Wireshark & Modbus Software Guide

V1.1

Created By:	Brian Hobby	Date:	November 2015

PART 1

Software requirements

Students can Logon to Electromeet (Follow the “How to Connect to Remote Labs_Electromeet_HTML5_Remote_Lab” instructions document)

The software is installed on Remote Lab 1 & 2

It is suggested that you run this in a virtual machine using a windows 7 32 bit image so that you do not break your real operating system – highly recommended. They are available for most virtualisation options here: https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/

Software: Wireshark, download and install to your own computer from http://www.wireshark.org

Tutorial video WireShark
http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/

Follow the ModBus specific software supplied.

- SetupVSPE (serial port emulator)
- Modbus slave and master sw.

Modbus Poll - install “mbpollsetup” and use the registration information provided in the Word or RTF file “Modbus_poll_slave_serial_numbers”. - Please note that everything is case sensitive!

Modbus Slave – install “mbslavesetup” as under Modbus Poll.

Virtual Serial Port Emulator – install “SetupVSPE.msi”. - There is a registration string to use in the VSPE_API_32_KEY.TXT file.

Screen Capture software if you don’t have it already a good and free option at http://getgreenshot.org/

Alternately this may be run on Remote Labs 1 and 2. The virtual com port software is different and this will be explained in a separate section.

Purpose / Background

The purpose of the first practical component of this assignment is for you to simulate a Modbus Master querying a Modbus Slave over a serial link.

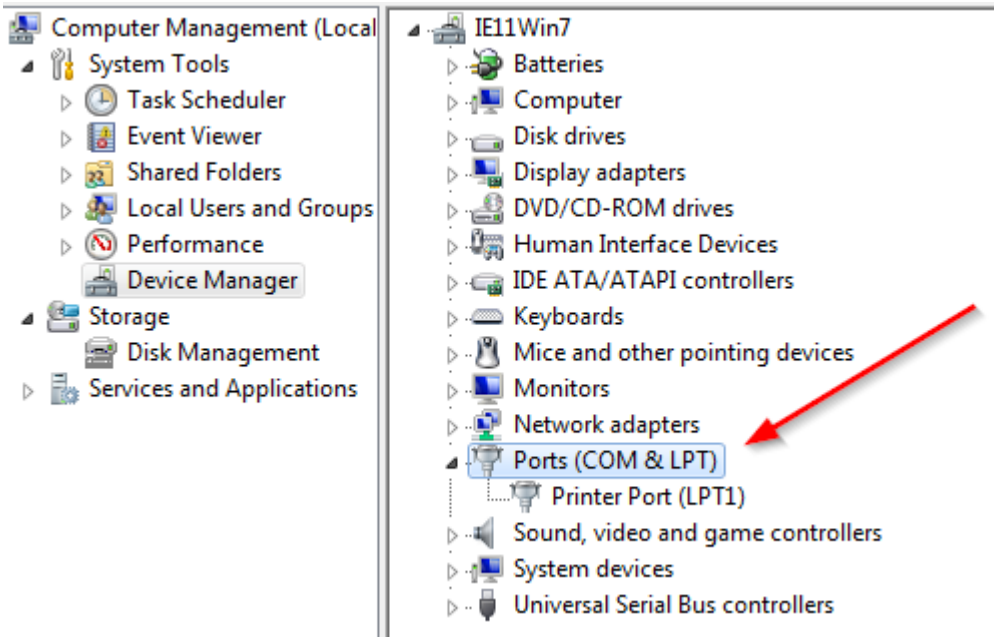
Typically one would run Modbus Poll on one machine and Modbus Slave on another linked by means of a serial communication. If you have 2 machines with Serial ports and a Null Modem cable this can be done with ease.

More typically recent machines do not have a serial port on them and as such one needs to work around this. One can install a USB-Serial converter on each machine and then again, link the 2 machines with a Null Modem cable.

