ICS011 ICS Lab 3 Packet Capture and Analysis with Wireshark

Lab Objective

The objective of this lab is to use Wireshark to capture packets from a network on the HMI programming device.

In this lab, you will learn to:

- Capture and analyze packets with Wireshark

Lab Environment

This lab requires Wireshark and the ICS lab kit.

Lab Duration

25 minutes

Lab Tasks

Capture packets on the network using Wireshark.

Background

Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Lab Scenario

Once network access is obtained, the network can be scanned for packets using Wireshark. The packets captured can then be used for further analysis. Full documentation for Wireshark can be found at https://www.wireshark.org/#learnWS.

Lab Procedure-Using Wireshark

Today, a typical Ethernet network will use switches to connect the Ethernet nodes together. This can increase network performance, but makes life much harder when capturing packets (Wireshark). Frames sent on a switch use an internal table called a MAC Address table to keep track of each device and the port that it is connected. Frames arriving at the switch are delivered directly to the destination port for efficient use of bandwidth. This creates a problem since our sniffing device is connected to another port outside of the communication path between the PLC and programming device.

In this lab, we will capture packets exchanged between the programming device and PLC in order to understand the use of Wireshark.

1. Launch Wireshark using the name of an interface under Interface List to start capturing packets on that interface. For this lab, we will use the wired interface to capture packets on the PLC programming device. **Fig. 1**

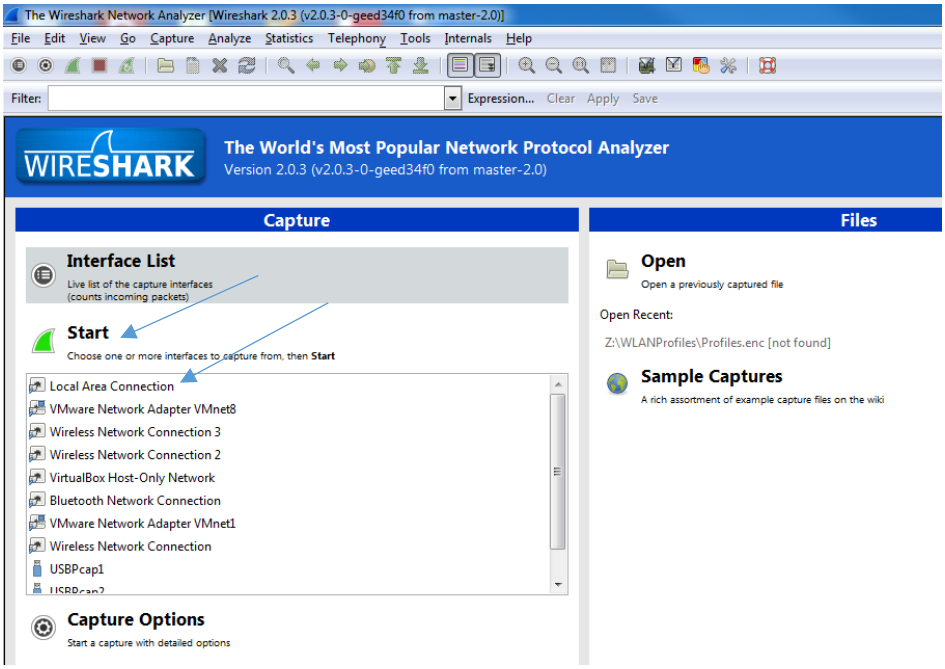

Fig. 1

2. Select the interface and click ***Start***.
3. Packets captured will be displayed in three panes from the main window. Fig 2
    a. Pane 1 contains packets as read on the wire.
    b. Pane 2 is the Packet Pane Details.
    c. Pane 3 shows the Packet Bytes in hexadecimal format.

