

# Advance Course in Factory Communication

## Assignment 1 MODBUS TCP

**Environment Setup:** For this Assignment two laptops were used. First of all, the provided softwares were downloaded and installed, in one the master application and another the slave simulator. Wireshark was installed in the pc which was selected as a master client. Then it was made sure that the two laptops are working on the same network, in this case same wireless network. Also the IP addresses of both the PC were known. It was also made sure that both the PC can communicate with each other. Then the IP address of the slave PC was assigned in Modbus Master application. After the setup both the master and slave simulator was connected and Wireshark was kept on run mode to capture the packets.

1. Some arbitrary changes were made in the slave simulator, like changing the values of some certain coils, discrete inputs and holding registers. Then the result was read from the master application and all the results were matched according to the address of the certain coils, discrete inputs and holding registers. The screenshots from both the master application and the slave simulator are provided below.

Modbus Master

File Options Commands View Language Help

Modbus Mode: TCP Unit ID: 1 Scan Rate (ms): 1000

Function Code: Read Coils (0x01) Format: Decimal

Start Address: 0 Number of Coils: 7

1 0 0 0 1 0 0 x x x

TCP : 192.168.001.060:502 Packets : 2 Errors : 0

MODBUS Eth. TCP/IP PLC - Simulator (port: 502)

Connected (0/10) : (received/sent) (2/2) Serv. listening.

Address : Hex Dec I/O Coil Outputs (00C) Fmt: decimal Prot: MODBUS TCF Clone

Address	+15	+14	+13	+12	+11	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+0	Total
1-16	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	8800
17-32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
33-48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
49-64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
65-80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
81-96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
97-112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
113-128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
129-144	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
145-160	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
161-176	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
177-192	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
193-208	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
209-224	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
225-240	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
241-256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
257-272	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
273-288	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
289-304	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
305-320	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25  
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

T Comms

Capture 1.1 Modbus Master reading data of 7 coils from Slave simulator

The image shows two software windows. The top window is 'Modbus Master' and the bottom window is 'MODBUS Eth. TCP/IP PLC - Simulator (port: 502)'.

**Modbus Master Configuration:**

- Modbus Mode: TCP
- Unit ID: 1
- Scan Rate (ms): 1000
- Function Code: Read Discrete Inputs (0x02)
- Format: Hex
- Start Address: 0
- Number of Coils: 8

**Modbus Master Data:**

1	0	1	0	1	0	1	0	x	x
---	---	---	---	---	---	---	---	---	---

**MODBUS Eth. TCP/IP PLC - Simulator (port: 502) Configuration:**

- Connected (2/10) : (received/sent) (4/4) Serv. idle.
- Address: Hex
- I/O: Digital Inputs (100)
- Fmt: decimal
- Prot: MODBUS TCP/IP
- Clone: ☐

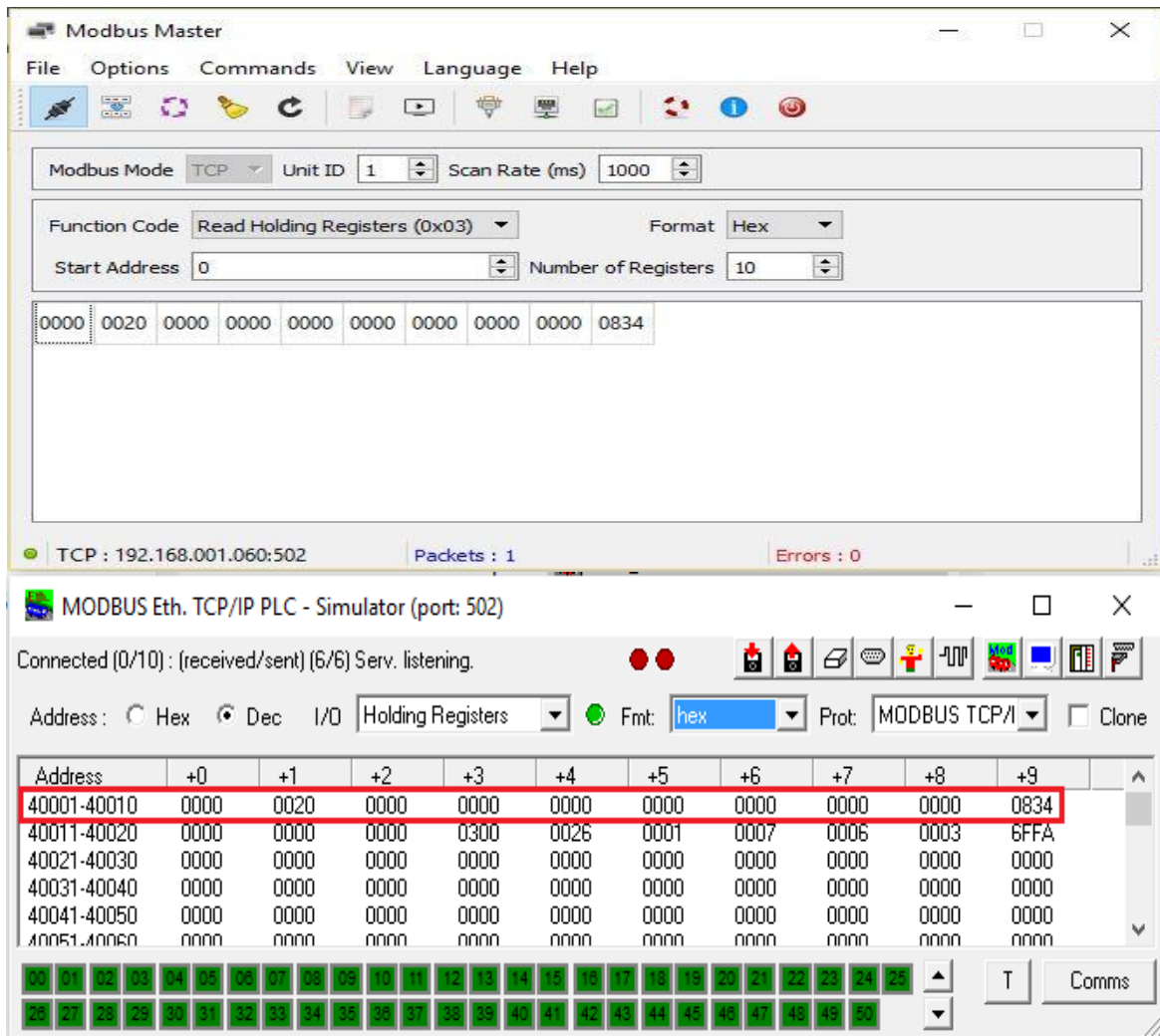
**MODBUS Eth. TCP/IP PLC - Simulator Data Table:**