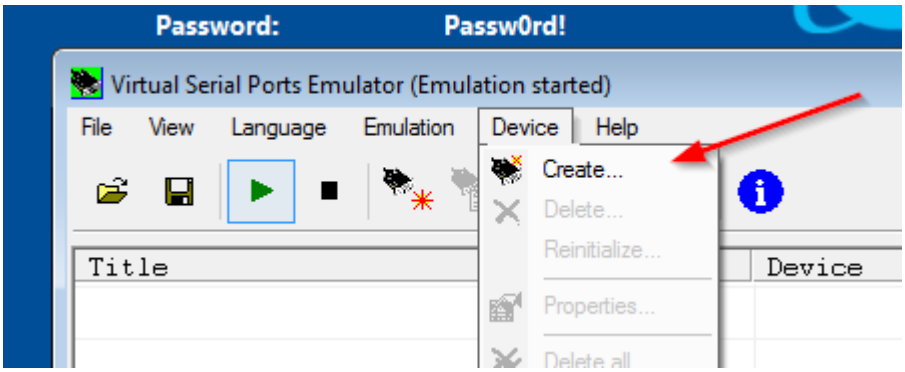
However – we have software - a Virtual Port Serial Emulator (VSPE) where you can run virtual serial ports on ONE PC in a configuration to which both Master and Slave applications can connect.

Virtual Comm Ports

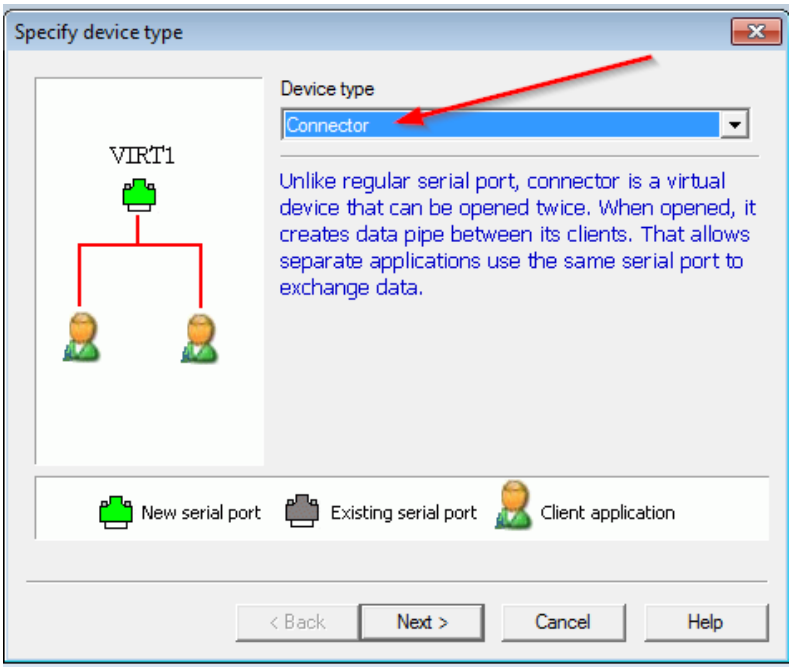
After installing all the software you need to check which serial ports are available on the PC by going into Device Manager and checking. As the example below, this sample is all clear for any port a user wants to use.



One then needs to setup a Connector within VSPE. This then opens up a new virtual serial port which can be opened twice – thus allowing us to run Modbus Poll and Modbus Slave locally within the same machine

