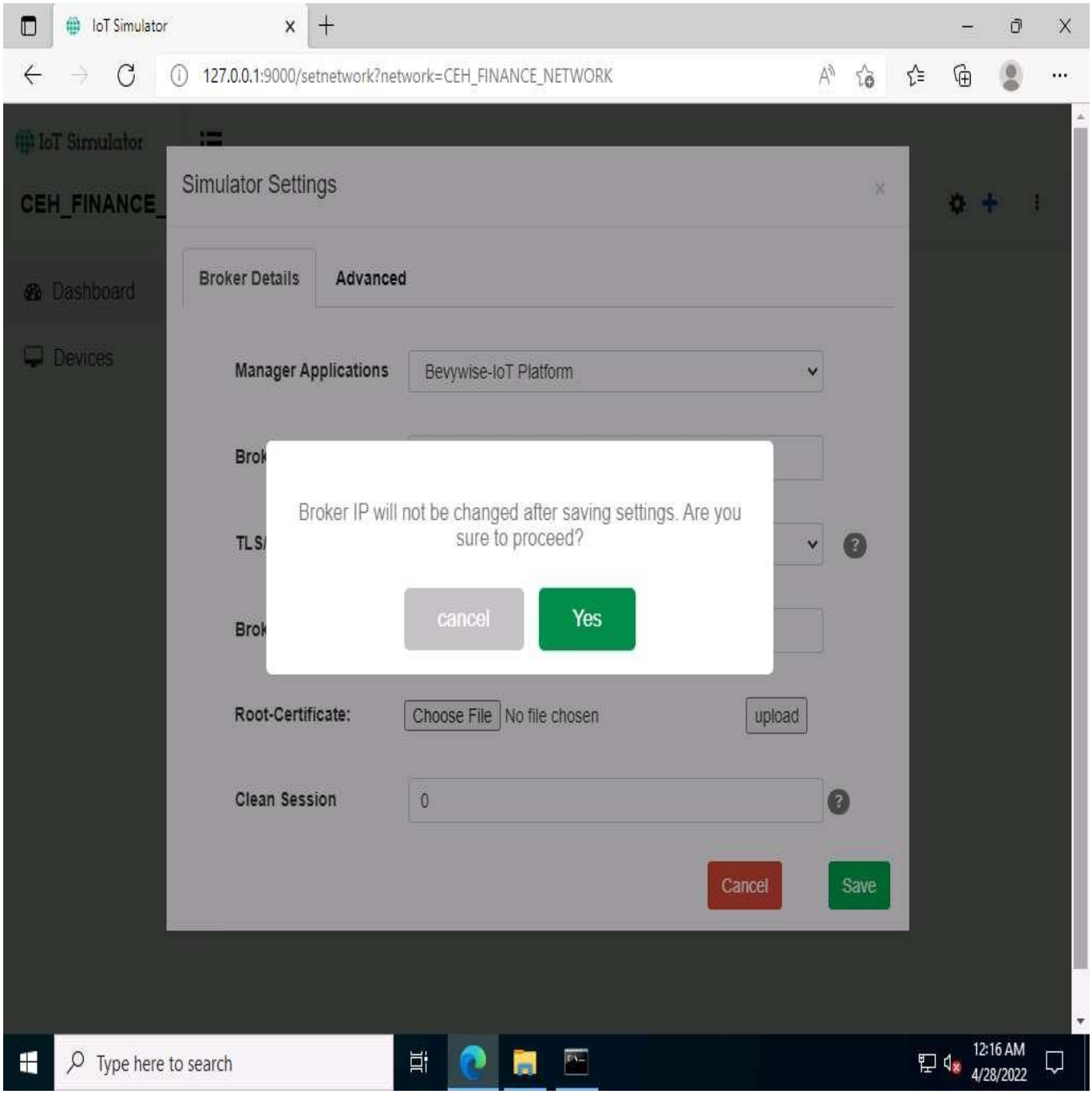
24. The **Create New Network** popup appears. Type any name (here, **CEH_FINANCE_NETWORK**) and description. Click on **Create**.



25. In the next screen, we will setup the **Simulator Settings**. Set the **Broker IP Address** as **10.10.1.19** (the IP address of the **Windows Server 2019**). Since we have installed the Broker on the web server, the created network will interact with the server using MQTT Broker. Do not change default settings and click on **Save**.

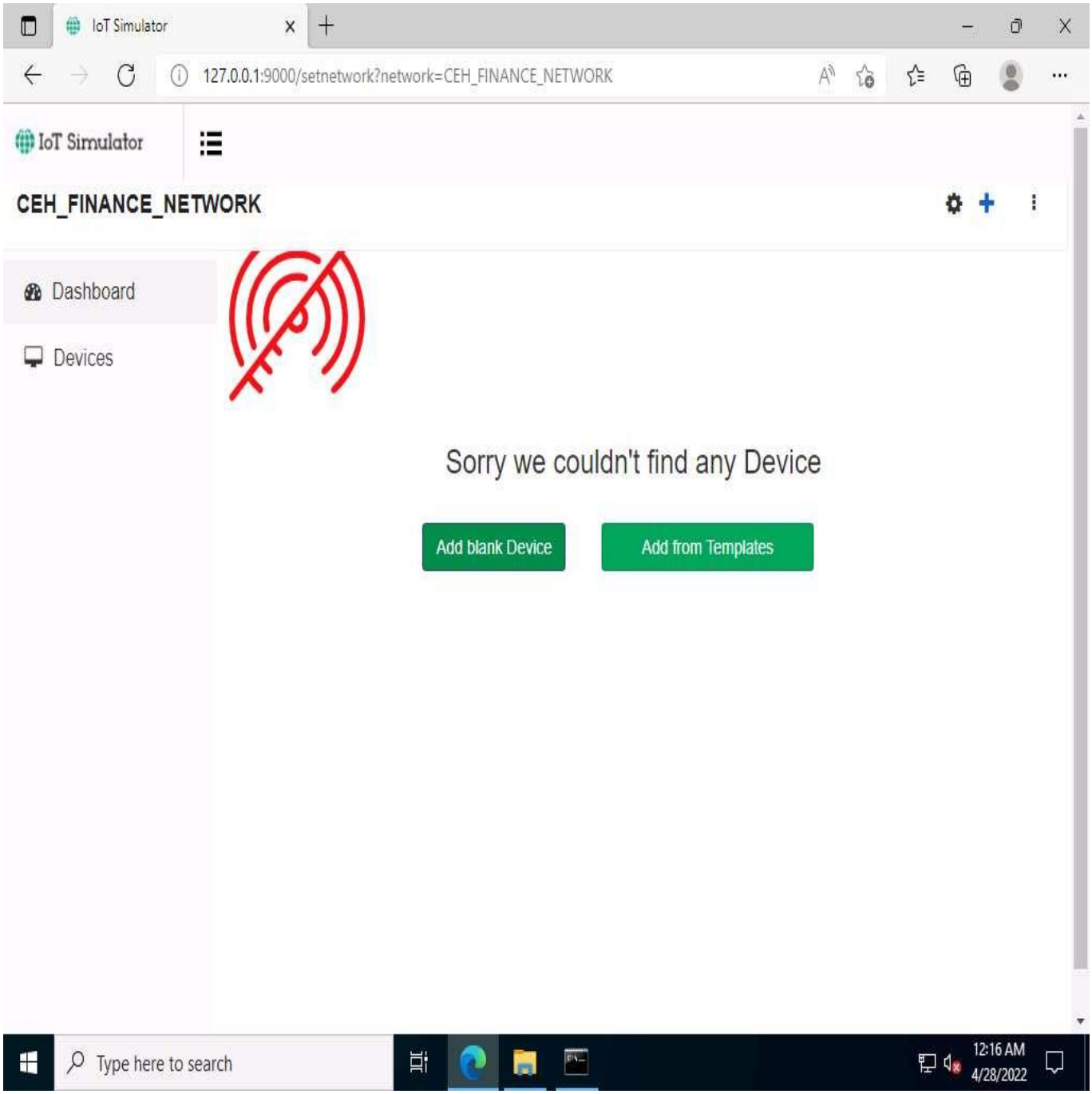


26. ☐ To proceed with the network creation, click on **Yes**.

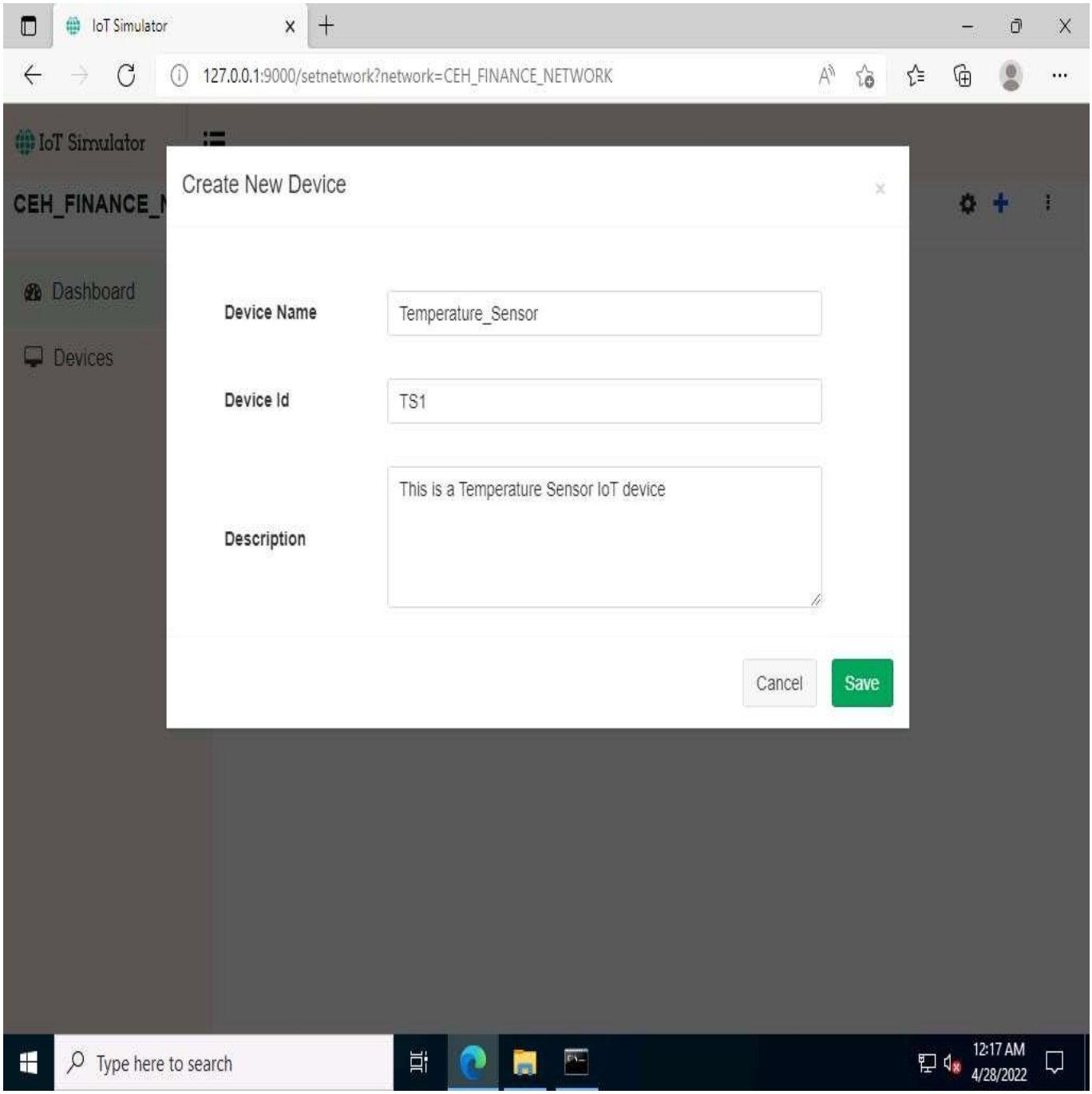


If **Configuration Saved** pop-up appears. Click on **OK** to continue. This step completes the creation of the virtual IoT network.

