Technical Note 179

Wireshark for Modbus RTU

Installation, setup and capture instructions

Introduction

Since its introduction in 1979, Modbus RTU became an industry standard for communication in control applications. It has been a standard in ABB drives for decades. As such, there is a significant installed base of applications using Modbus. When issues arise which require an understanding of what Modbus registers and services are being accessed, troubleshooting can stall without this information. This paper describes how to configure a common network analysis tool – Wireshark – to capture Modbus RTU traffic over RS-485, providing necessary information regarding Modbus communication in an application.

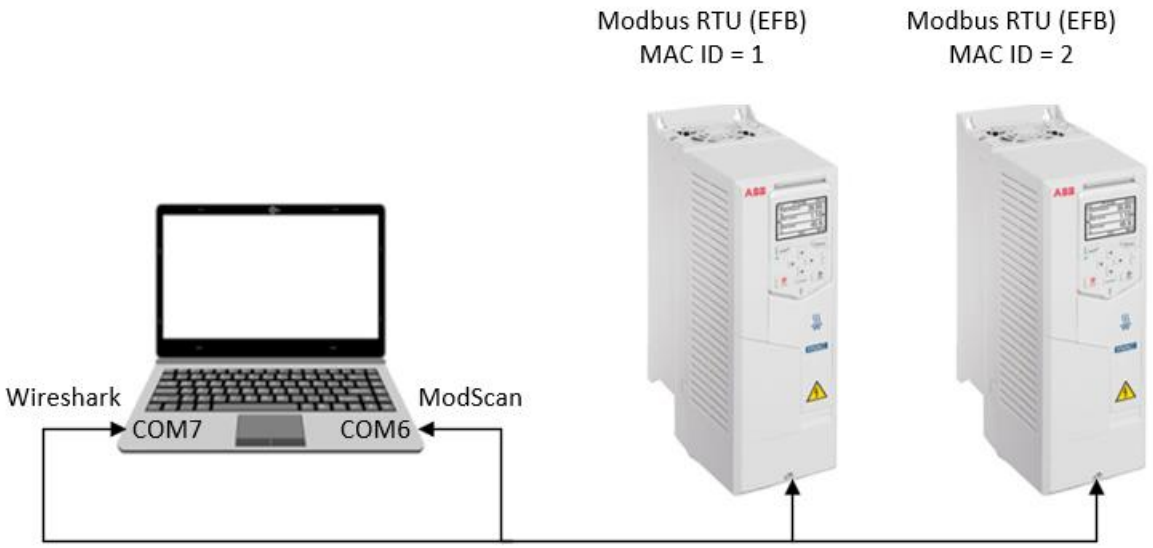
What is Wireshark?

Wireshark is a network packet analyzer. Historically, such an analysis tool was either expensive or proprietary. Wireshark, however, is available for free as an open-source project maintained by its users. It is widely considered to be one of the best packet analyzers available today.

Although best known as a capture and analysis tool for Ethernet-based protocols, it has evolved to also accept input from a computer's serial COM ports. As well, user-demand has driven Wireshark developers to add Modbus RTU protocol decoders to this open-source project, as it already supported Modbus/TCP over IP.

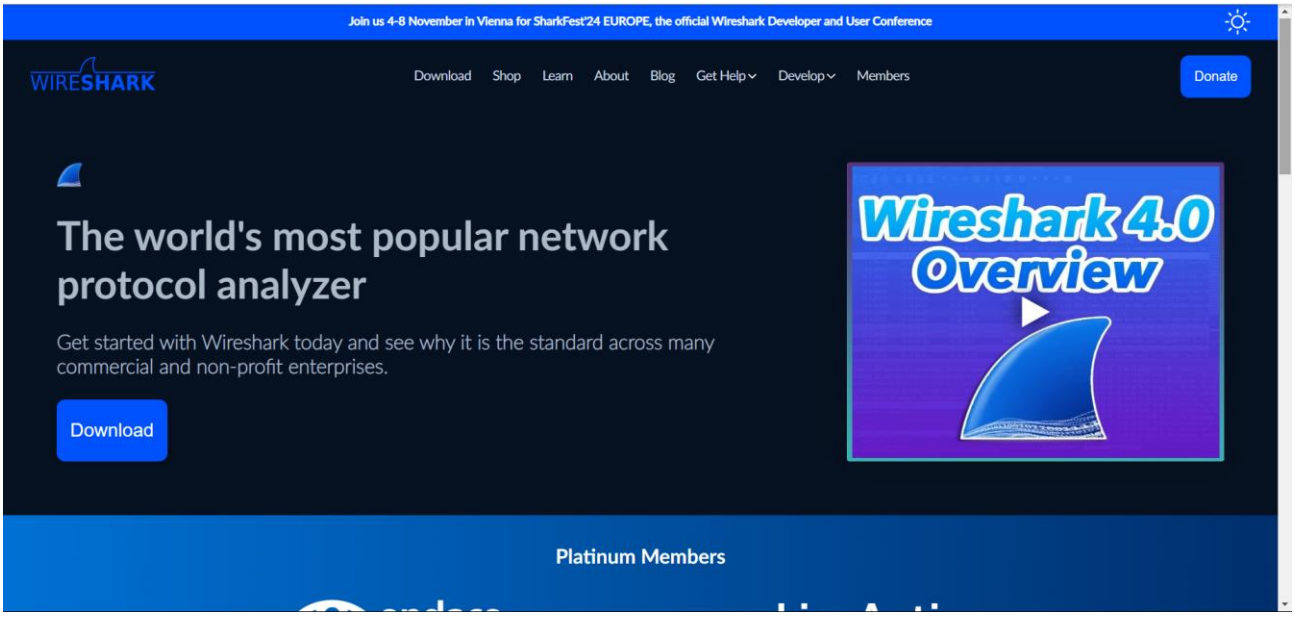
Network Example

Below is a simple network that will be used in this technical note. It features two ACH580s configured for Modbus RTU connected to a Modbus client (ModScan) hosted on a laptop. These are using COM6. COM7 is used separately to connect Wireshark to the Modbus RTU network and capture the traffic:



Wireshark installation

- The latest Wireshark application is available at the following link: https://www.wireshark.org/



- Click on the "Download" icon and select your operating system.