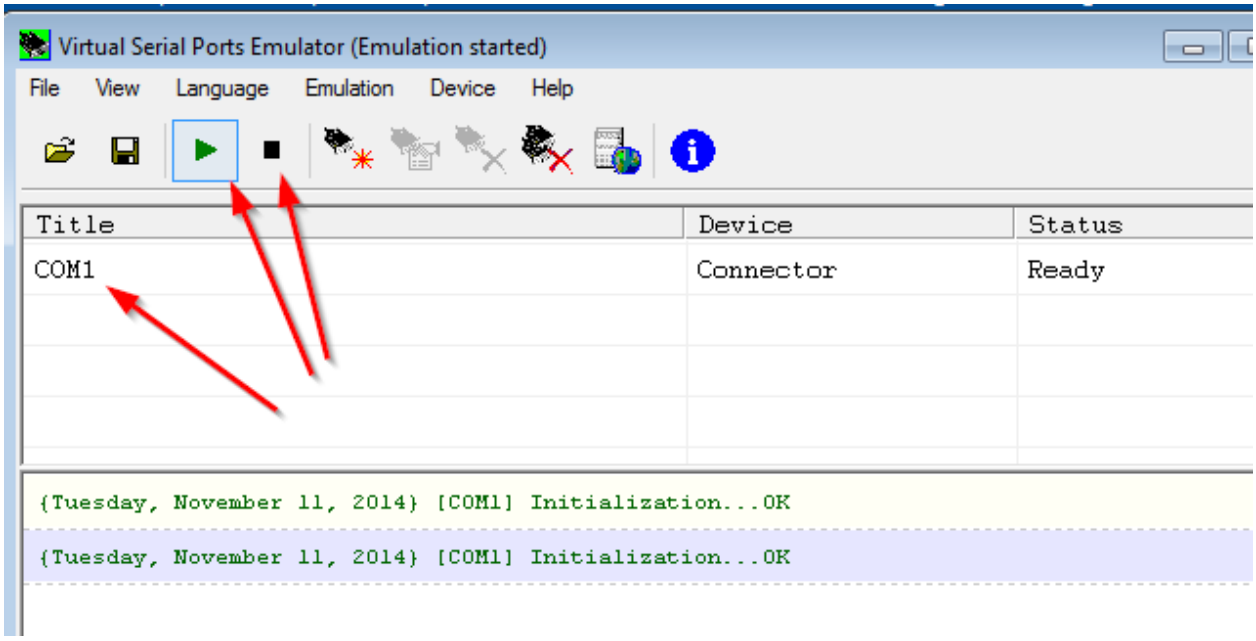


Select Connector and then Next



Pick a free port from your device check and click on “Finish”.

You should now have a virtual comm port that you can turn on and off at will



Once you have nominated the Connector within VSPE the infrastructure is in place. **Note** that you should use a Comm port Number up to and including 8 ONLY, because the Modbus software does not go beyond that. Once you have setup the VSPE Connector minimise it to the Task bar.

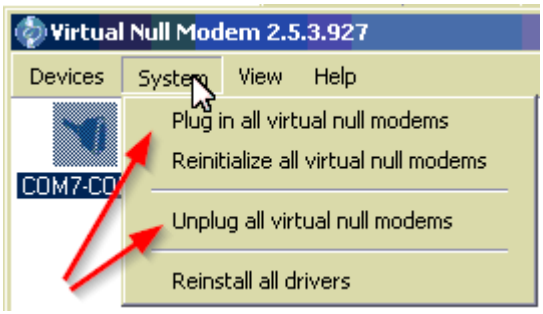
Remote Lab Virtual comm ports

On the remote lab you will find this icon

When double clicking it a window like this should appear

The comm ports shown are a connected pair and you need to set the Modbus Slave to one of them and the Modbus Poll to the other, they may vary between the labs so make sure to check. Ensure you use a pair that is port 8 or less to be compatible with the Modbus software.

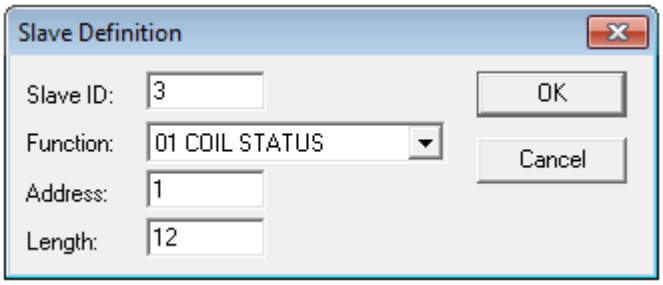
If you don't get serial working in the modbus software you may need to unplug and plug back in the Virtual modem from the system menu