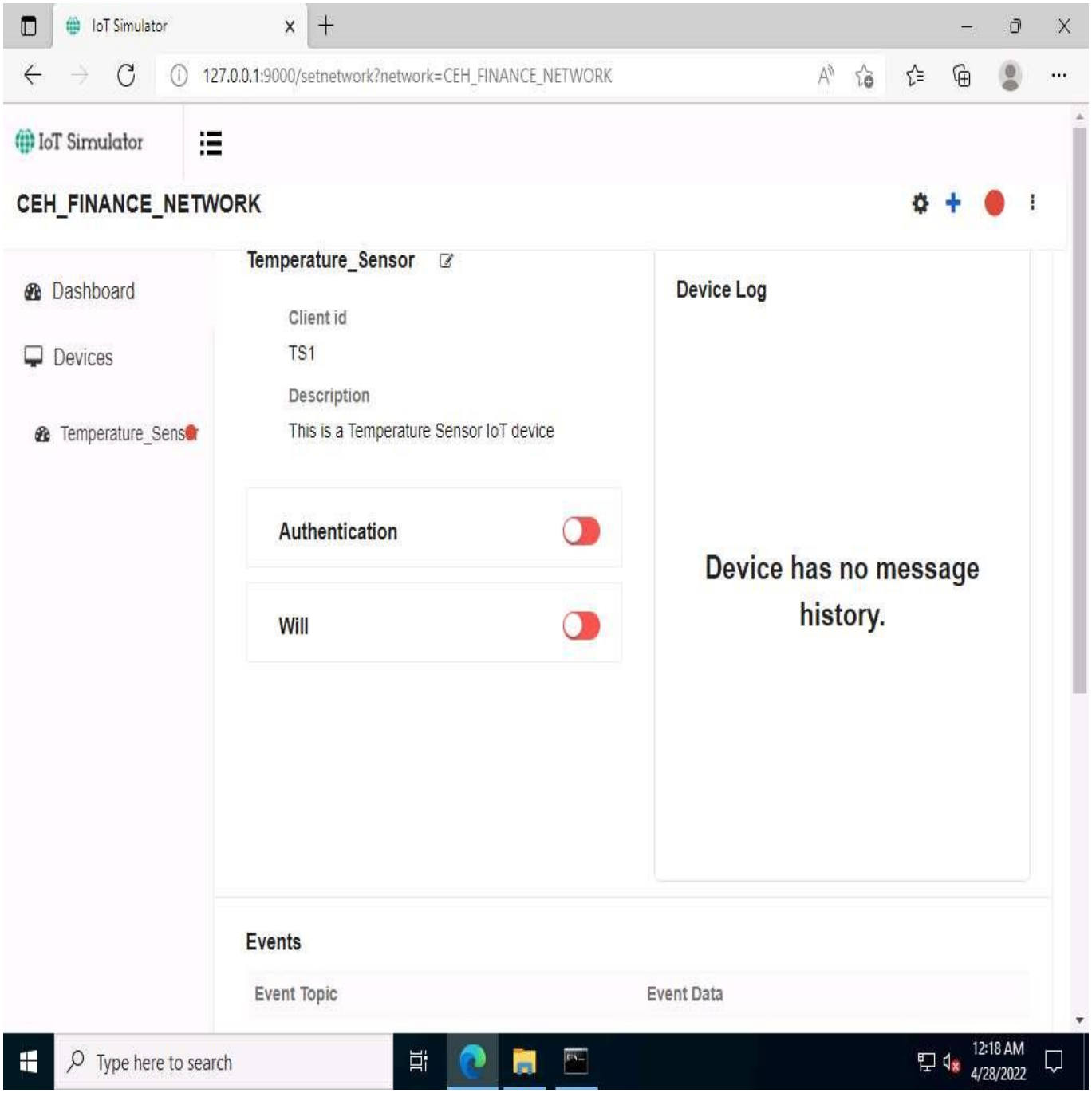
27. To add IoT devices to the created network, click on the **Add blank Device** button.



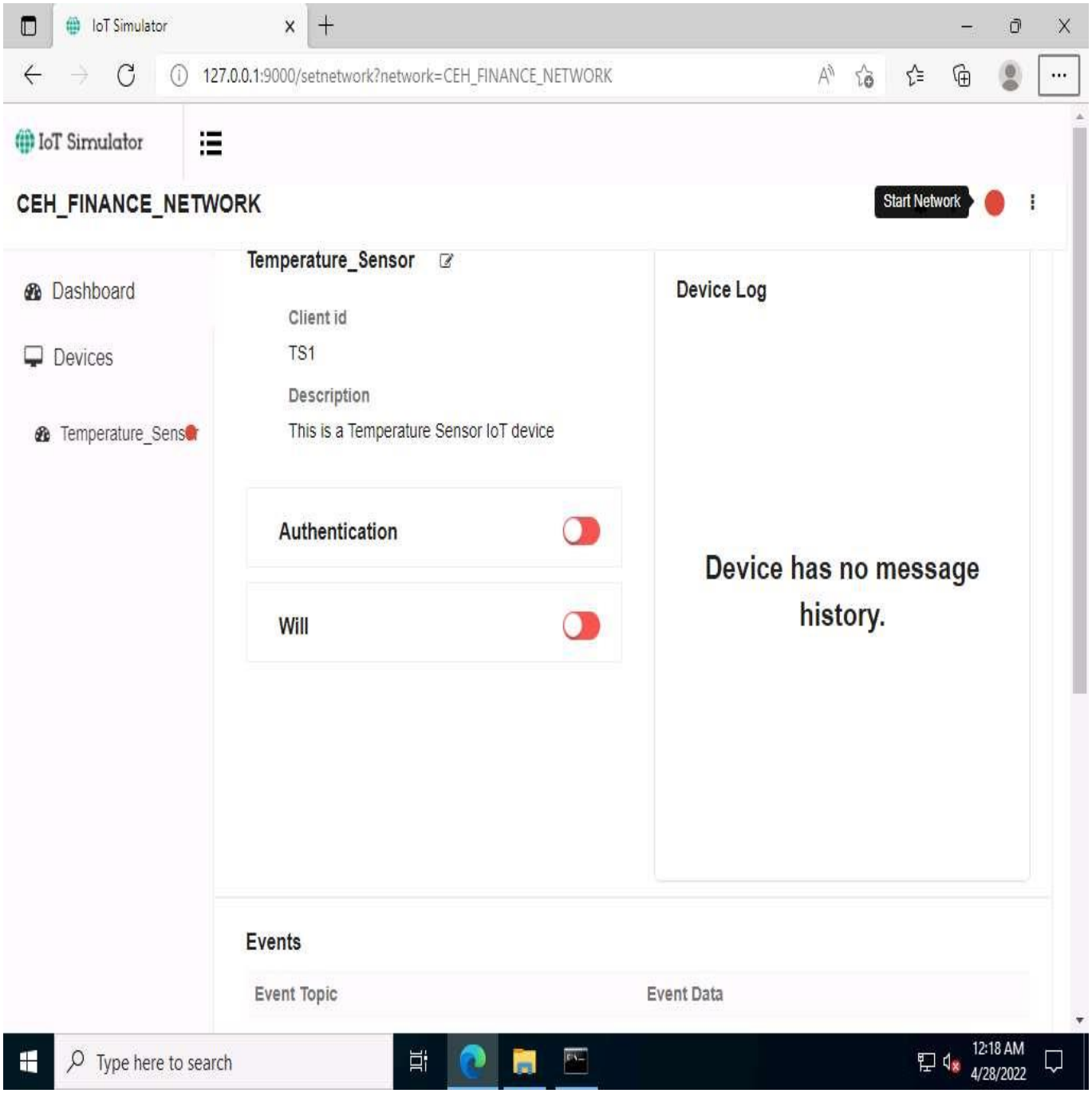
28. The **Create New Device** popup opens. Type the device name (here, we use **Temperature_Sensor**), enter Device Id (here, we use **TS1**), provide a **Description** and click on **Save**.



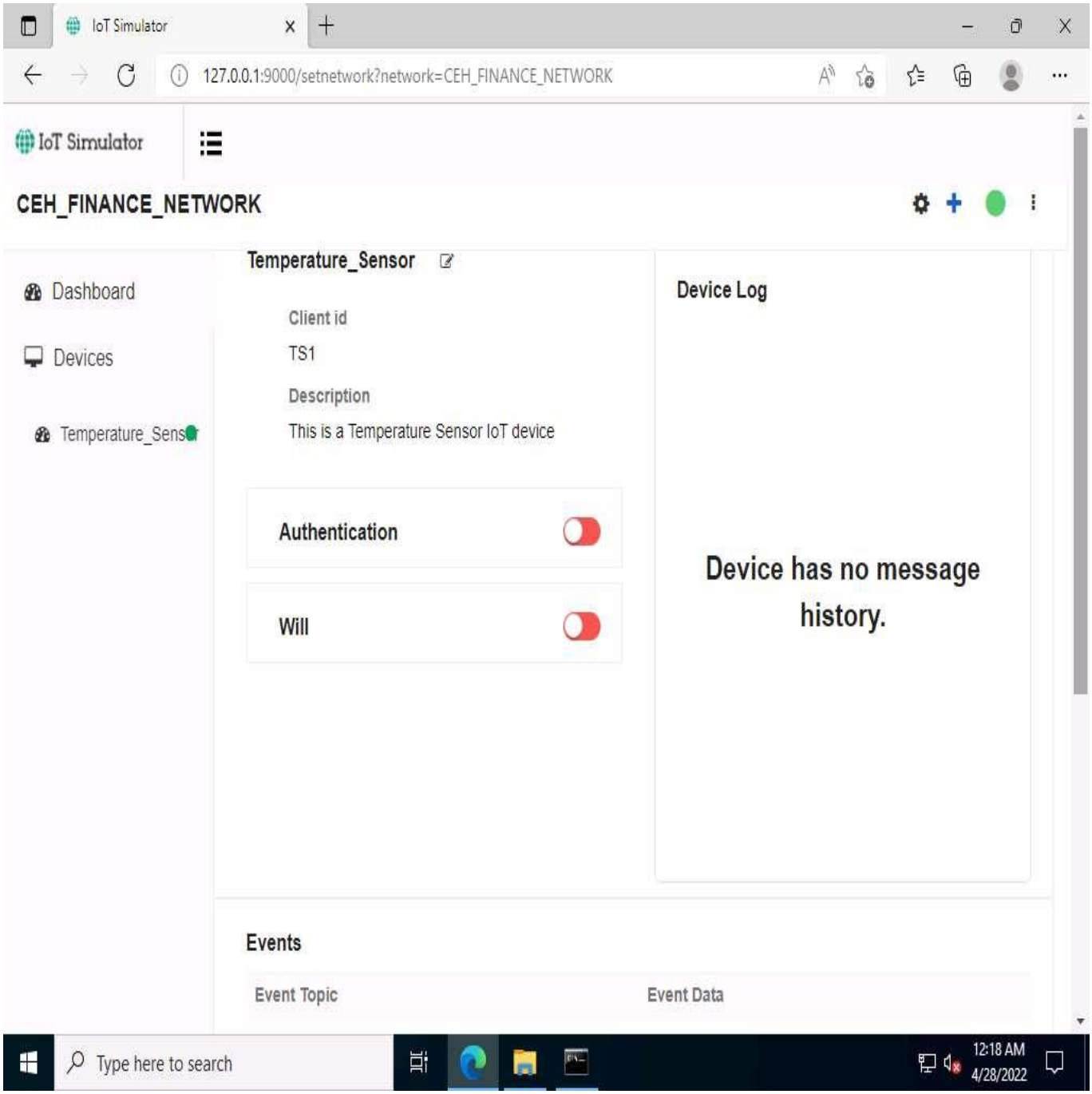
29. ☐ The device will be added to the **CEH_FINANCE_NETWORK**.