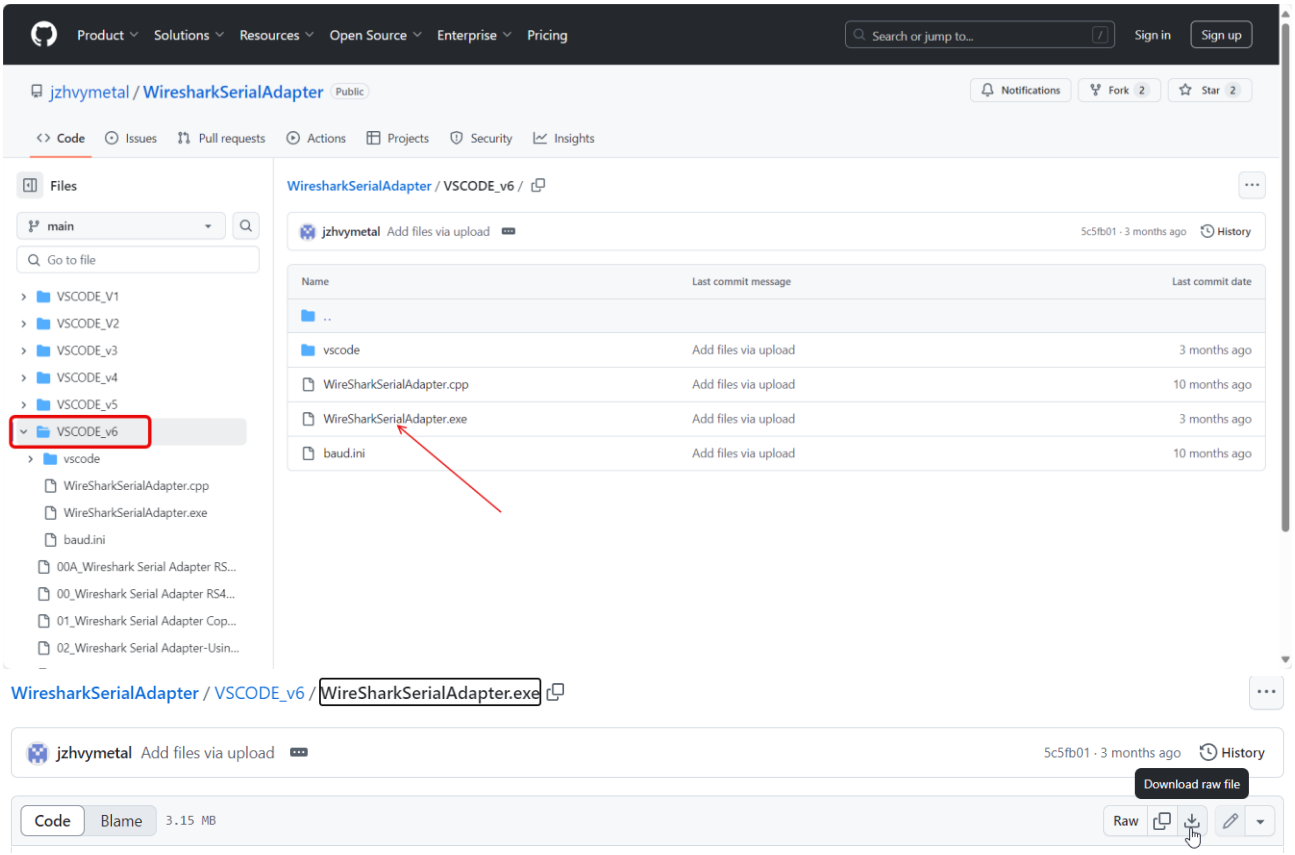
- Launch the downloaded setup file to install Wireshark. The default installation options can typically be used, unless the user has a specific reason to select others.

Modbus RTU capture extension for Wireshark

- With Wireshark installed, there is an additional capture extension for Modbus RTU that must be installed. This extension can be found at the following link:

  GitHub - jzhvymetal/WiresharkSerialAdapter: Wireshark Serial Adapter for Windows

- Navigate to the latest version and download WireSharkSerialAdapter.exe:



- With this file downloaded, navigate to the Wireshark application folder and locate the following subfolder:

System (C:) › Program Files › Wireshark › extcap › wireshark

- If it doesn't exist, create it. Copy WireSharkSerialAdapter.exe to this folder.
- Note that this isn't an executable to be explicitly launched by the user. Wireshark will execute it as an additional capture option.