Modbus Slave and Poll

In order to get the link up and running go into Modbus Slave first.
Go into Setup, Slave Definition

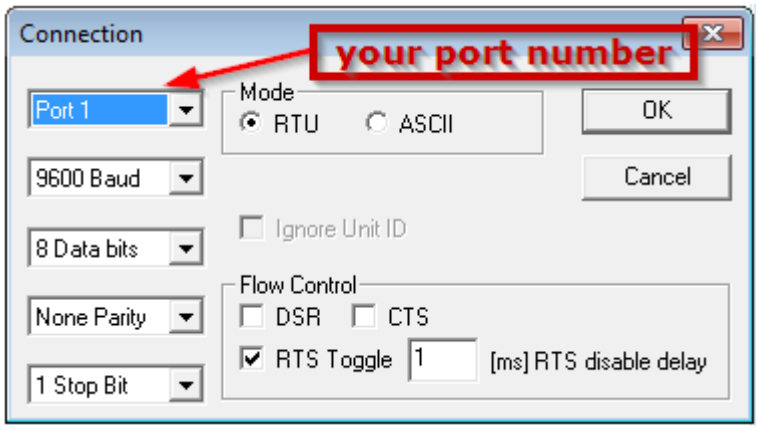
Change the Slave ID to 3 and Function to 01 – Coil Status. Alter the range (Address 1 for a length of 12 coils)
OK this.



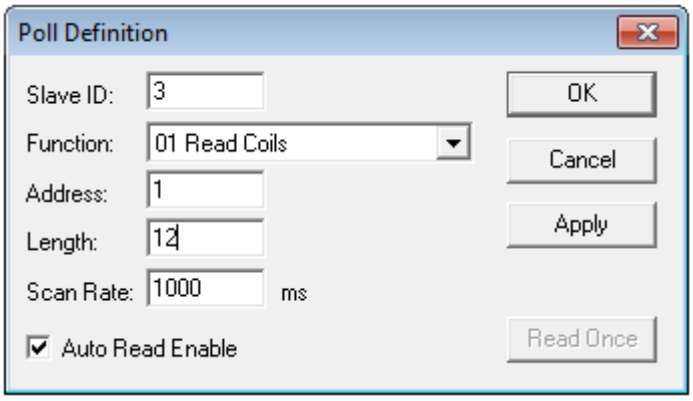
Go into Connection, > Connect.

Select the virtual Connector you have defined in VSPE (or one of the ports on the Lab)
Set the rates … typically 9600, 8 Data Bits, No parity, 1 Stop bit

Select RTU mode
OK this.

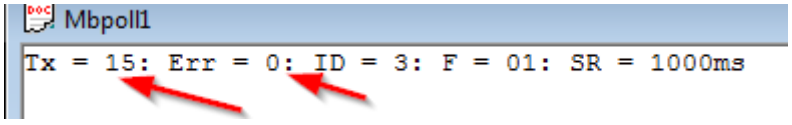


Then go into Modbus Poll.
Go into Setup, > Poll Definition
Change the Slave ID to 3 and Function to 01 – Read Coils. Alter the range (Address 1 for a length of 12 coils)
Leave the Scan rate as 1000 ms.
Click OK.