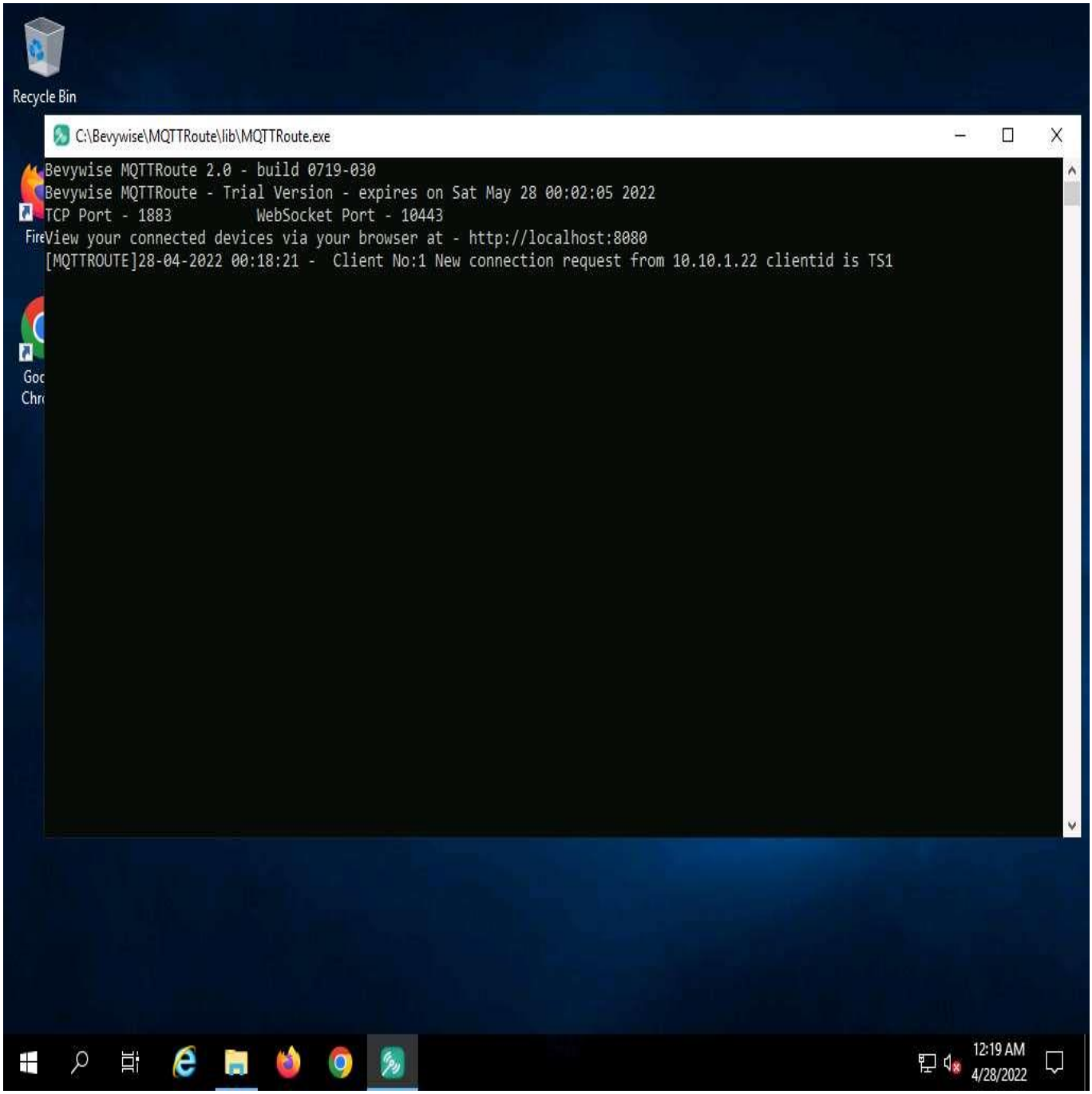
30. ☐ To connect the Network and the added devices to the server or Broker, click on the **Start Network** red color circular icon in right corner.



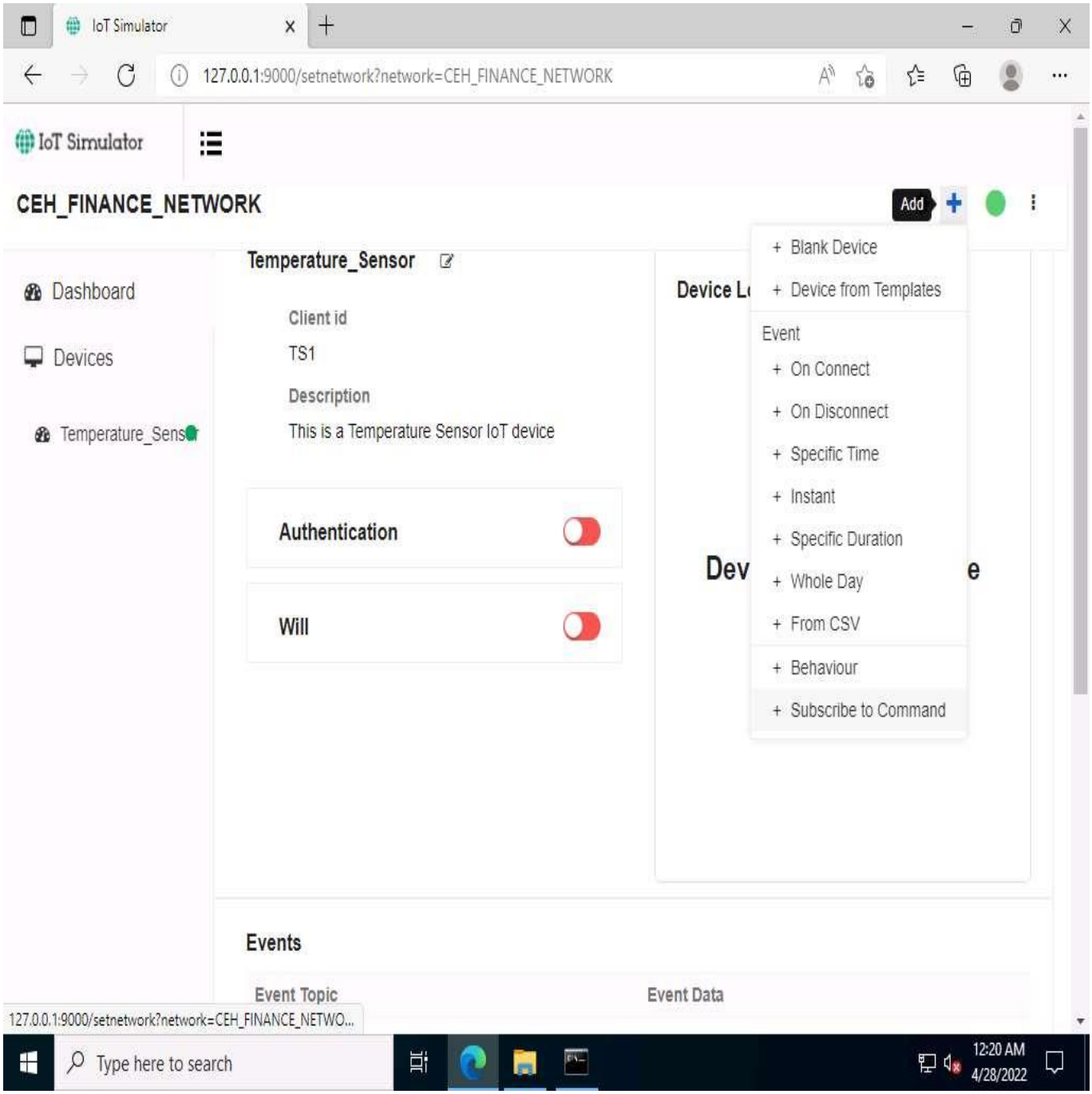
31. ☐ When a connection is established between the network and the added devices and the web server or the MQTT Broker, the red button turns into **green**.



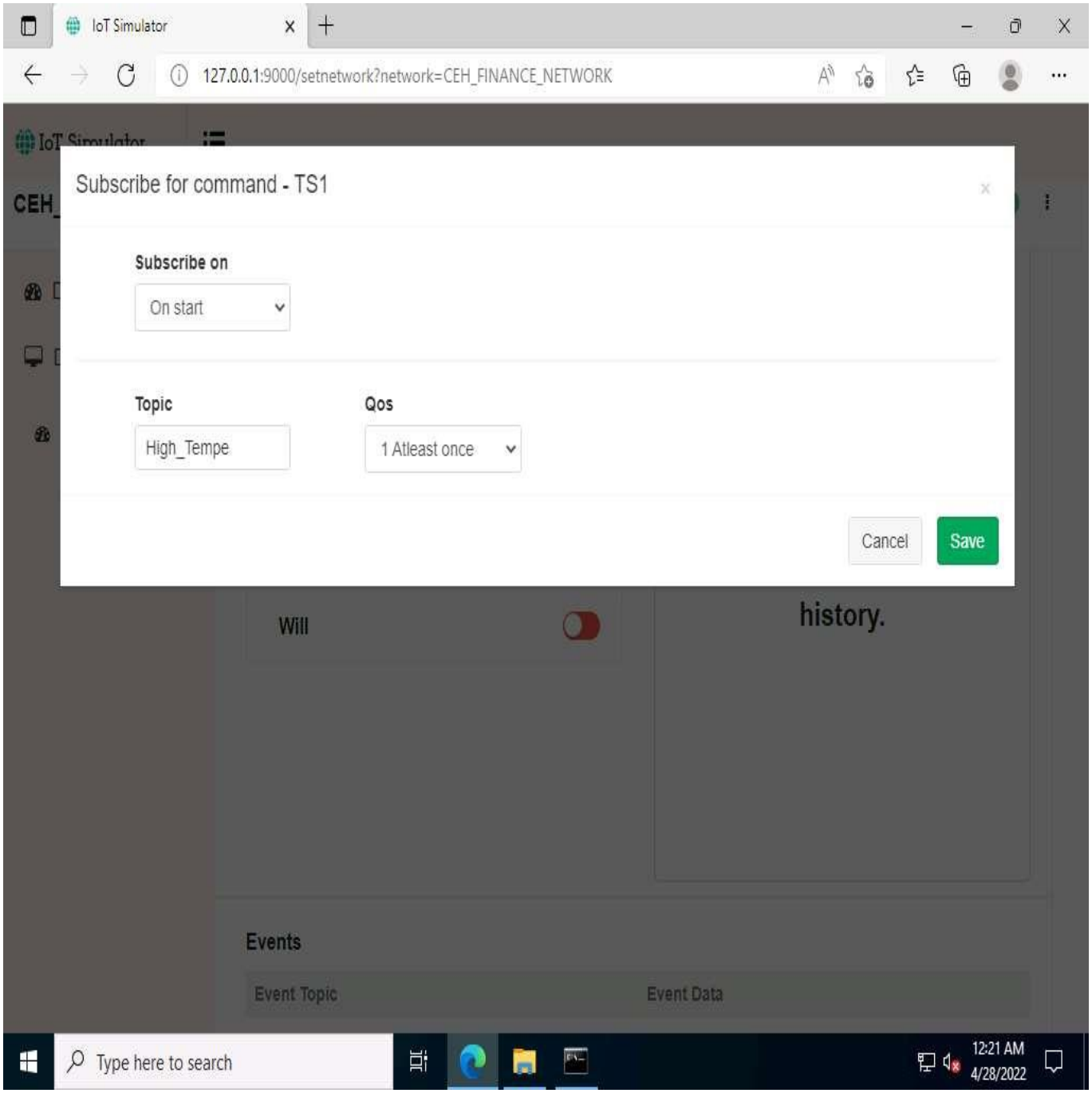
32. ☐ Next, switch to the Windows Server 2019 machine. Since the Broker was **left running**, you can see a connection request from machine **10.10.1.22** for the device **TS1**.