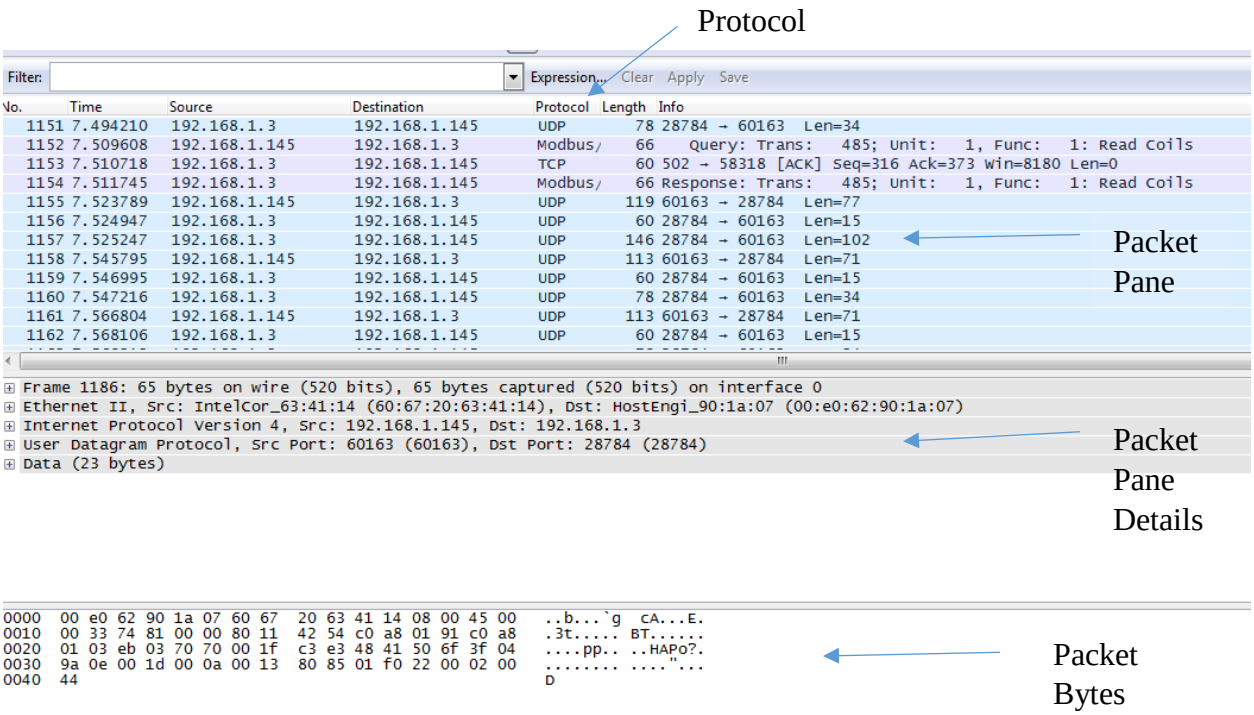

Fig 2

4. Click on any packet with the protocol listed as Modbus/TCP to view the contents.

NOTE: Certain implementations of Modbus may be seen as ***asa-appl-pro*** in the Wireshark application. Asa-appl-pro basically encapsulates the Modbus traffic to the HMI device. The source or destination ports may be different than port 502, but at least one port will be noted as 502.