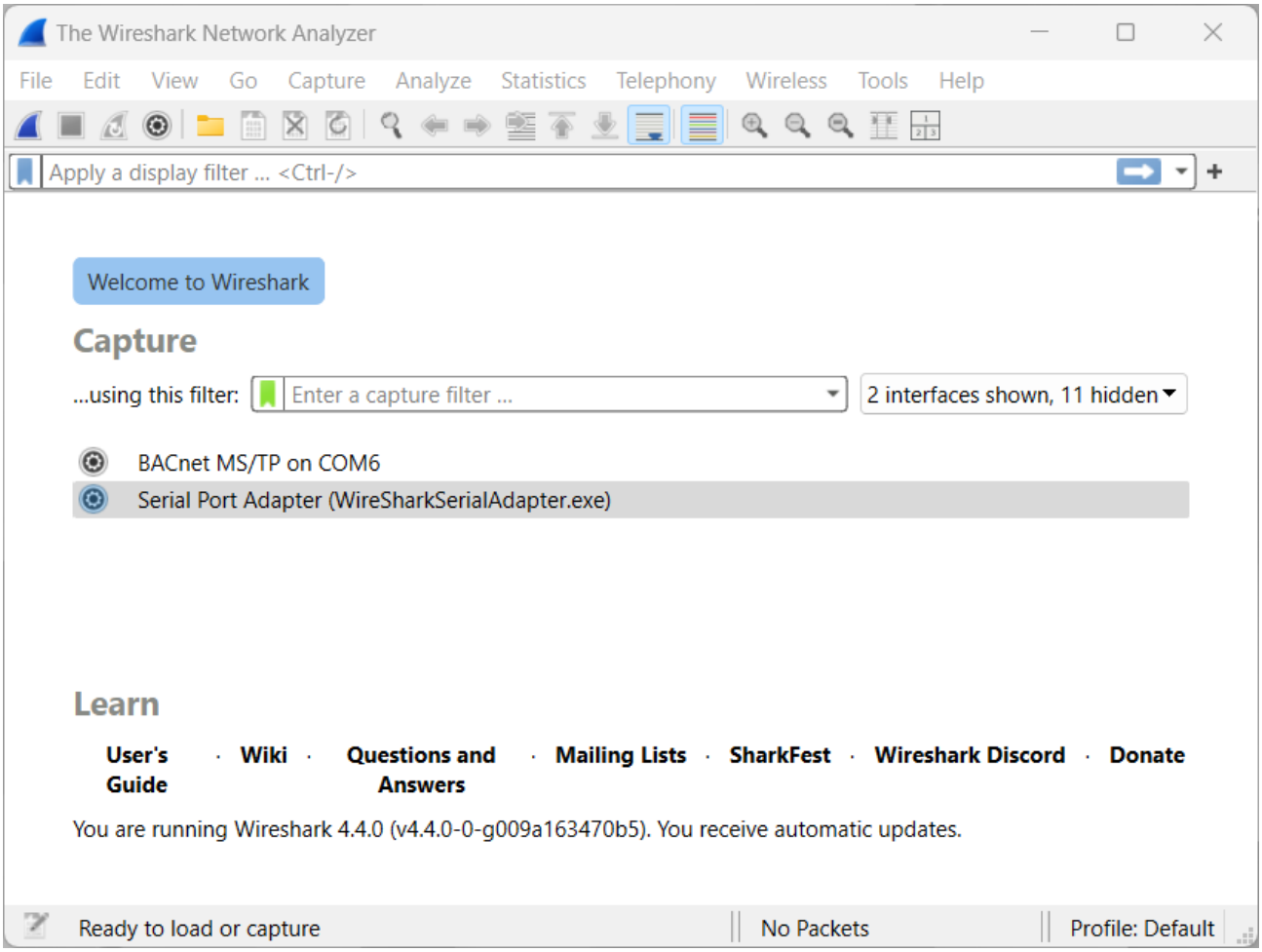
USB-to-485 communication adapter

- This technical note is written assuming a USB-to-485 communication adapter has already been installed and setup on the user's computer. If assistance is needed in getting this setup, please refer to ABB Technical Note 76:

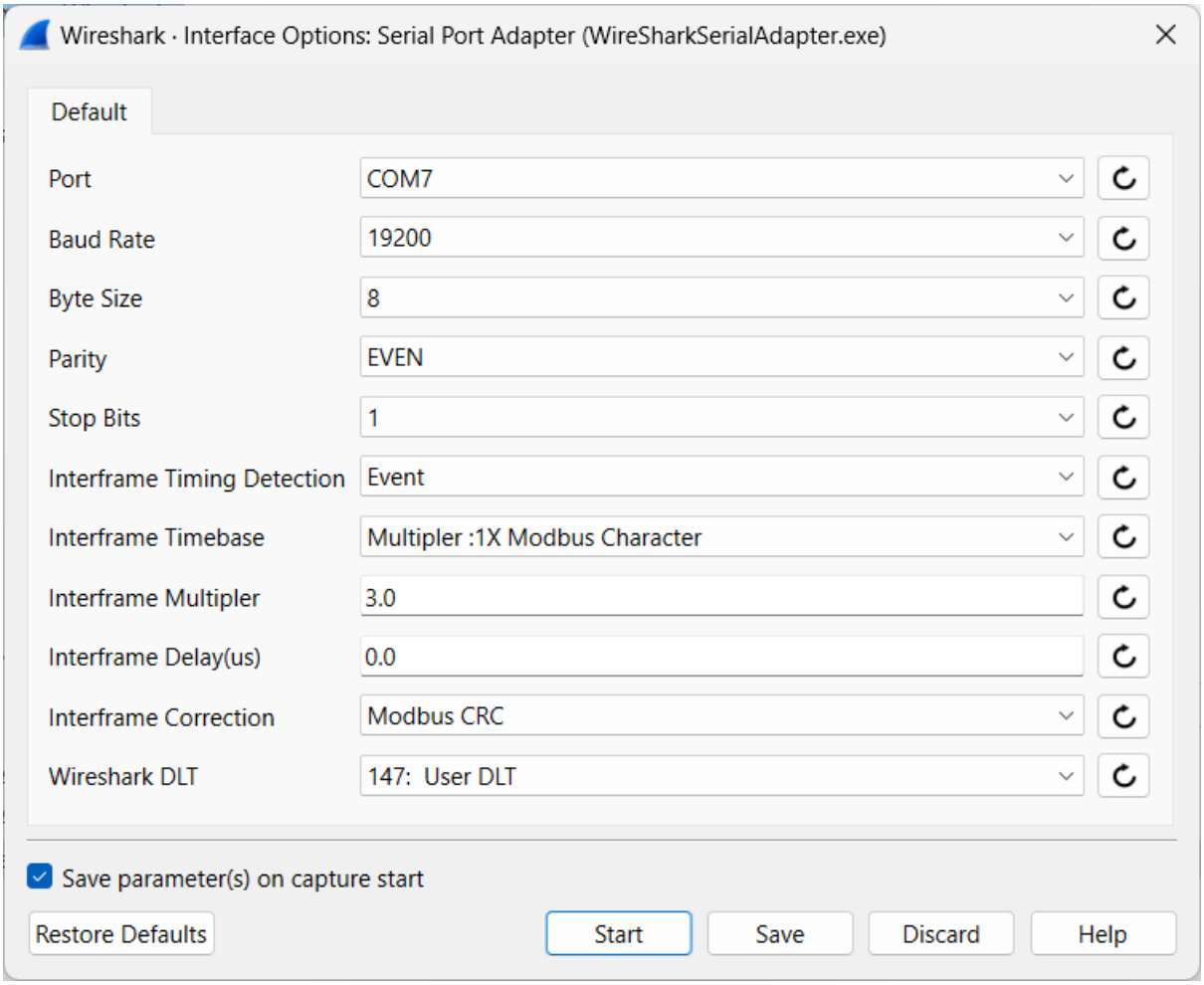
  https://search.abb.com/library/Download.aspx?DocumentID=LVD-EOTKN076U-EN&LanguageCode=en&DocumentPartId=&Action=Launch