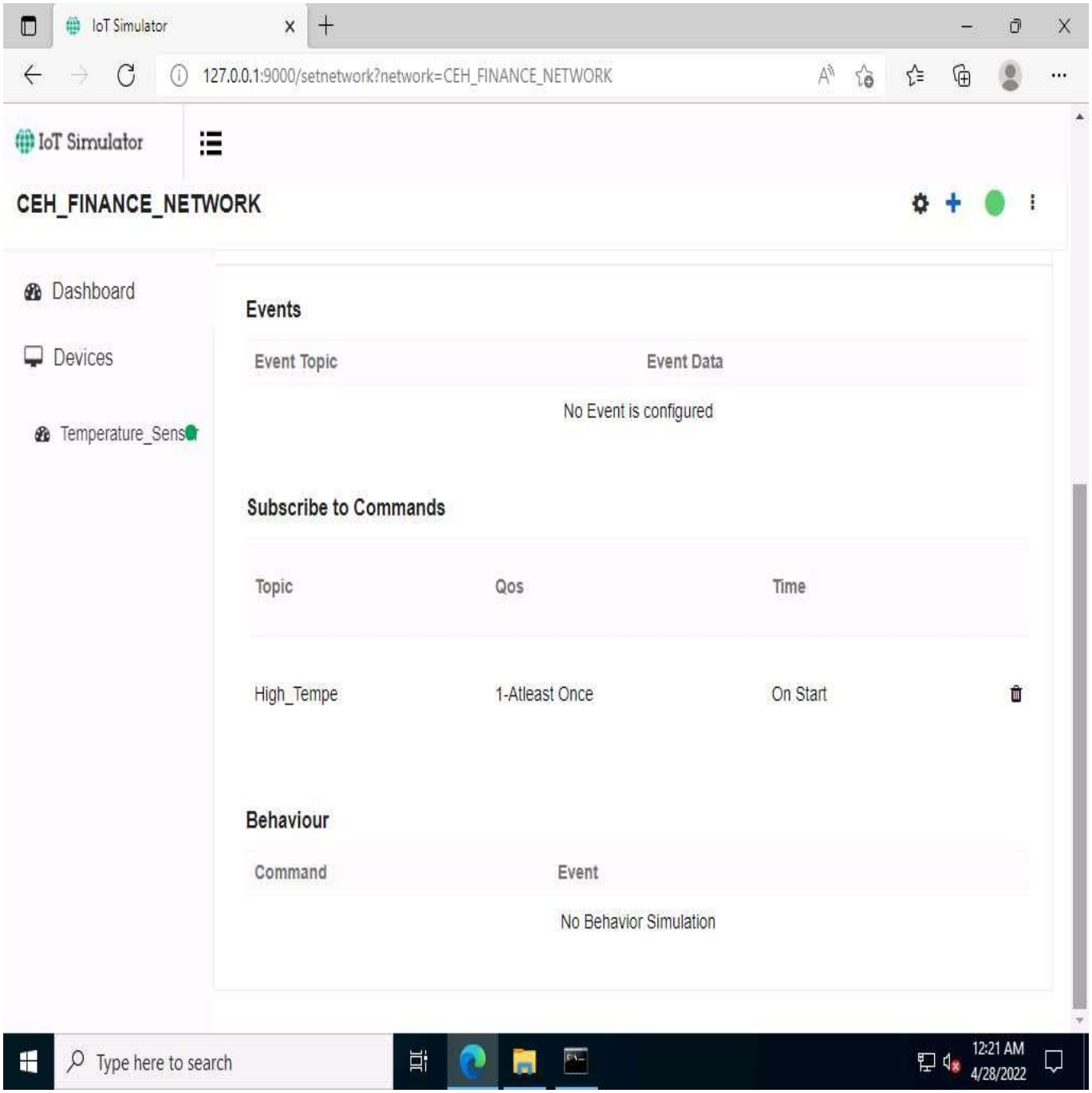
33. ☐ Switch back to Windows Server 2022 machine.
34. ☐ Next, we will create the **Subscribe command** for the device Temperature_Sensor.
35. ☐ Click on the **Plus** icon in **the top right corner** and select the **Subscribe to Command** option.



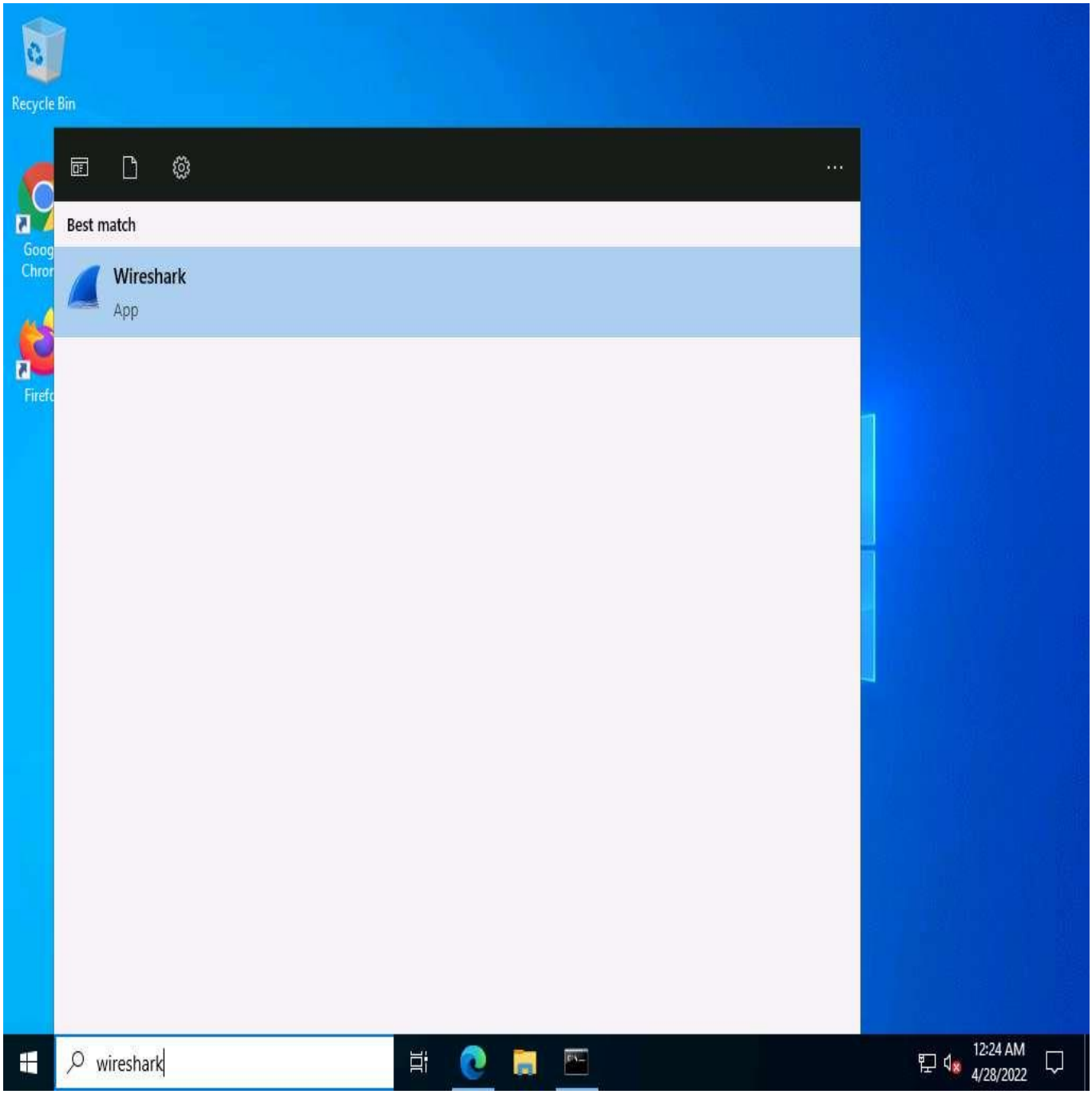
36. The **Subscribe for command - TS1** popup opens. Select **On start** under the Subscribe on tab, type **High_Tempe** under the **Topic tab**, and select **1 Atleast once** below the **Qos** option. Click on **Save**.



37. ☐ Scroll down the page, you can see the **Topic** added under the **Subscribe to Commands** section.



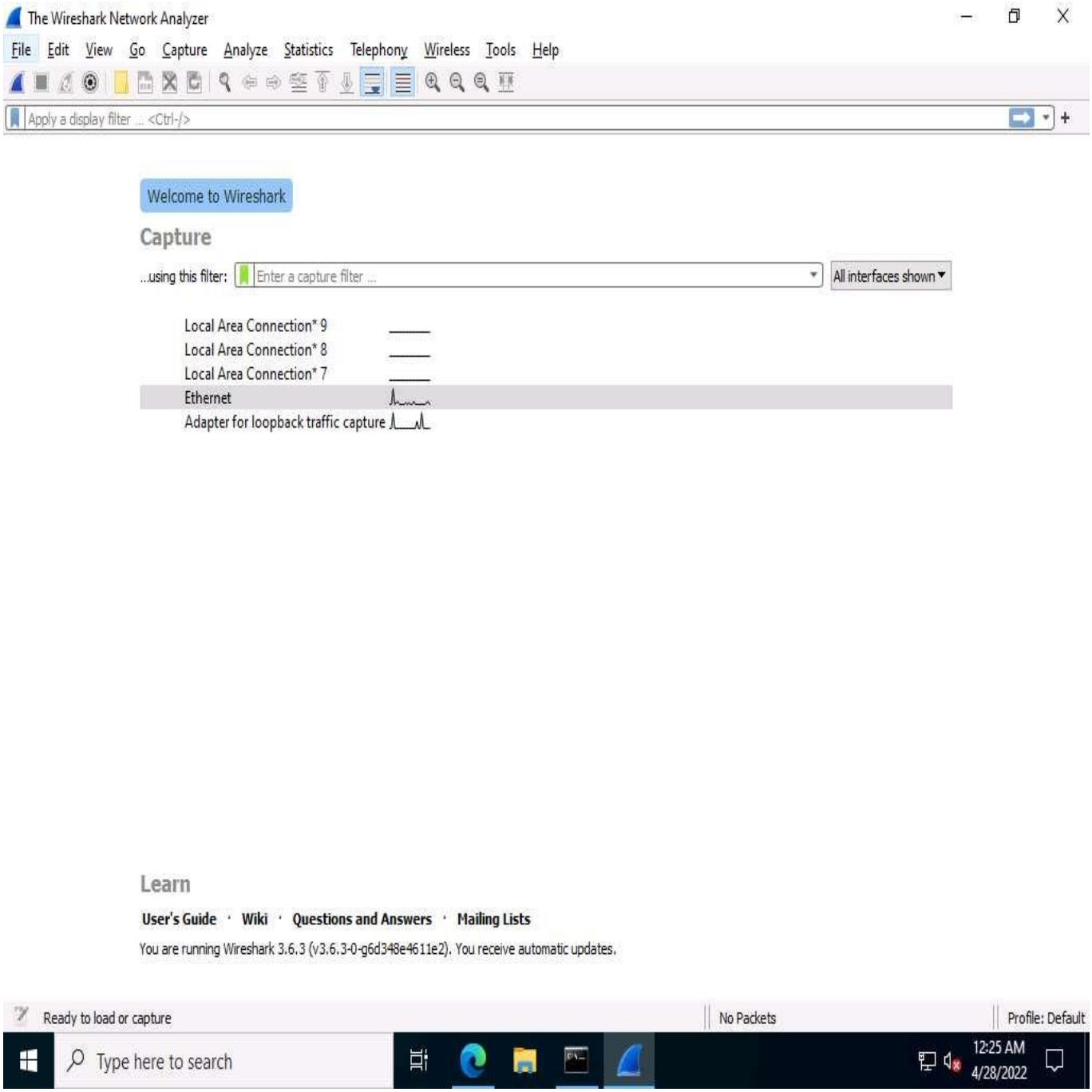
38. ☐ Next, we will capture the traffic between the **virtual IoT network and the MQTT Broker** to monitor the secure communication.
39. ☐ Minimise the Edge browser. Click on **Type here to search** at the bottom left of the desktop, type wireshark and select Wireshark from the results to launch the **Wireshark** from the application list.



40. ☐ The Wireshark Application window appears, select the **Ethernet** as interface.