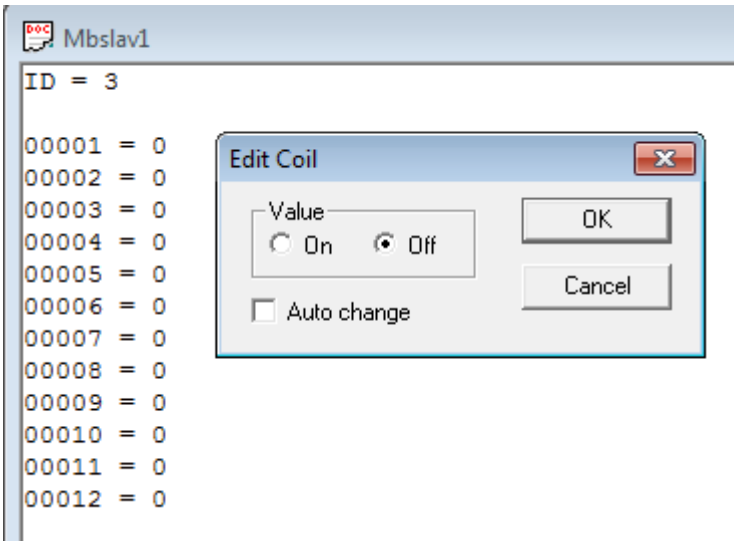


Go into Connection, > Connect.
Select the **same** virtual Connector comm port you have defined in VSPE (or on the Lab the other comm port of the pair)
Set the rates … To what you used in the Slave (note the defaults between Modbus Poll and Slave are different!!)
Select RTU mode
Click OK.

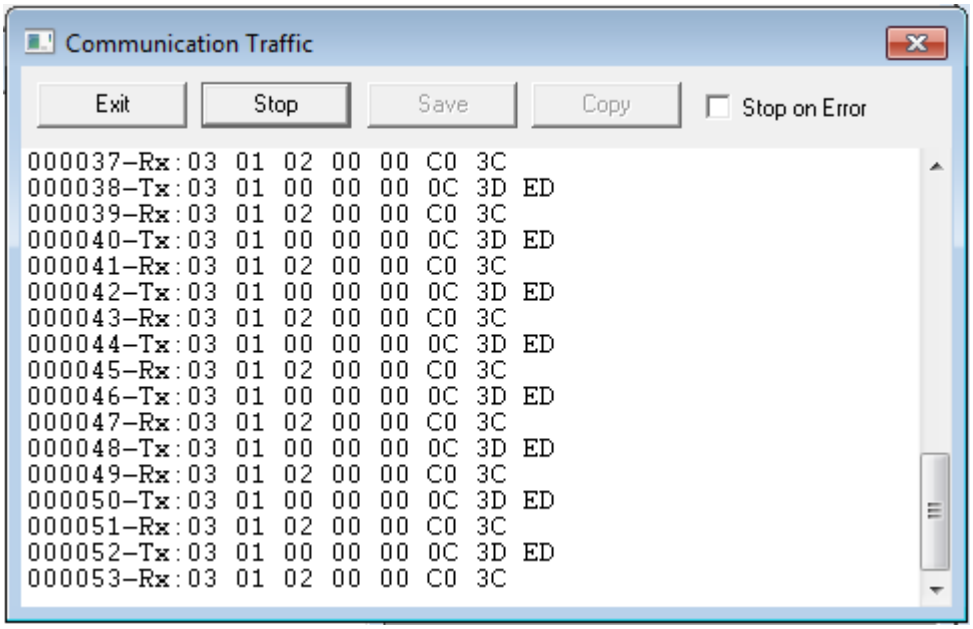
Modbus Poll will then be sending messages to Modbus Slave. You will see this in the Modbus Poll window with Tx and Error count. The Tx should be going up and the error rate not going up (there may be a couple of errors initially).



To change a coil – you can double click on a coil within Modbus Slave and change it). On accepting (clicking OK), you will see the value change within Modbus Master ie. It has been successfully read.



Also please look at Display, Communication in either (the Tx/Rx will be reversed from one to the other) – which shows what is being sent across the network.