Wireshark COM port setup

- Launch the Wireshark application. The initial start-up screen will list the available capture ports. This list will be different for each user's computer, depending on its configuration. Below is an example of what this screen looks like:

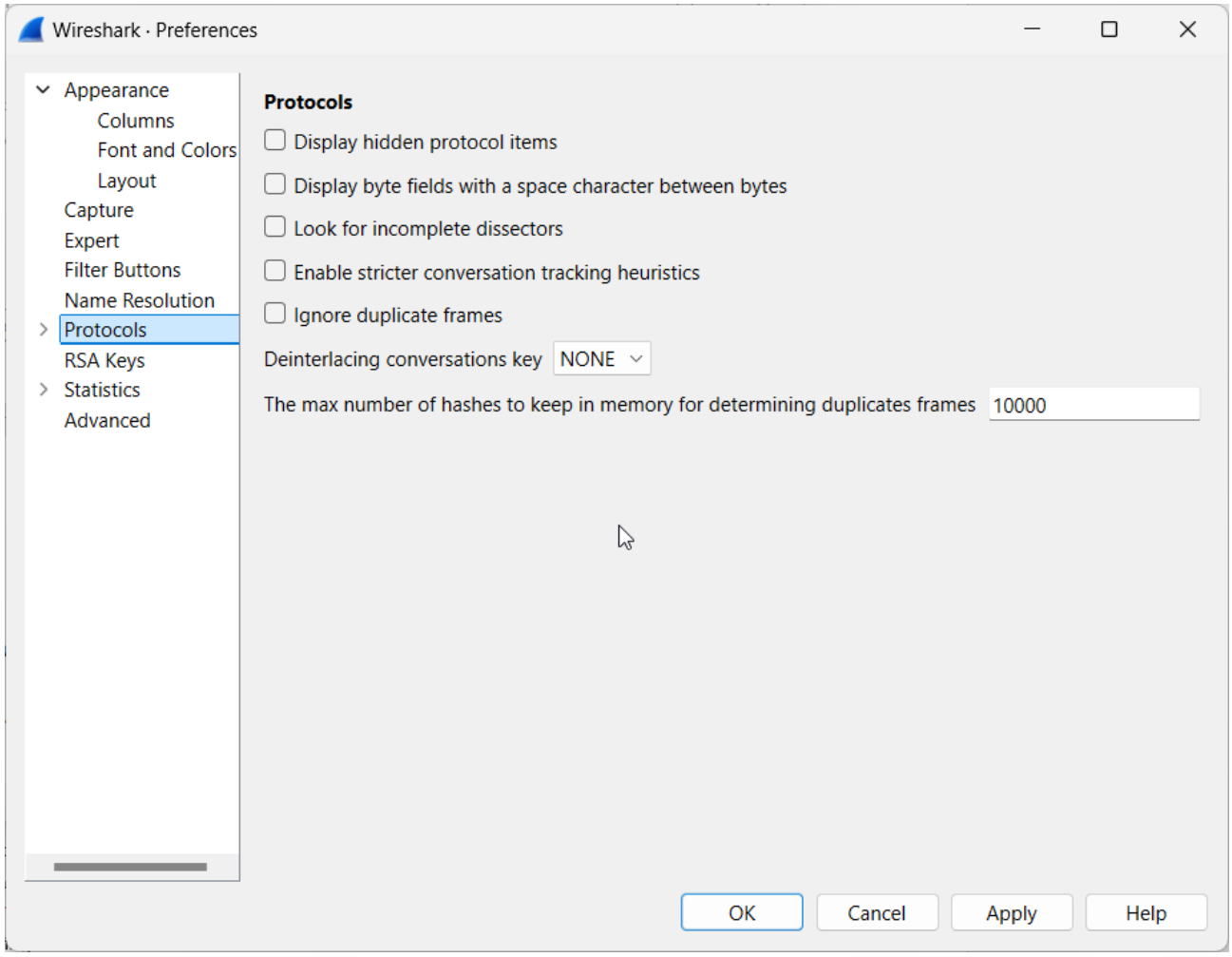


- In this list, Serial Port Adapter (WireSharkSerialAdapter.exe) should be an option. Click on the settings icon to the left to bring up the setup options:

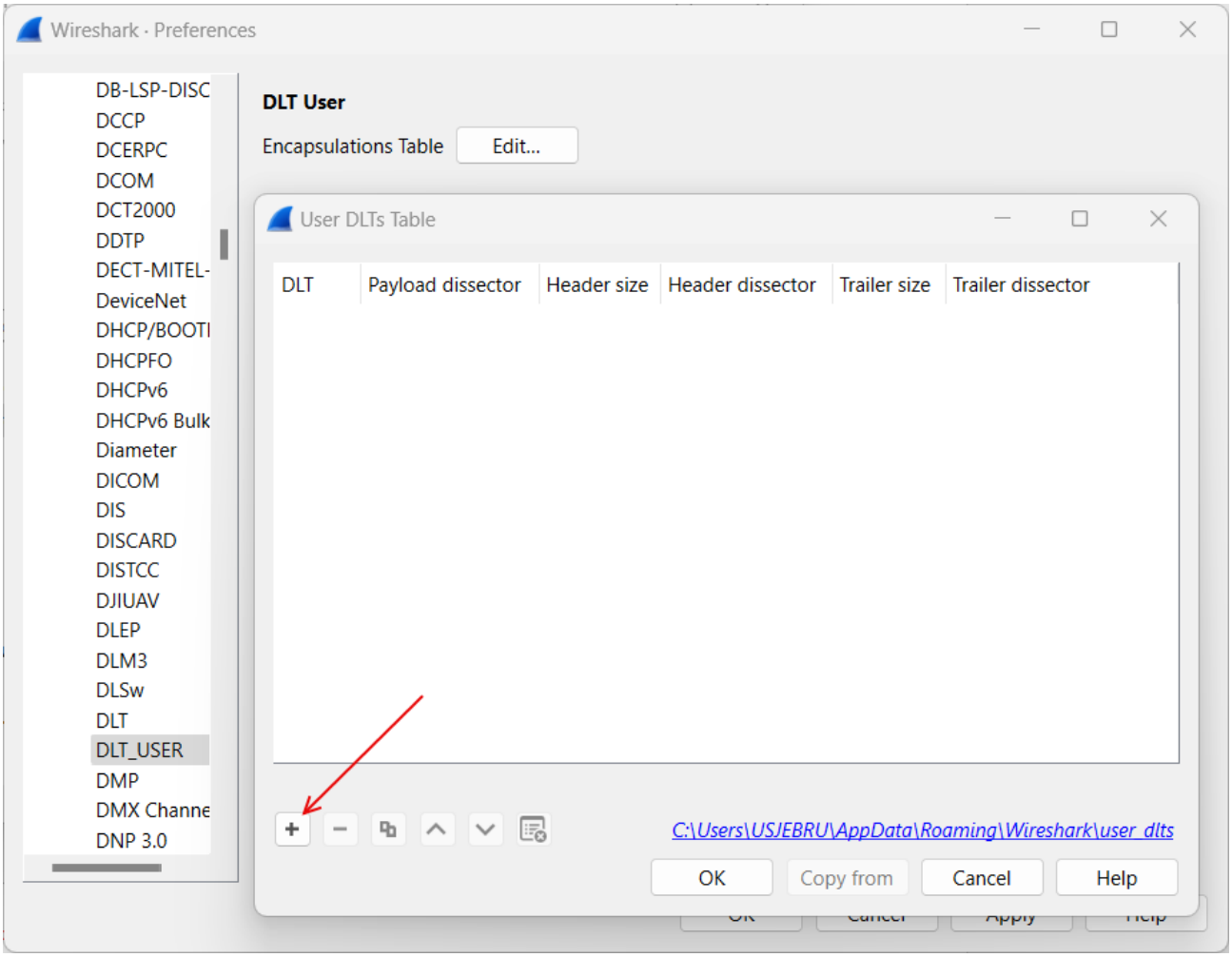


- Launch Windows Device Manager to confirm the COM port assigned to the connected USB-485 adapter
- Select this COM port and set the baud rate, byte size, parity and stop bits of the Modbus RTU channel to be monitored.
- Use the Interframe settings shown in the screenshot above.
- Select User DLT 147 as the Wireshark DLT.
- Save these settings.

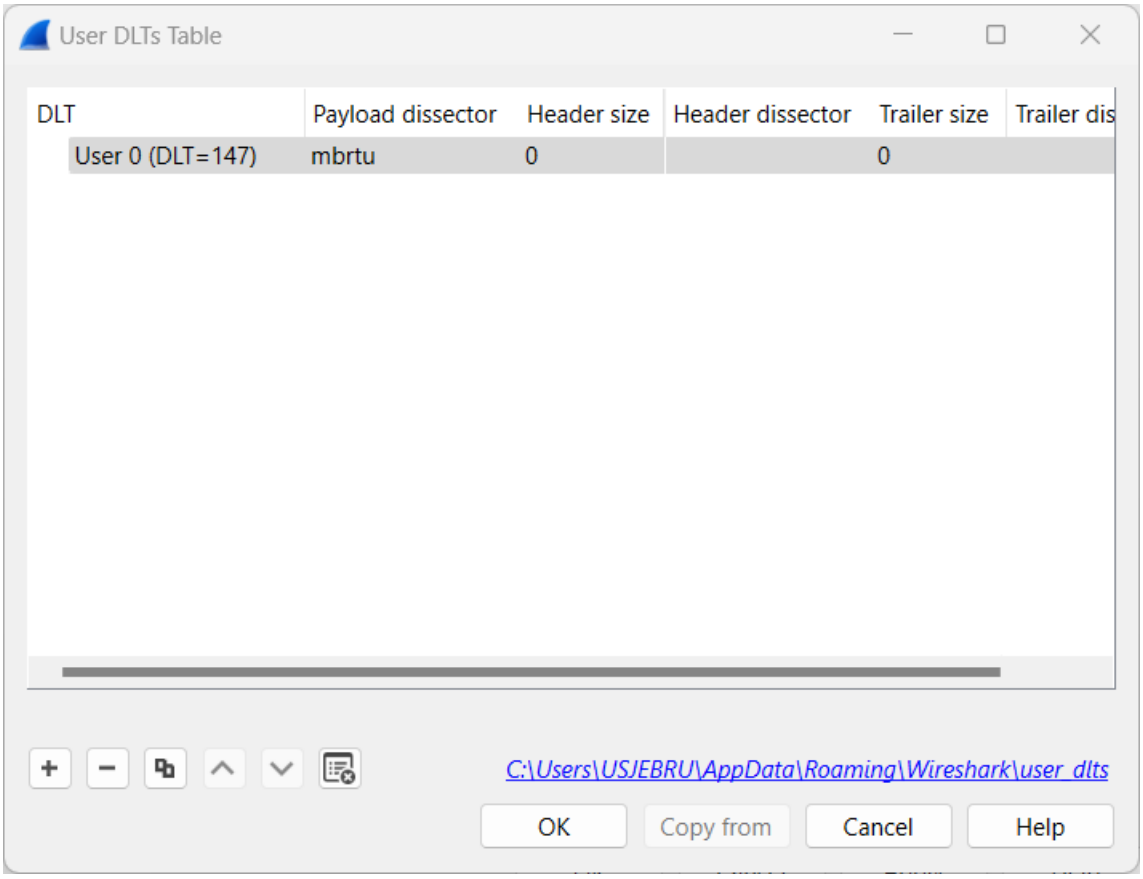
- Returning to the main screen, select Preferences from the Edit pull-down menu and navigate to Protocols:



- Expand Protocols and select DLT_User. Click on Edit to add an entry to the Encapsulation Tables. Click the "+" button to add a DLT:



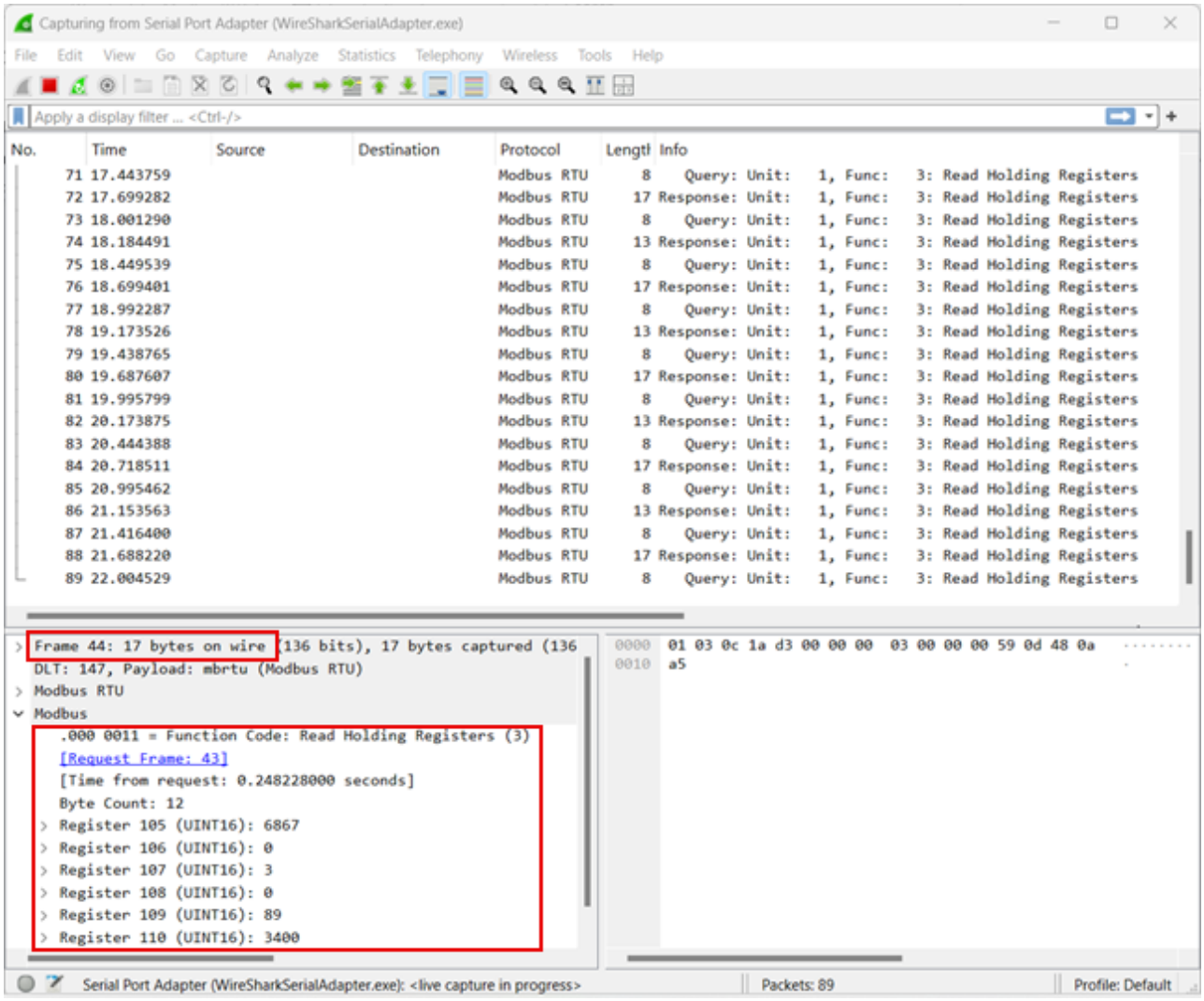
- Select User 0 (DLT = 147) and manually edit the Payload dissector to be mbrtu:



- Click OK and return to the main screen.