Address	+15	+14	+13	+12	+11	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+0	Total
10001-10016	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	AA00
10017-10032	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10033-10048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10049-10064	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10065-10080	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10081-10096	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10097-10112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10113-10128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10129-10144	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10145-10160	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10161-10176	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10177-10192	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10193-10208	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10209-10224	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10225-10240	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10241-10256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10257-10272	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10273-10288	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10289-10304	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10305-10320	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10321-10336	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10337-10352	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

**MODBUS Eth. TCP/IP PLC - Simulator Data Table (Hex):**

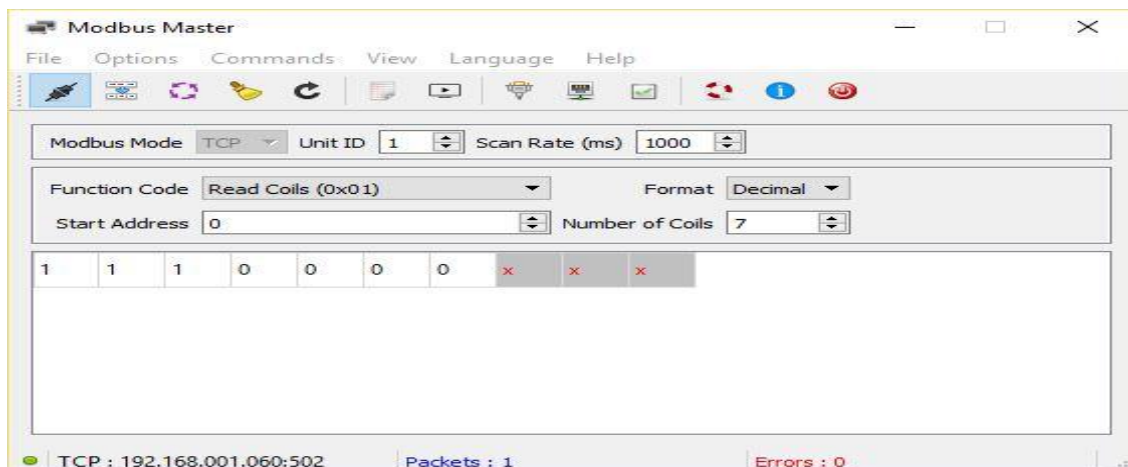
00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11
12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23
24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35
36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47
48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59

**Capture 1.2 Modbus Master reading 8 Digital inputs from server simulator**



Capture 1.3 Modbus Master reading status of 10 Holding Registers from server simulator

- 4.a Reading 7 coils from bit 0 and reading 4 coils from bit 1:



The image shows two windows. The top window is the 'MODBUS Eth. TCP/IP PLC - Simulator (port: 502)'. It displays a table of coil outputs. The bottom window is Wireshark, showing packet 82, which is a Modbus/TCP Read Coils request. The request details show a function code of 01 (Read Coils), a byte count of 1, and data representing 7 coils (00000001).