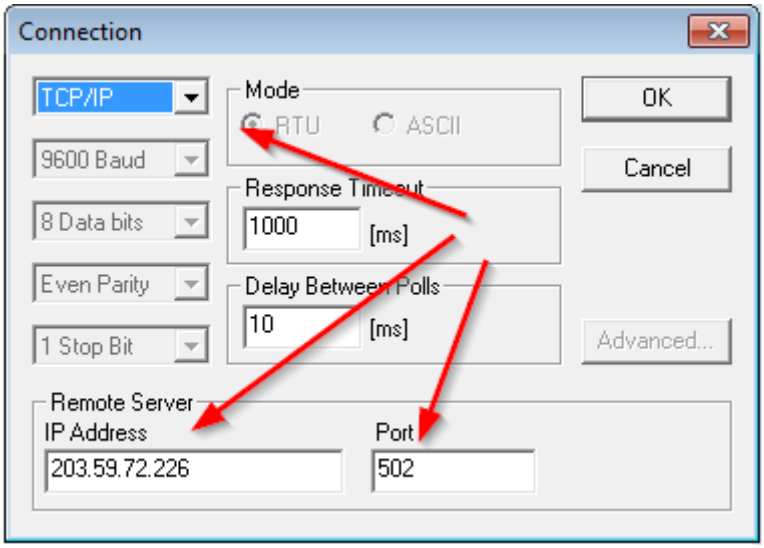
You can play around with the software to familiarise yourself with it all – that is absolutely fine – but please revert to the settings above (in terms of COILS) for the practical unless given other instructions.

Please use screen capture software such as GreenShot to capture screenshots from Modbus Poll / Slave to paste into your Assignment Answer document where directed to support any questions/tasks asked .

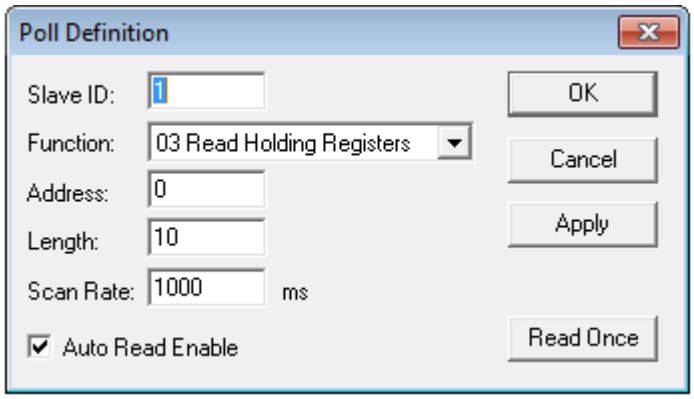
PLEASE do not expect the assessor to interpret these Windows for you – these are backup to show what you have done. YOU must also explicitly answer all questions and if you have any difficulties setting up the software, please contact the module instructor.

PART 2

We are running a Modbus server at IDC as a Remote Lab. So, instead of running MBSlave, use your MBPoll to connect to this server at IP address 203.59.72.226 with standard port number 502. If you are running this on the Remote Labs use IP address 192.168.1.30 port 502



Set Slave ID as 1. Execute an FC03, and read the contents of the first 10 registers using Base 0 addressing. (ie. Relative addresses 0 through 9, set through Display > Protocol Addresses)

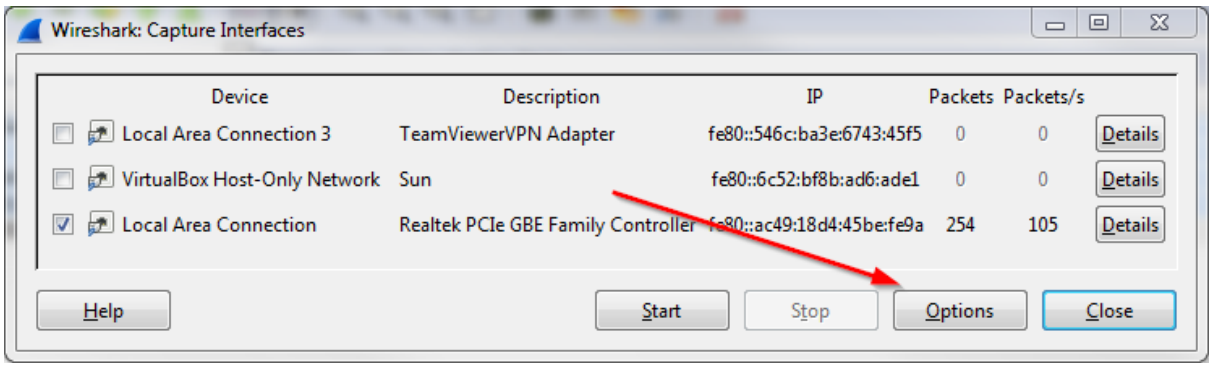


You will see Registers set to values by previous students. Please alter one or two yourself.