Wireshark capture

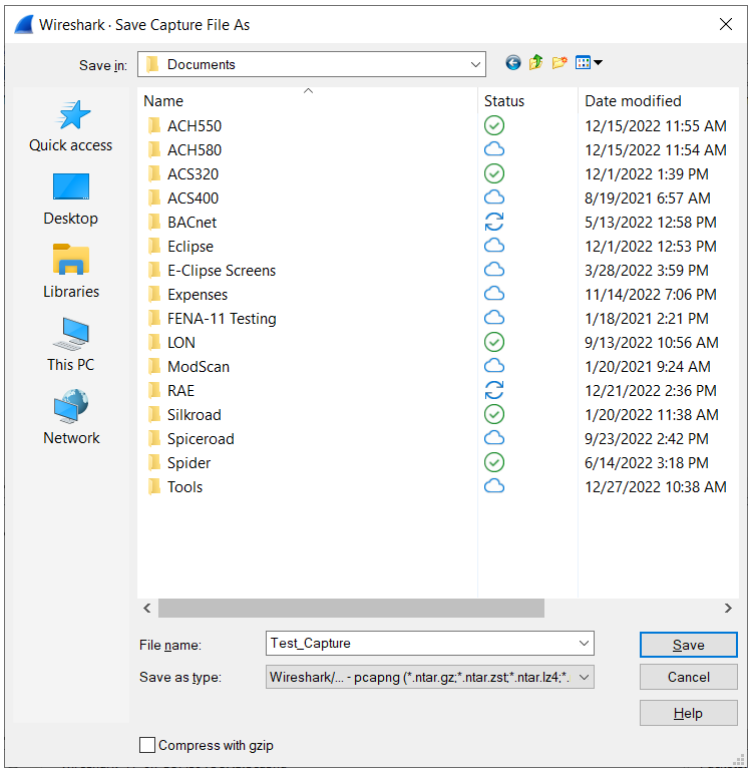
- With the COM port properly configured, a traffic capture is initiated by double-clicking the selected COM port. The content of the capture will depend on the connected devices. The following is an example of the active window panes:



- The main pane is an overall summary of the Modbus RTU traffic, with a brief description of each message type. When a frame is selected in this pane, the lower-left pane contains a breakdown of the packet content by field-type, and the lower-right packet is the packet content in hexadecimal format.
- The selected frame number is displayed in the packet details frame on the lower left, as well as the contents of the Modbus message. In this example, the results of the Modbus Read Holding Request for 6 registers is shown.
- The Wireshark capture is stopped by clicking on the red square, second from the left.

Wireshark capture save

- Finally, the contents of the Wireshark capture can be saved to a file for later review. This is found under the File->Save pulldown:



- Enter a filename and save to a known location. The file extension is .pcapng. This file can be shared for additional review.

Wireshark capture review

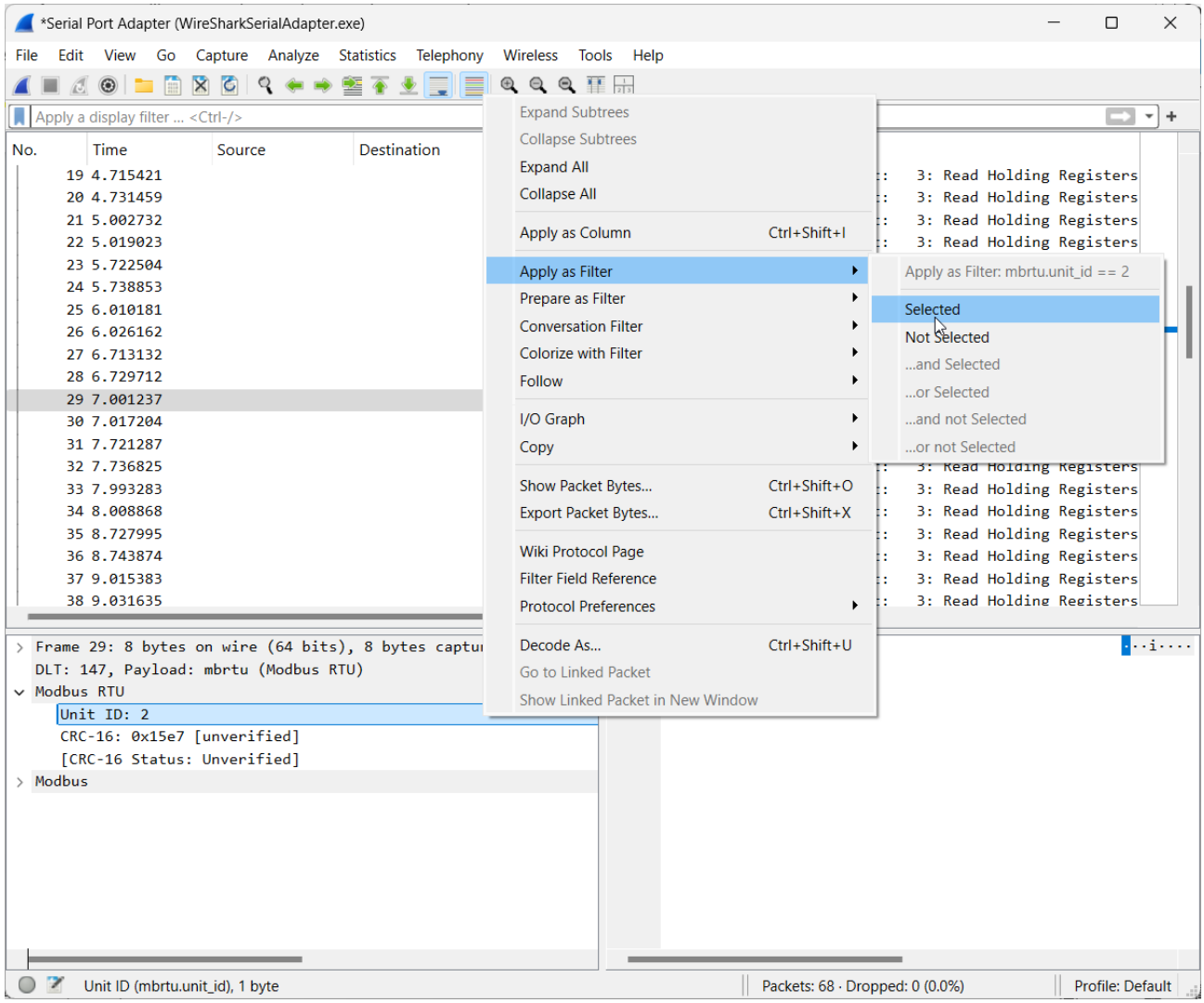
To review a previous Wireshark capture, simply double-click on the .pcapng file and Wireshark will automatically open, proceeding immediately to the capture window shown previously. From here, additional review and filtering can be done to analyze network issues.

