

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**

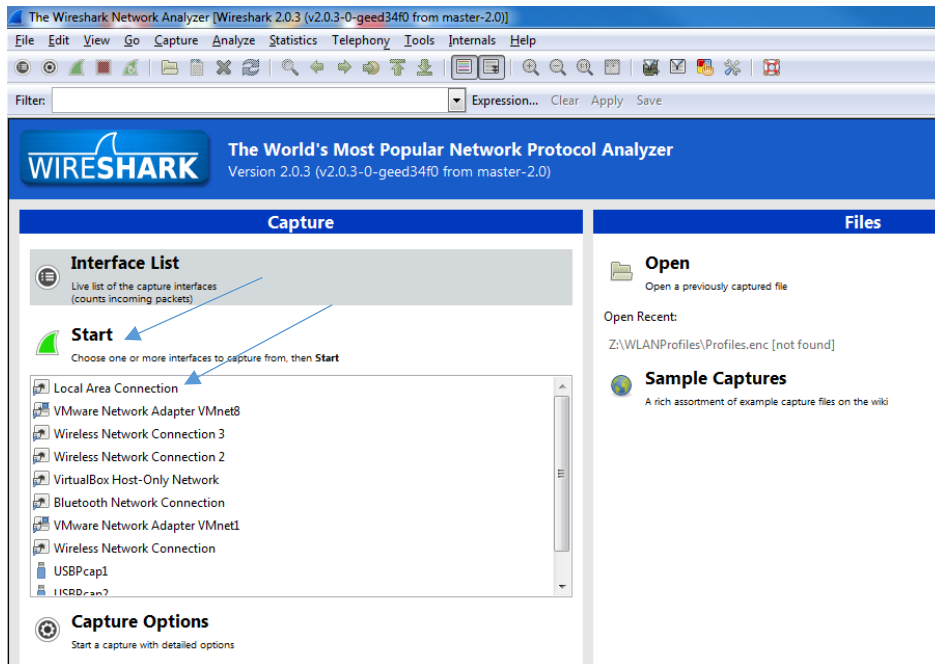


Fig. 1

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.

Protocol

The screenshot shows the Wireshark Network Analyzer interface with the 'Packet Pane' selected. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The 'Packet Pane Details' pane shows the details of the selected packet (Frame 1186), and the 'Packet Bytes' pane shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
1151	7.494210	192.168.1.3	192.168.1.145	UDP	78	28784 → 60163 Len=34
1152	7.509608	192.168.1.145	192.168.1.3	Modbus/	66	Query: Trans: 485; Unit: 1, Func: 1: Read Coils
1153	7.510718	192.168.1.3	192.168.1.145	TCP	60	502 → 58318 [ACK] Seq=316 Ack=373 win=8180 Len=0
1154	7.511745	192.168.1.3	192.168.1.145	Modbus/	66	Response: Trans: 485; Unit: 1, Func: 1: Read Coils
1155	7.523789	192.168.1.145	192.168.1.3	UDP	119	60163 → 28784 Len=77
1156	7.524947	192.168.1.3	192.168.1.145	UDP	60	28784 → 60163 Len=15
1157	7.525247	192.168.1.3	192.168.1.145	UDP	146	28784 → 60163 Len=102
1158	7.545795	192.168.1.145	192.168.1.3	UDP	113	60163 → 28784 Len=71
1159	7.546995	192.168.1.3	192.168.1.145	UDP	60	28784 → 60163 Len=15
1160	7.547216	192.168.1.3	192.168.1.145	UDP	78	28784 → 60163 Len=34
1161	7.566804	192.168.1.145	192.168.1.3	UDP	113	60163 → 28784 Len=71
1162	7.568106	192.168.1.3	192.168.1.145	UDP	60	28784 → 60163 Len=15

Frame 1186: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
 Ethernet II, Src: IntelCor_63:41:14 (60:67:20:63:41:14), Dst: HostEngi_90:1a:07 (00:e0:62:90:1a:07)
 Internet Protocol Version 4, Src: 192.168.1.145, Dst: 192.168.1.3
 User Datagram Protocol, Src Port: 60163 (60163), Dst Port: 28784 (28784)
 Data (23 bytes)

```

0000  00 e0 62 90 1a 07 60 67 20 63 41 14 08 00 45 00  ..b...`g  CA...E.
0010  00 33 74 81 00 00 80 11 42 54 c0 a8 01 91 c0 a8  ..3t.... BT.....
0020  01 03 eb 03 70 70 00 1f c3 e3 48 41 50 6f 3f 04  ....pp.. ..HAPo?..
0030  9a 0e 00 1d 00 0a 00 13 80 85 01 f0 22 00 02 00  ....
0040  44
  
```

Fig 2

- 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.