5. The contents of the frame originated from the Application layer as an Application Data Unit (ADU). Fig. 3

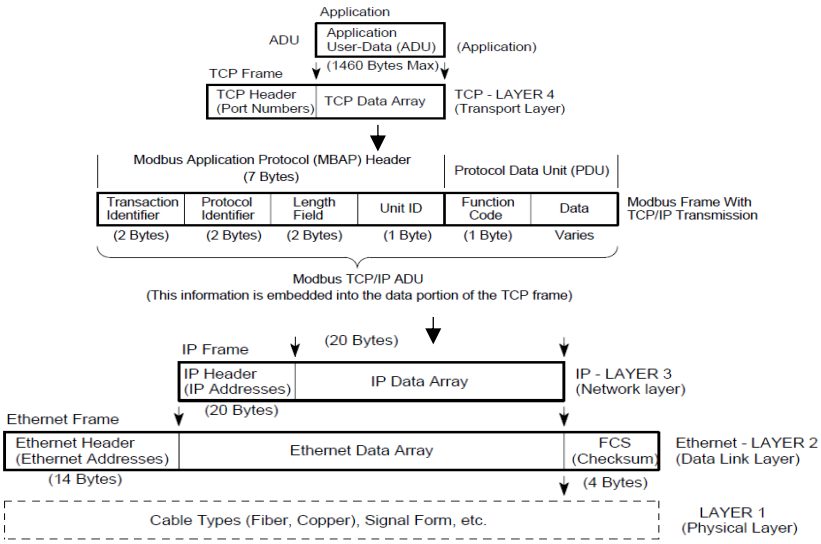

Fig. 3

6. Packet Pane List. Fig. 4

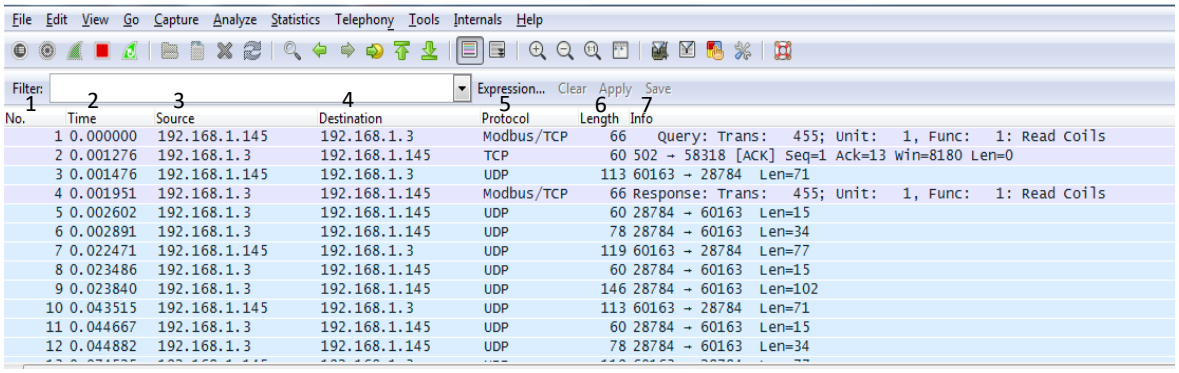

Fig. 4

The default columns will show:

1. **No.** The number of the packet in the capture file. This number will not change, even if a display filter is used.
2. **Time** The timestamp of the packet.
3. **Source** The address where this packet is coming from.
4. **Destination** The address where this packet is going.
5. **Protocol** The protocol name in a short (perhaps abbreviated) version.
6. **Length** The length of each packet.

7. **Info** Additional information about the packet content.

7. Once you have selected a packet of interest (Modbus/TCP), you can now observe the Details Pane to view the information for that particular packet. Fig. 5

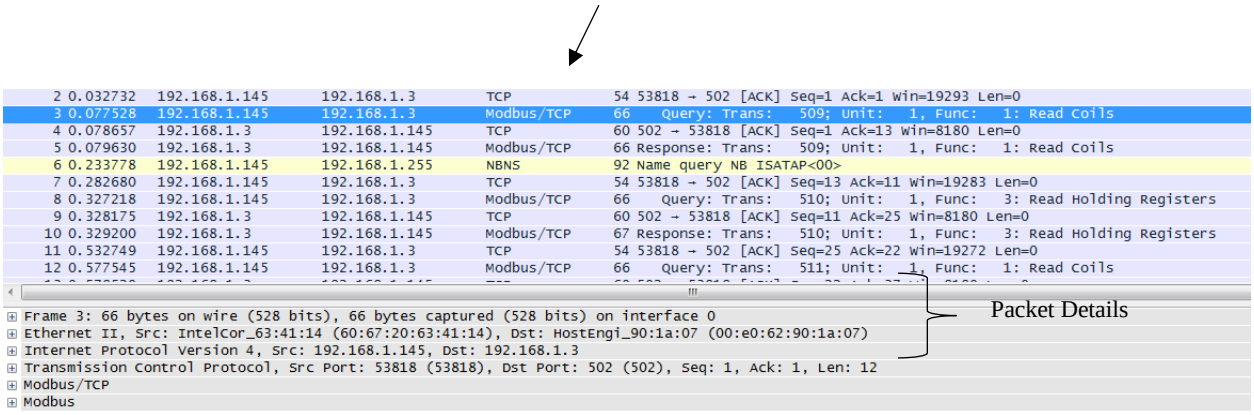

Fig. 5

8. Click the plus sign next to second row where it reads Ethernet II to expand the contents. Fig. 6

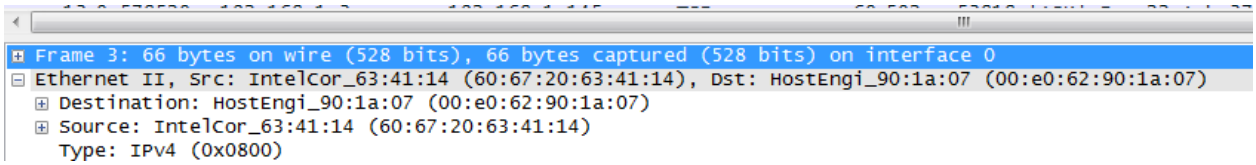

Fig. 6

- What is the source MAC address from where the frame originated? _____
- What is the destination MAC address of the device receiving the frame?_____