Wireshark capture file filtering

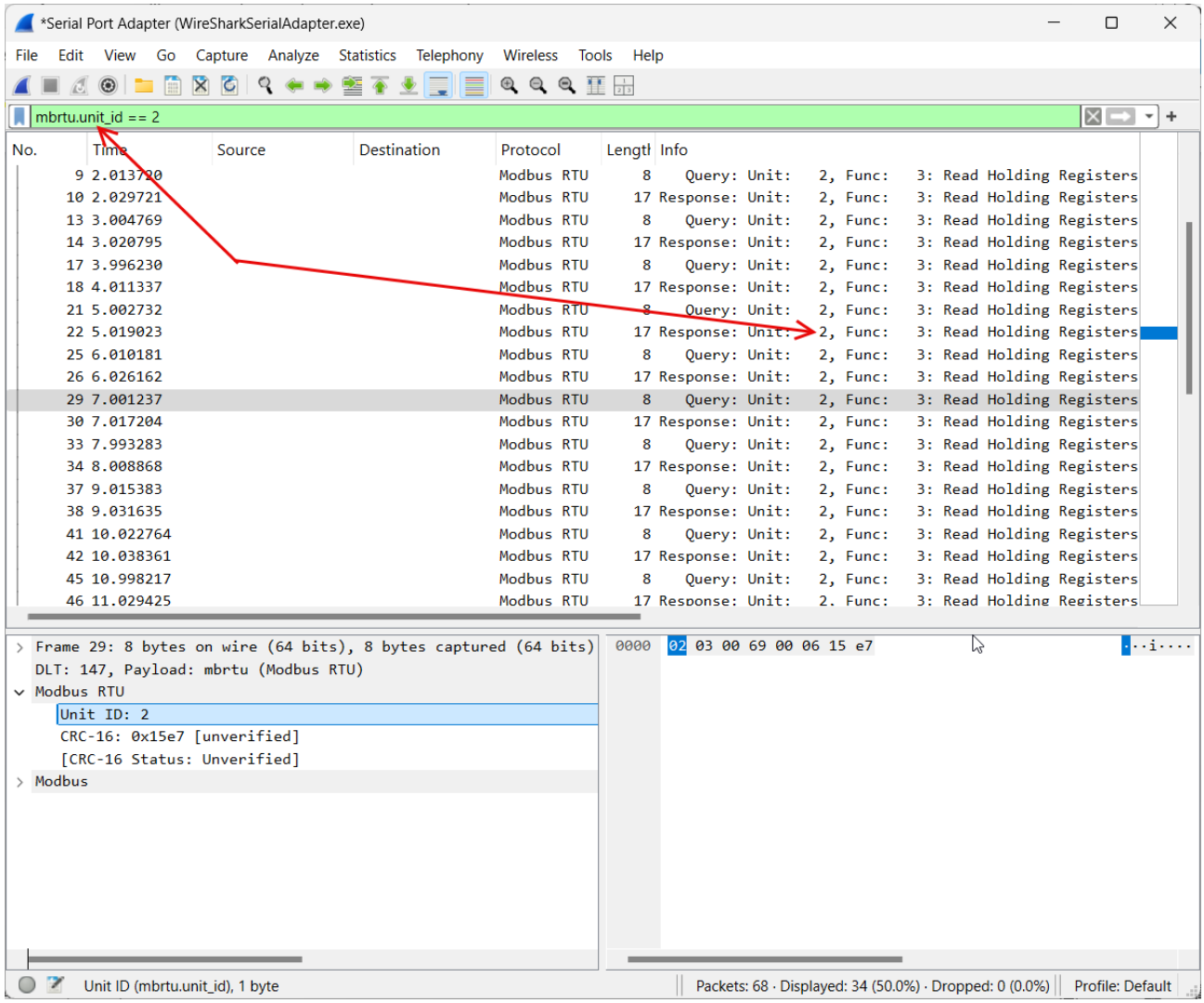
Due to typically large capture files, one of the more useful filtering options is to sort specifically for the device that is reported to have issues. Thus, only those transactions for the device of interest can be isolated and saved to a separate file. This makes capture files much more manageable.

- Select any frame in the upper pane and expand the details in the lower left pane by clicking on the caret next to the Modbus RTU portion of the packet.

- The field of interest for this example is Unit ID. Select it in the lower left pane by clicking on it, and right-mouse click to display the filtering options. From these, select Apply as Filter->Selected:



- This will populate the display filter field with the filter syntax to select Modbus device #2. Only transactions for this device will be displayed:



- These can then be saved to a new capture file which only includes these frames.
- Similar filters can be applied to other message fields to isolate only the frames of interest. This makes capture file sharing and analysis much more manageable.

Summary

Modbus RTU communication issues can be difficult to isolate without visibility of the network traffic. However, with a capture of network traffic, troubleshooting often proceeds very quickly. Wireshark is a free network packet analyzer that is very powerful. Once installed and setup, capturing the traffic on a Modbus RTU network can be accomplished easily, and has shown to be a very valuable tool. This technical note summarizes the installation and setup of Wireshark for Modbus RTU packet traffic.