Next: Make sure you have the latest version of wire shark.

Now lets grab some modbus packets with wireshark.
Open up WireShark and click the “Capture Interfaces” button or “Capture > Interfaces”

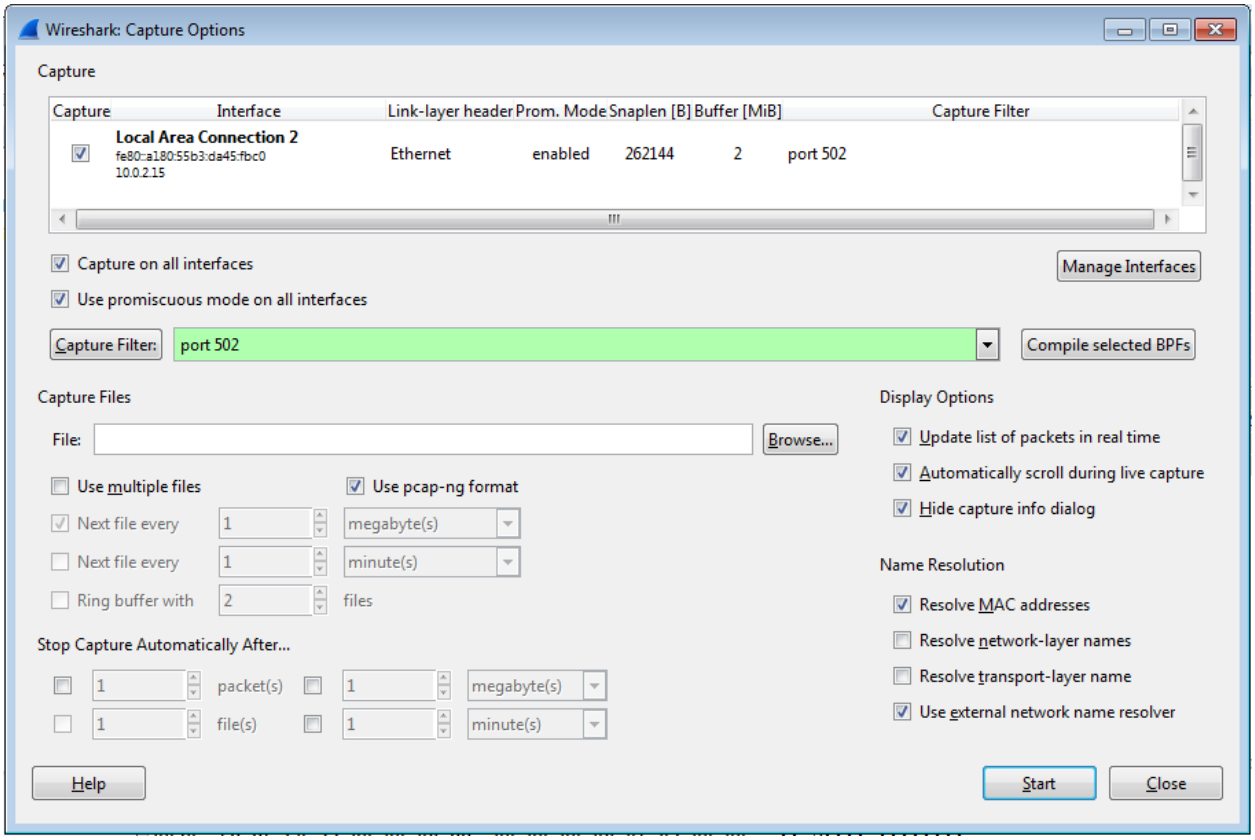
In this window click options



Select your interface

Add a filter so we only capture modbus packets

Then click Start



Once you have some packets “stop capture”

You should have something like this, open up the tree structure and explore the packets you have captured