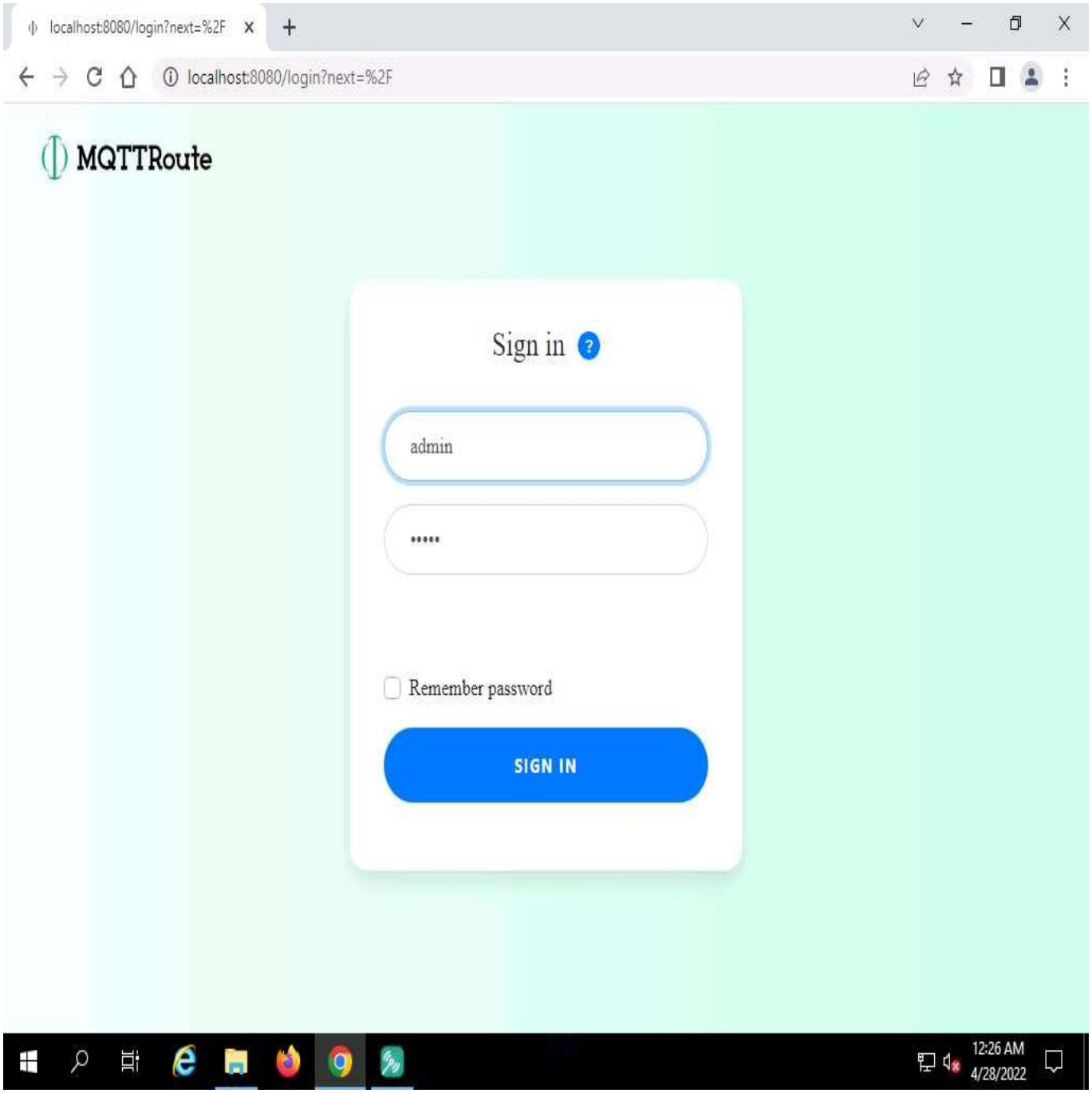
Make sure you have selected interface which has **10.10.1.22** as the IP address.

If Software update popup appears click on **Skip this version**.

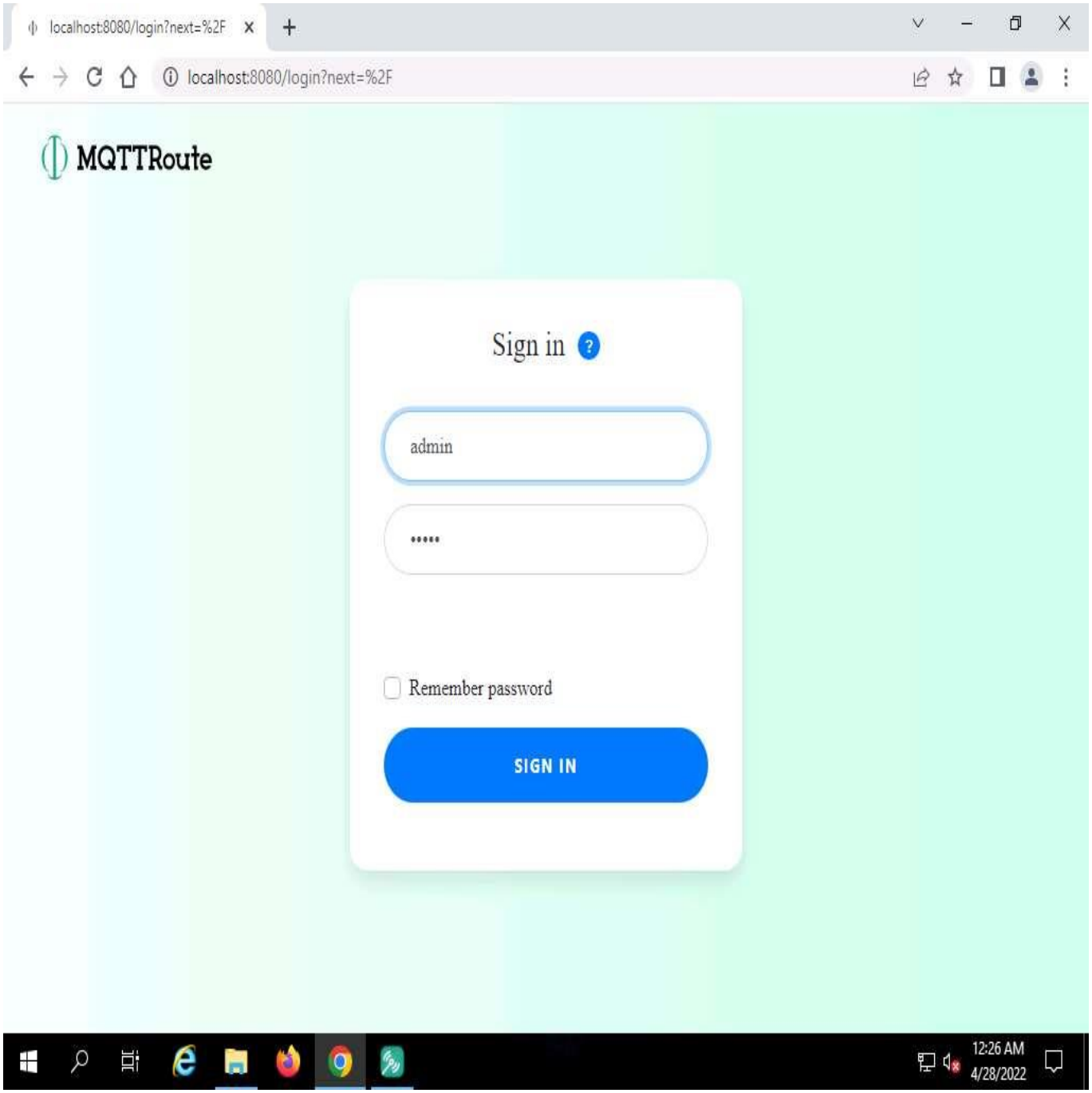


41. ☐ Click on the **Start Wireshark** icon to start the capturing packets, leave the Wireshark running.
42. ☐ Leave the IoT simulator running and switch to the Windows Server 2019 machine.
43. ☐ Minimise all opened applications and windows, Open Chrome browser, type **http://localhost:8080** and press **Enter**.

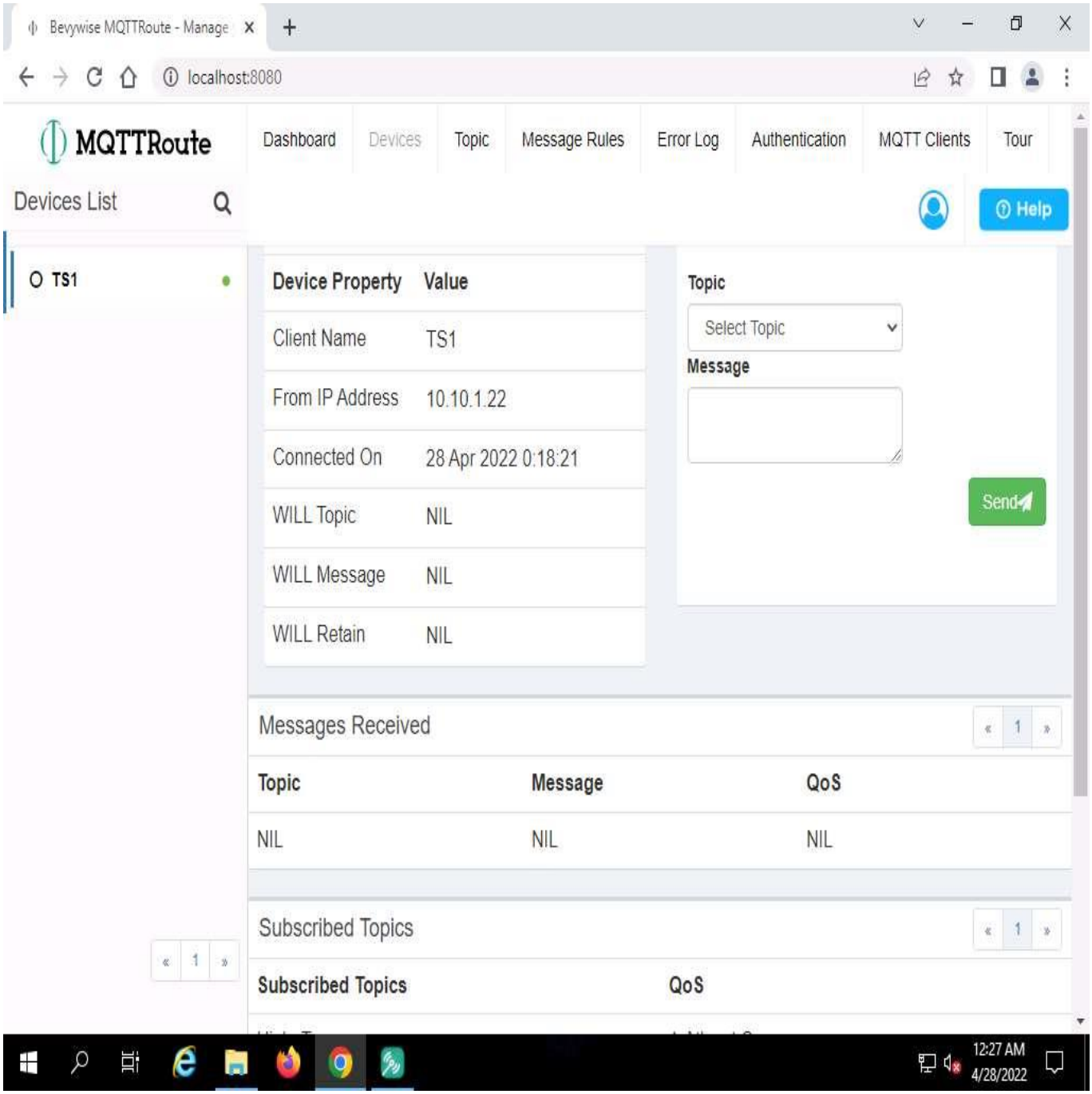
Do not use Internet Explorer web browser to open the above URL.