9. Click on the third row where it reads Internet Protocol Version 4. Fig. 7

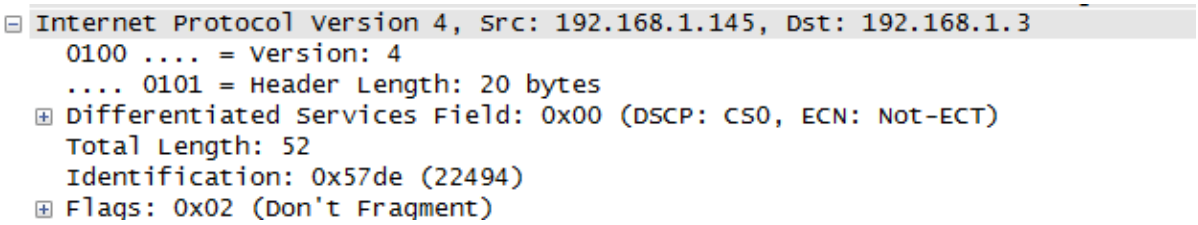

Fig. 7

- What is the source IP Address from where the frame originated? _____
- What is the destination IP Address of the device receiving the frame?_____

10. Click on the fourth row where it reads Transmission Control Protocol. Fig. 8

```
Transmission Control Protocol, Src Port: 53818 (53818), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
    Source Port: 53818
    Destination Port: 502
    [Stream index: 0]
    [TCP Segment Len: 12]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 13    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ⊞ Flags: 0x018 (PSH, ACK)
    Window size value: 19293
    [Calculated window size: 19293]
    [Window size scaling factor: -1 (unknown)]
  ⊞ Checksum: 0x20d4 [validation disabled]
    Urgent pointer: 0
  ⊞ [SEQ/ACK analysis]
    [PDU Size: 12]
```

Fig. 8

- What is the source port from where the frame originated? _____
- What is the destination port of the device receiving the frame?_____

11. Expand Modbus/TCP and Modbus details. Fig. 9

```
⊟ Modbus/TCP
    Transaction Identifier: 510
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 1
⊟ Modbus
    Function Code: Read Holding Registers (3)
    [Request Frame: 8]
    Byte Count: 2
    Register 0 (UINT16): 6050
```

Fig. 9

Examine the contents (payload) of the Modbus/TCP.

12. Create a filter in Wireshark to view only Modbus traffic. Fig. 10

a. Type: **tcp.port eq 502** into the Filter box and click Apply

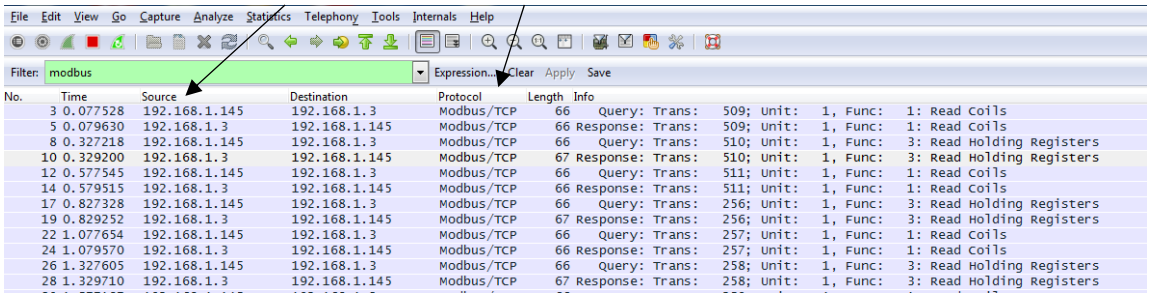

Fig. 10

You can now view only the Modbus protocol operating on port 502

13. At this point, save the capture for further analysis. Fig. 11

a. Stop the capture
b. Click File-Save As
c. Type Filename as: **modbusfilter** to your Desktop.

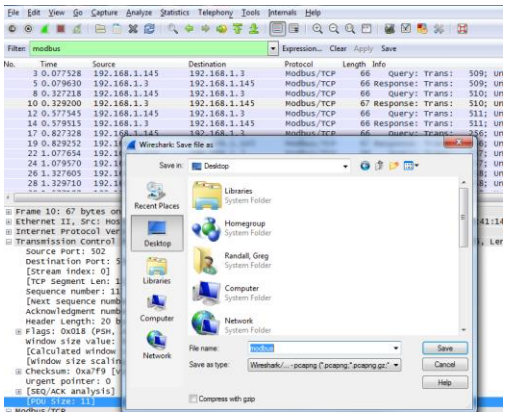

Fig. 11

References

Wireshark. "CaptureSetup/Ethernet - The Wireshark Wiki." *FrontPage - The Wireshark Wiki*. N.p., 12 Sept. 2014. Web. 22 May 2016.