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

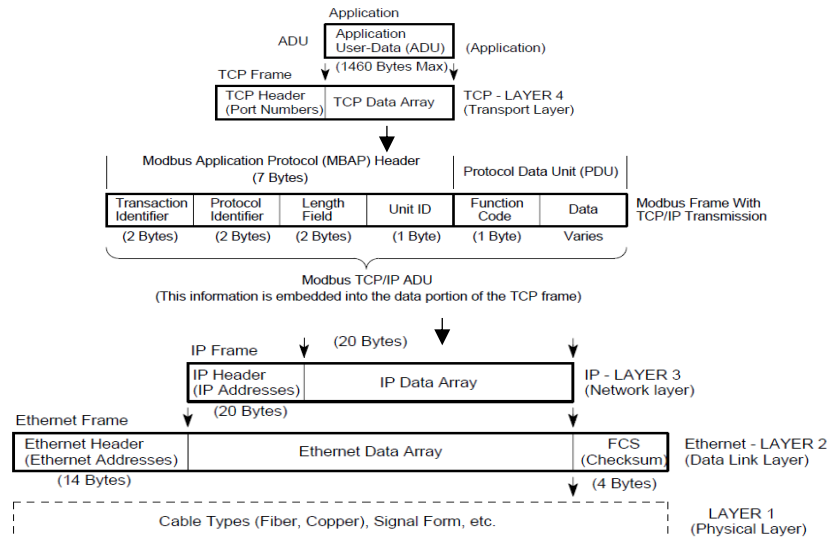


Fig. 3

- Packet Pane List. Fig. 4

1	2	3	4	5	6	7
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 455; Unit: 1, Func: 1: Read Coils
2	0.001276	192.168.1.3	192.168.1.145	TCP	60	502 → 58318 [ACK] Seq=1 Ack=13 win=8180 Len=0
3	0.001476	192.168.1.145	192.168.1.3	UDP	113	60163 → 28784 Len=71
4	0.001951	192.168.1.3	192.168.1.145	Modbus/TCP	66	Response: Trans: 455; Unit: 1, Func: 1: Read Coils
5	0.002602	192.168.1.3	192.168.1.145	UDP	60	28784 → 60163 Len=15
6	0.002891	192.168.1.3	192.168.1.145	UDP	78	28784 → 60163 Len=34
7	0.022471	192.168.1.145	192.168.1.3	UDP	119	60163 → 28784 Len=77
8	0.023486	192.168.1.3	192.168.1.145	UDP	60	28784 → 60163 Len=15
9	0.023840	192.168.1.3	192.168.1.145	UDP	146	28784 → 60163 Len=102
10	0.043515	192.168.1.145	192.168.1.3	UDP	113	60163 → 28784 Len=71
11	0.044667	192.168.1.3	192.168.1.145	UDP	60	28784 → 60163 Len=15
12	0.044882	192.168.1.3	192.168.1.145	UDP	78	28784 → 60163 Len=34

Fig. 4

The default columns will show:

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

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

- 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

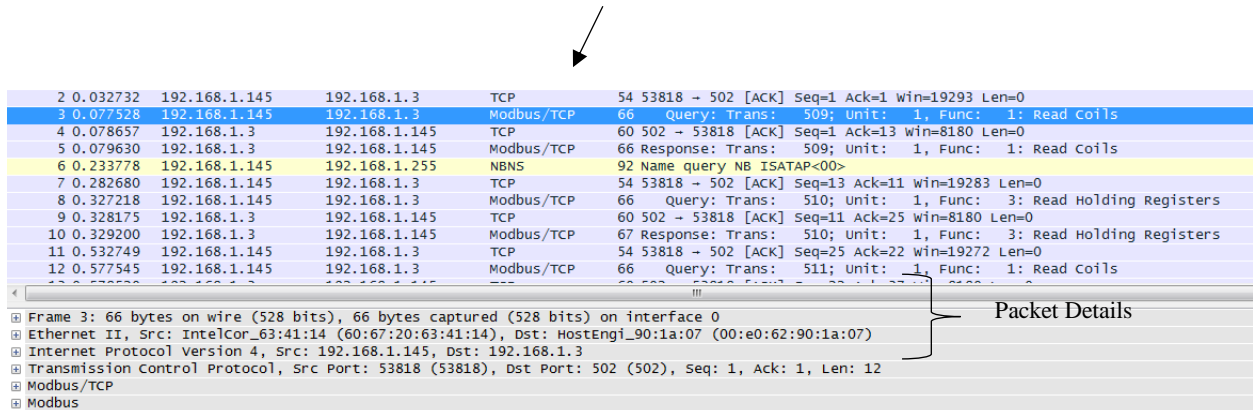


Fig. 5

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

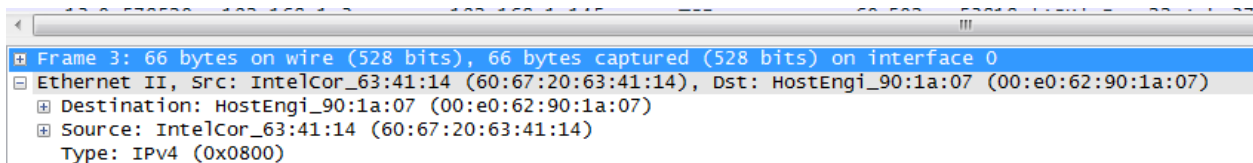


Fig. 6

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

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

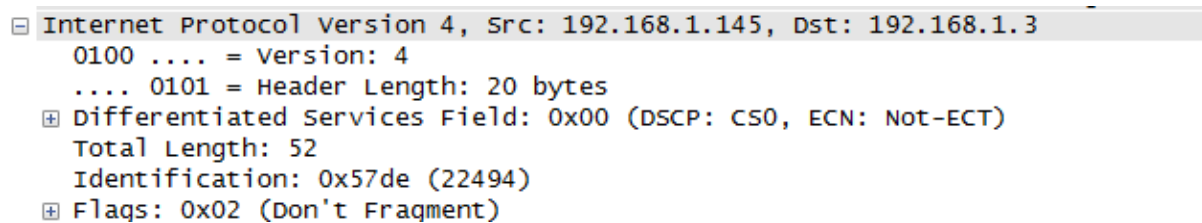


Fig. 7

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

- 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]
  [Data 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

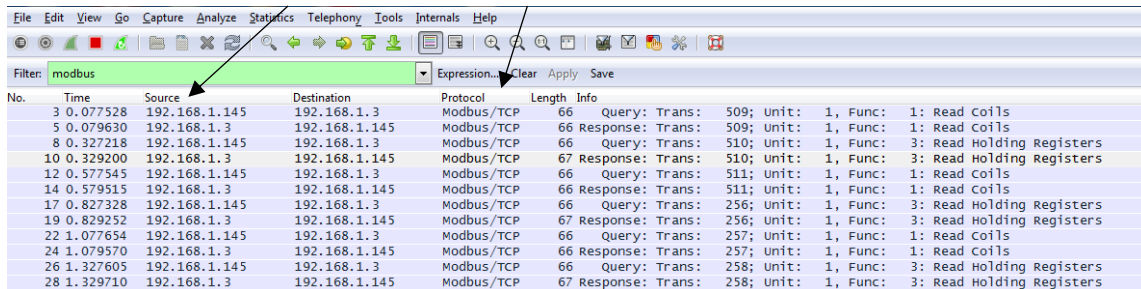
```

Fig. 9

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

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

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



No.	Time	Source	Destination	Protocol	Length	Info
3	0.077528	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 509; Unit: 1, Func: 1: Read Coils
5	0.079630	192.168.1.3	192.168.1.145	Modbus/TCP	66	Response: Trans: 509; Unit: 1, Func: 1: Read Coils
8	0.327218	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 510; Unit: 1, Func: 3: Read Holding Registers
10	0.329200	192.168.1.3	192.168.1.145	Modbus/TCP	67	Response: Trans: 510; Unit: 1, Func: 3: Read Holding Registers
12	0.577545	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 511; Unit: 1, Func: 1: Read Coils
14	0.579515	192.168.1.3	192.168.1.145	Modbus/TCP	66	Response: Trans: 511; Unit: 1, Func: 1: Read Coils
17	0.827328	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 256; Unit: 1, Func: 3: Read Holding Registers
19	0.829252	192.168.1.3	192.168.1.145	Modbus/TCP	67	Response: Trans: 256; Unit: 1, Func: 3: Read Holding Registers
22	1.077654	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 257; Unit: 1, Func: 1: Read Coils
24	1.079570	192.168.1.3	192.168.1.145	Modbus/TCP	66	Response: Trans: 257; Unit: 1, Func: 1: Read Coils
26	1.327605	192.168.1.145	192.168.1.3	Modbus/TCP	66	Query: Trans: 258; Unit: 1, Func: 3: Read Holding Registers
28	1.329710	192.168.1.3	192.168.1.145	Modbus/TCP	67	Response: Trans: 258; Unit: 1, Func: 3: Read Holding Registers

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

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

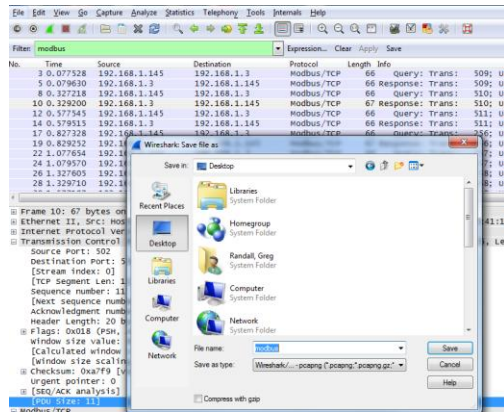


Fig. 11

References

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