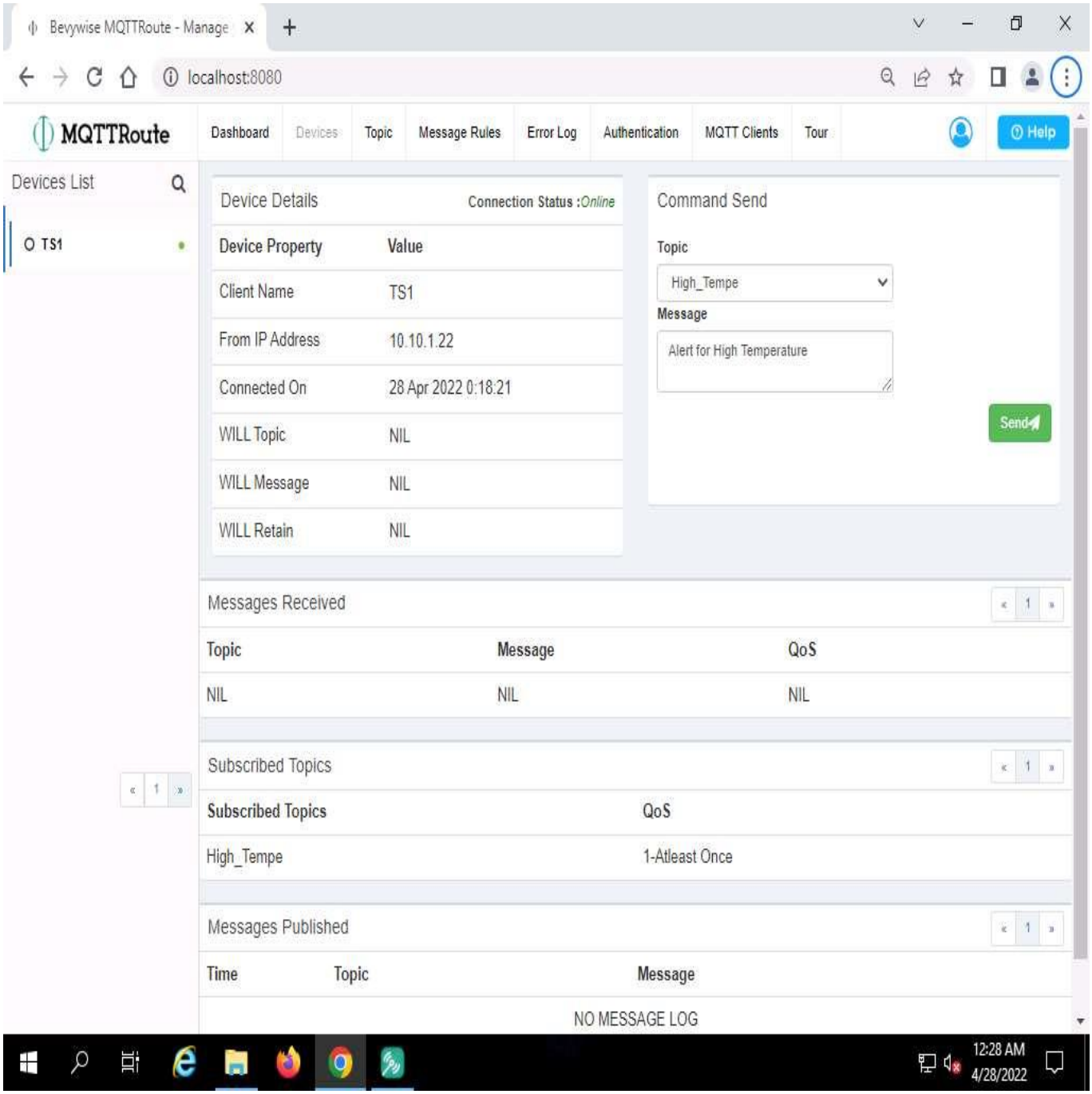
44. ☐ As soon as you press **Enter**, the **MQTTRoute Sign in** page appears, keep the default credential unchanged and click on **SIGN IN**.



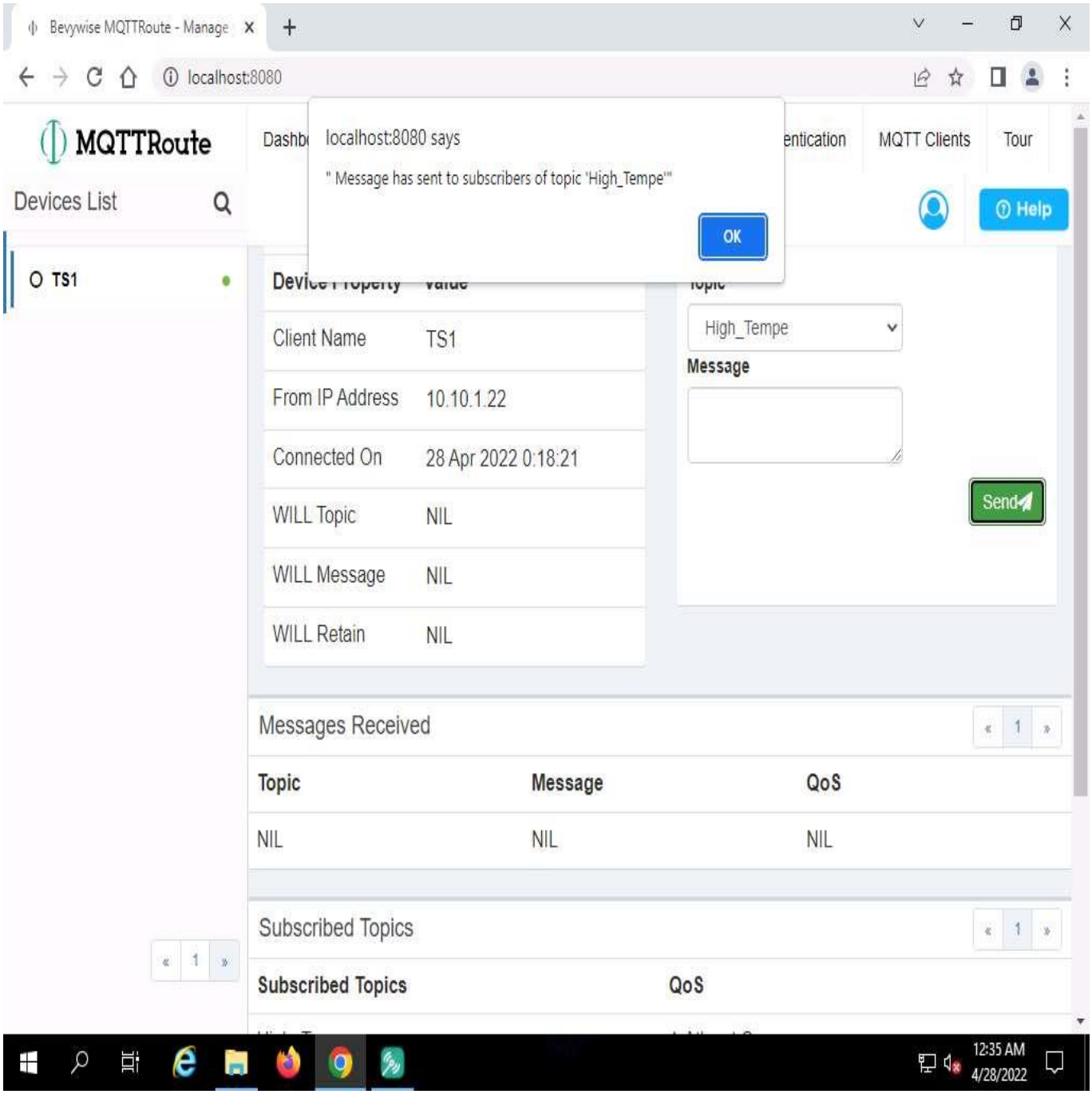
45. ☐ Navigate to **Devices** menu. You will be able to see the connected device **TS1** in the left pane.



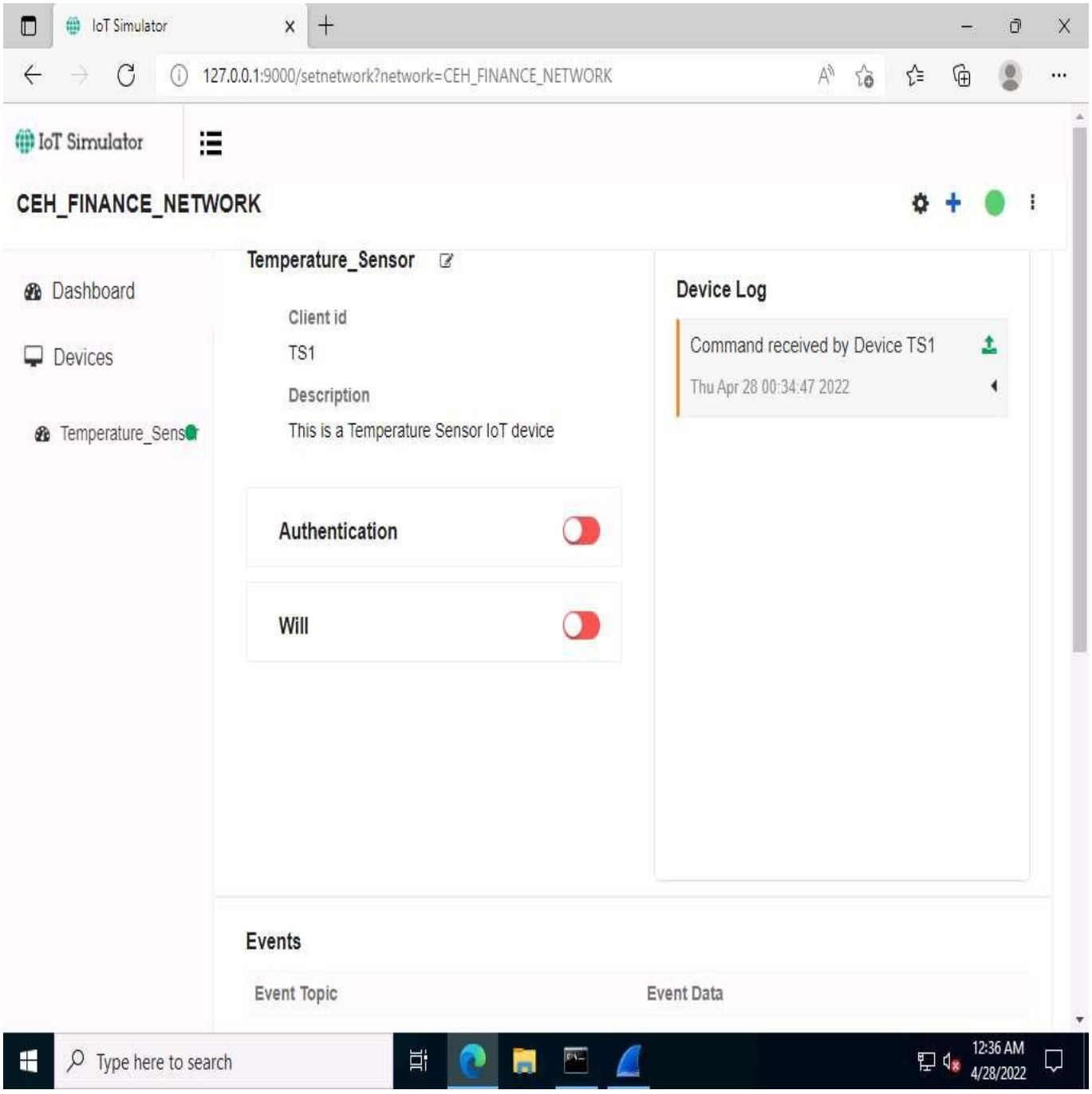
46. ☐ Now, we will send the command to **TS1** using the **High_Tempe** topic.
47. ☐ Go to the **Command Send** section, select **Topic** as **High_Tempe**, type **Alert for High Temperature** and click on the **Send** button.



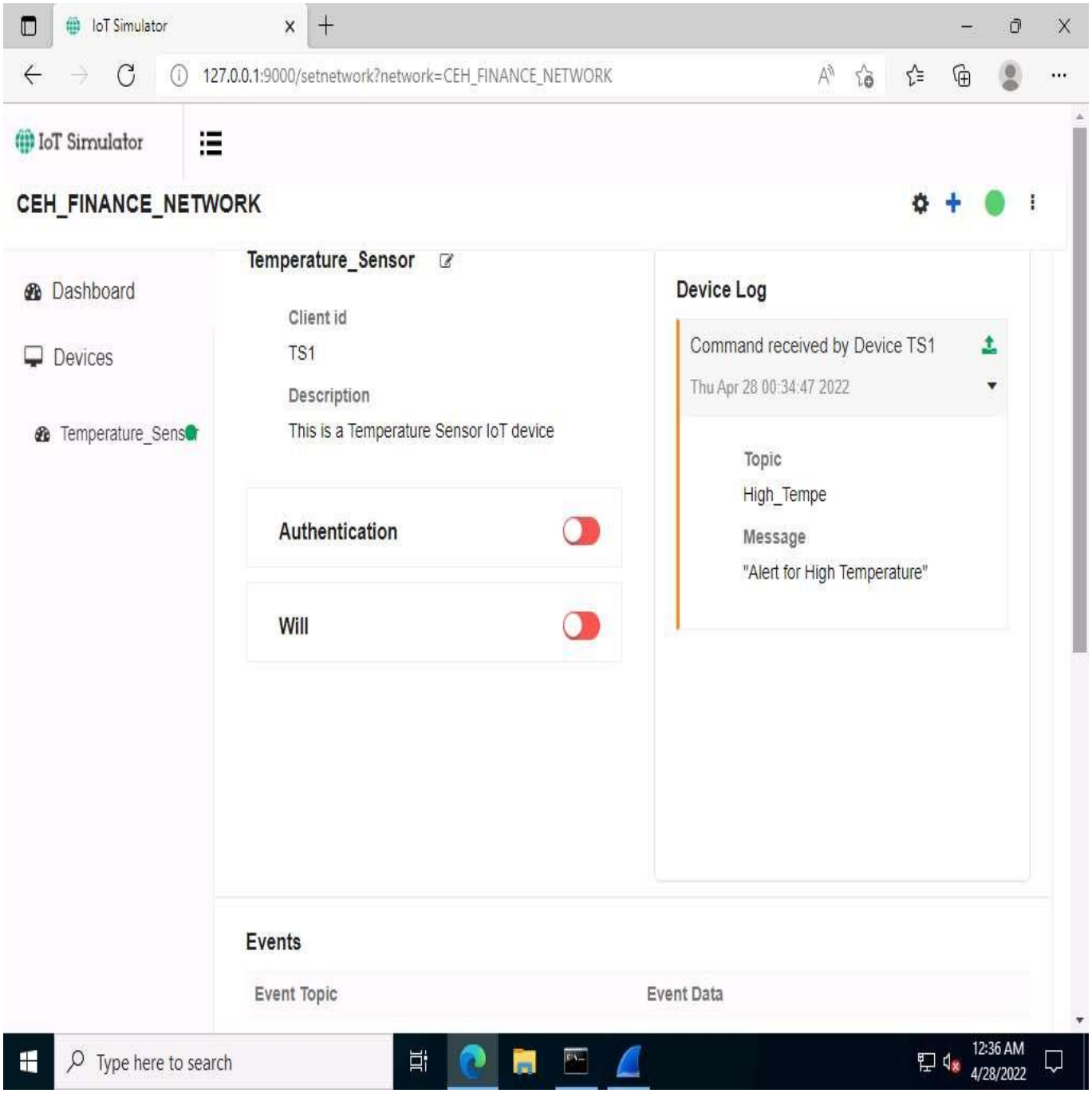
48. ☐ The alert popup appears, then click on **OK**.



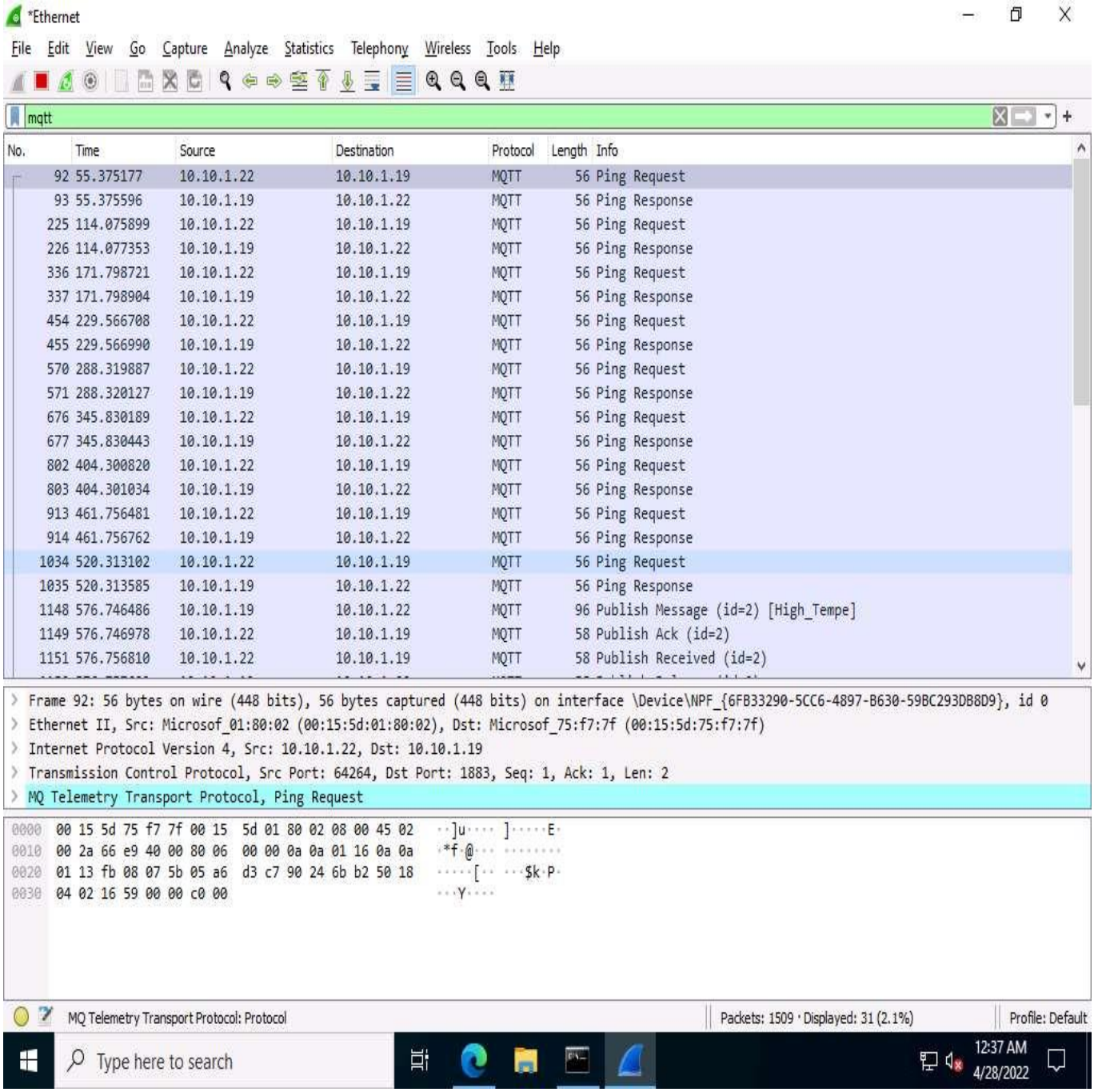
49. ☐ The message has been sent to the device using this topic.
50. ☐ Next, switch to Windows Server 2022 machine.
51. ☐ We have left the IoT simulator running in the web browser. To see the alert message, maximise the Edge browser and expand the arrow under the connected **Temperature_Sensor**, **Device Log** section.



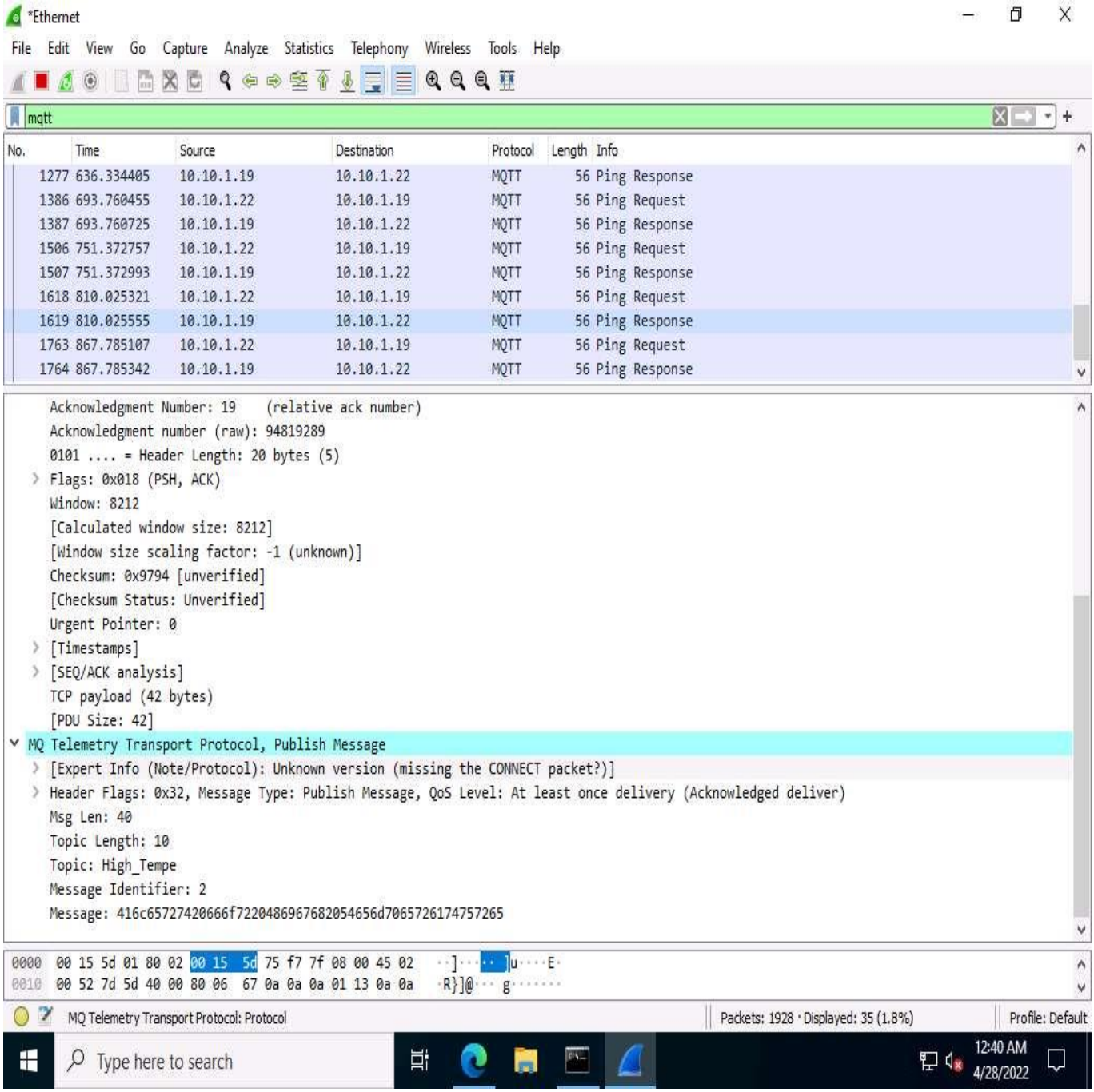
52. ☐ You can see the alert message "**Alert for High Temperature**"



53. ☐ To verify the communication, we have executed **Wireshark** application, switch to the Wireshark traffic capturing window.
54. ☐ Type **mqtt** under the **filter** field and press **Enter**. To display only the MQTT protocol packets.



55. ☐ Select any **Publish Message** packet from the **Packet List** pane. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
56. ☐ Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Topic Length**, **Topic**, and **Message**.
57. ☐ Publish Message can be used to obtain the message sent by the MQTT client to the broker.

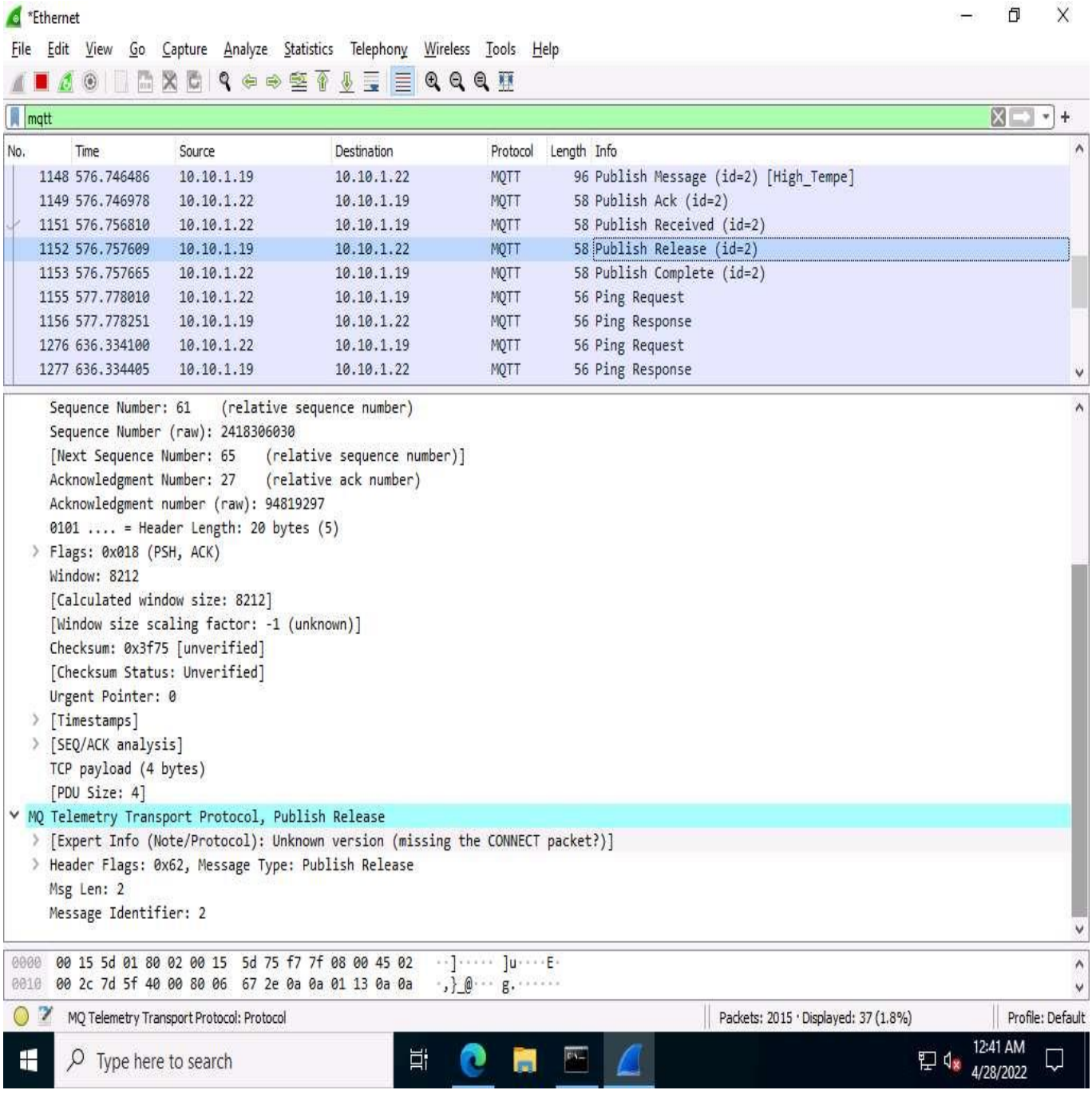


Note: After establishing a successful connection with the MQTT broker, the MQTT client can publish messages. The headers in the Publish Message packet are given below:

- Header Flags: Contains information regarding the MQTT control packet type.
- DUP flag: If the DUP flag is 0, it indicates the first attempt at sending this PUBLISH packet; if the flag is 1, it indicates a possible re-attempt at sending the message.
- QoS: Determines the assurance level of a message.
- Retain Flag: If the retain flag is set to 1, the server must store the message and its QoS, so it can cater to future subscriptions matching the topic.
- Topic Name: Contains a UTF-8 string that can also include forward slashes when it needs to be hierarchically structured.
- Message: Contains the actual data to be transmitted.
- Payload: Contains the message that is being published.

58. ☐ Select any **Publish Release** packet from the **Packet List** pane. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

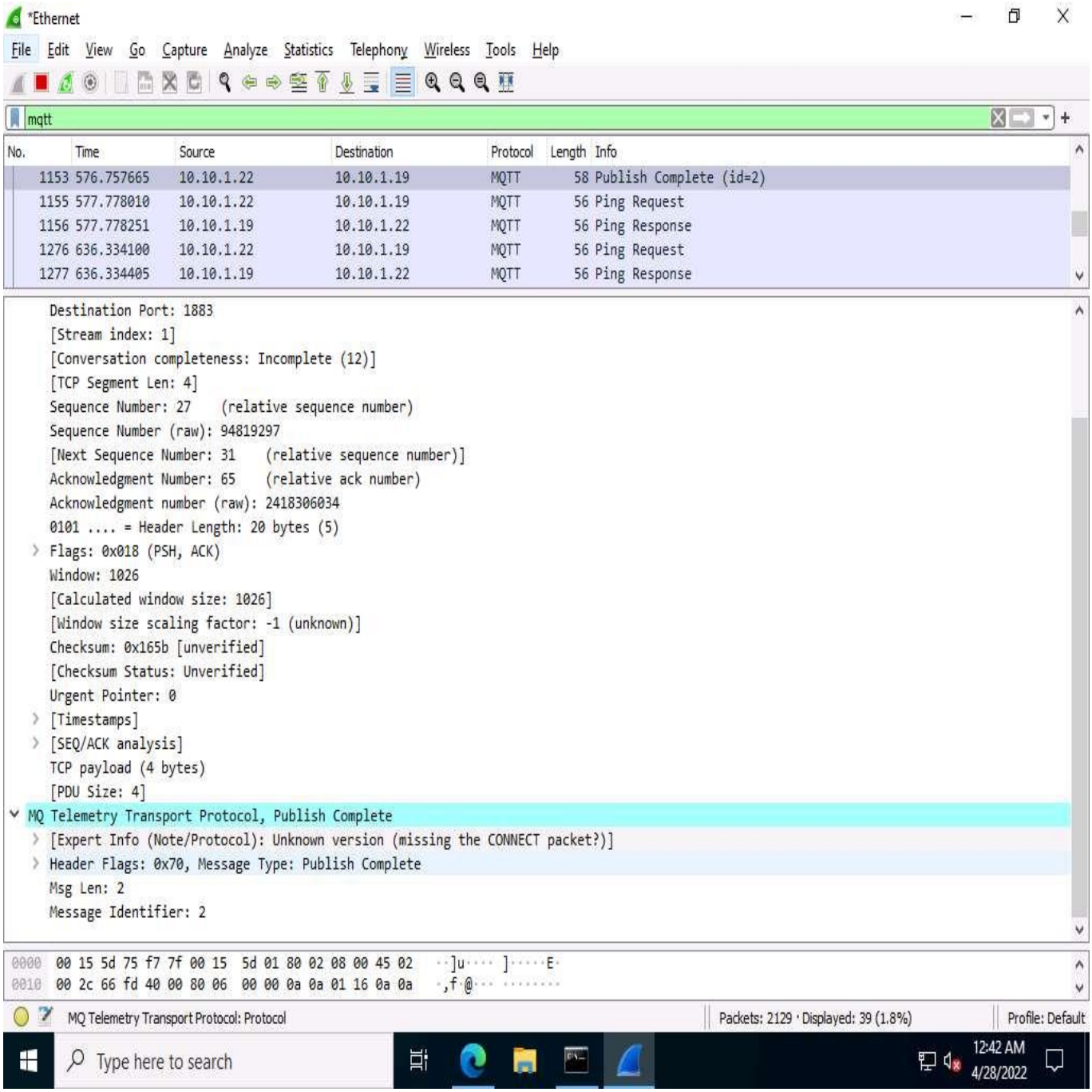
59. ☐ Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Message Type**, **Message Identifier**.



Note: A Publish Release (PUBREL) packet is the response to a Publish Received (PUBREC) packet.

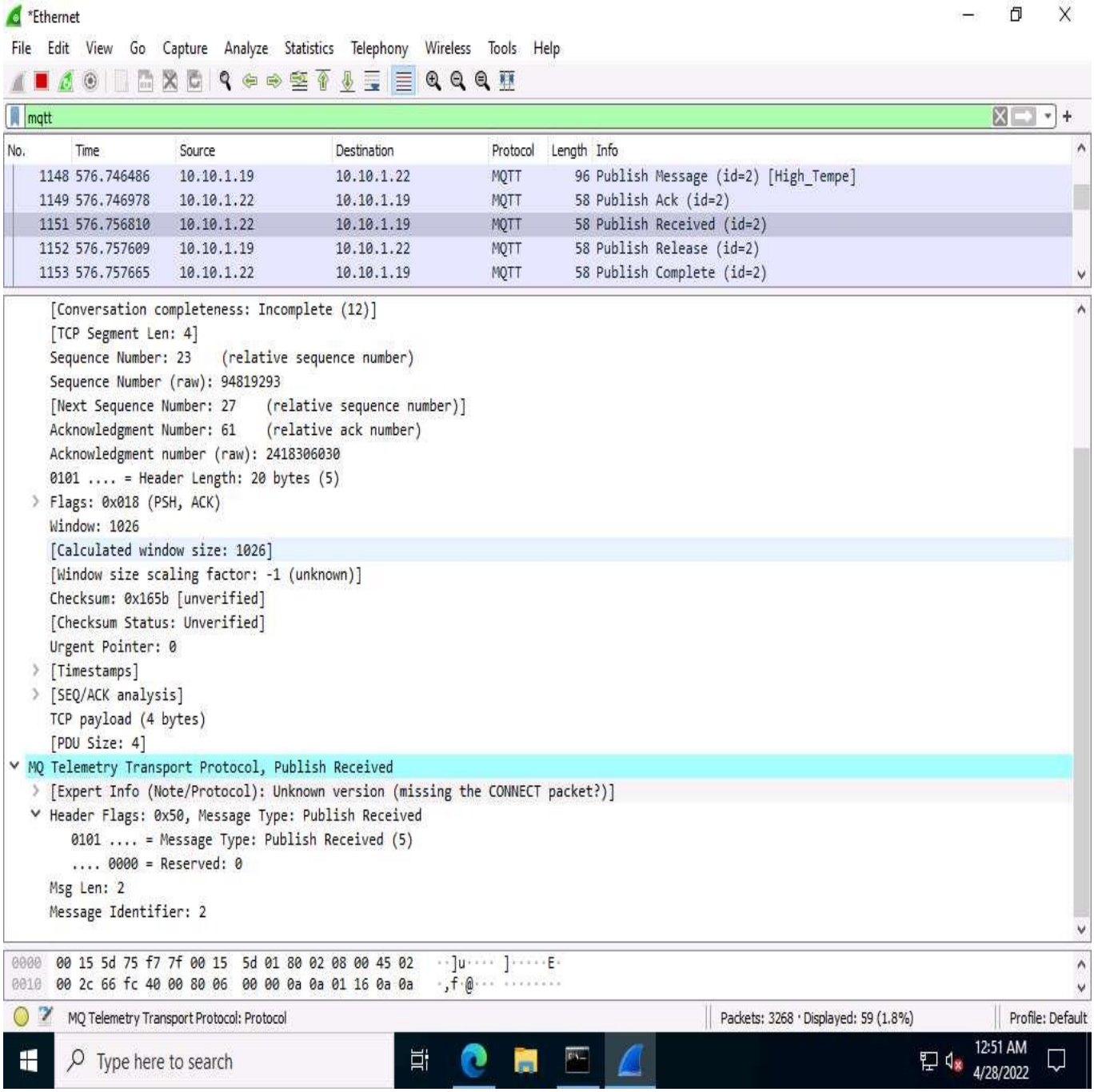
60. ☐ Now, scroll down, look for the **Publish Complete** packet from the **Packet List** pane, and click on it. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

61. ☐ Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.



Note: The Publish Complete (PUBCOMP) packet is the response to a Publish Release (PUBREL) packet.

62. ☐ Now, scroll down, look for the **Publish Received** packet from the **Packet List** pane, and click on it. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
63. ☐ Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Message Type**, **Msg Len** and **Message Identifier**.



64. ☐ Similarly you can select **Ping Request**, **Ping Response** and **Publish Ack** packets and observe the details.
65. ☐ This concludes the demonstration of capturing and analyzing MQTT protocol packets. Here, we analyzed different processes involved in the communication between an MQTT client and an MQTT broker using Wireshark. Understanding these metrics as well as the workflow can help you in quickly identifying the MQTT-related issues.
66. ☐ Close all open windows and document all the acquired information.