Address	+15	+14	+13	+12	+11	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+0	Total
1-16	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	E000
17-32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
33-48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
49-64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
65-80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
81-96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
97-112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
113-128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

Wireshark Packet 82 details:

- Frame 82: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
- Ethernet II, Src: LiteonTe\_6d:85:7b (ac:e0:10:6d:85:7b), Dst: LiteonTe\_c5:b6:d8 (ac:e0:10:c5:b6:d8)
- Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.57
- Transmission Control Protocol, Src Port: 502 (502), Dst Port: 49987 (49987), Seq: 1, Ack: 13, Len: 10
- Modbus/TCP
- Modbus
  - Function Code: Read Coils (1)
  - [Request Frame: 81]
  - Byte Count: 1
  - Data: 07

**Capture 4. a1: Modbus master request for 7 coils from 0 bit, slave and wireshark response packet**

Message Analysis:

- Function code matches the request by Modbus Master
- Byte count is 1 which is correct for 7 coils.
- Data is 7 bit for 7 coils.
- Source and destination of message is also ok
- Total frame size is 64 bytes

The image shows the 'Modbus Master' application window. It is configured for a 'Read Coils (0x01)' operation. The start address is 1, and the number of coils is 4. The status bar shows 'Packets : 2' and 'Errors : 0'.

Modbus Master Configuration:

- Modbus Mode: TCP
- Unit ID: 1
- Scan Rate (ms): 1000
- Function Code: Read Coils (0x01)
- Format: Decimal
- Start Address: 1
- Number of Coils: 4

Coil Status (0 to 15):

0	0	1	0	x	x	x	x	x
---	---	---	---	---	---	---	---	---

MODBUS Eth. TCP/IP PLC - Simulator (port: 502)

Connected (1/10) : (received/sent) (8/8) Serv. idle.

Address : ☐ Hex ☒ Dec I/O ☐ Coil Outputs ☐ (00C) Fmt: decimal Prot: MODBUS TCF

Address	+15	+14	+13	+12	+11	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+0	Total
1-16	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1000
17-32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
33-48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
49-64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
65-80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
81-96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
97-112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
113-128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

Wireshark · Packet 265 · wireshark\_pcapng\_AB6B5B5E-EF1C-486E-AF88-7F711D57AA02\_20160406222720\_a06028

> Frame 265: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

> Ethernet II, Src: LiteonTe\_6d:85:7b (ac:e0:10:6d:85:7b), Dst: LiteonTe\_c5:b6:d8 (ac:e0:10:c5:b6:d8)

> Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.57

> Transmission Control Protocol, Src Port: 502 (502), Dst Port: 50072 (50072), Seq: 1, Ack: 13, Len: 10

> Modbus/TCP

Modbus

Function Code: Read Coils (1)

[Request Frame: 264]

Byte Count: 1

Data: 04

No.: 265 · Time: 16.387930 · Source: 192.168.1.60 · Destination: 192.168.1.57 · Protocol: Modbus/TCP · Length: 64 · Info: Response: Trans: 1; Unit: 1, Func: 1: Read Coils

Close Help

**Capture 4. a2: Modbus Master request to read 4 coils from bit 1 & Wireshark response packet for reading 4 coils starting from bit 1.**

Message Analysis:

- Function code matches the request by Modbus Master
  - Byte count is 1 which is correct for 4 coils.
  - Data is 4 bit for 4 coils.
  - Source and destination of message is also ok.
  - Total frame size is 64 bytes.
- **4.b Reading 4 discrete inputs starting from bit 5 & reading 11 bits starting from bit 2**

Modbus Master

File Options Commands View Language Help

Modbus Mode TCP Unit ID 1 Scan Rate (ms) 1000

Function Code Read Discrete Inputs (0x02) Format Decimal

Start Address 5 Number of Coils 4

1 1 1 1

TCP : 192.168.001.060:502 Packets : 5 Errors : 0

The image shows two overlapping windows. The top window is 'MODBUS Eth. TCP/IP PLC - Simulator (port: 502)'. It displays a table of digital inputs. A red box highlights the values for addresses 10001-10016, specifically the bits for addresses 10001, 10002, 10003, and 10004, which are all set to 1.

Address	+15	+14	+13	+12	+11	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+0	Total
10001-10016	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0780
10017-10032	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10033-10048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10049-10064	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10065-10080	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10081-10096	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10097-10112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

The bottom window is 'Wireshark - Packet 1416'. It shows the details of a Modbus/TCP packet. The packet is a response from the PLC to a request for reading discrete inputs. The function code is 02 (Read Discrete Inputs), the byte count is 1, and the data is 0f (15 bits).

Frame 1416: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0  
> Ethernet II, Src: LiteonTe\_6d:85:7b (ac:e0:10:6d:85:7b), Dst: LiteonTe\_c5:b6:d8 (ac:e0:10:c5:b6:d8)  
> Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.57  
> Transmission Control Protocol, Src Port: 502 (502), Dst Port: 50159 (50159), Seq: 1, Ack: 13, Len: 10  
> Modbus/TCP  
Modbus  
Function Code: Read Discrete Inputs (2)  
[Request Frame: 1415]  
Byte Count: 1  
Data: 0f  
No.: 1416 · Time: 477.665919 · Source: 192.168.1.60 · Destination: 192.168.1.57 · Protocol: Modbus/TCP · Length: 64 · Info: Response: Trans: 1; Unit: 1; Func: 2; Read Discrete Inputs

Capture 4. B1: Wireshark response packet for reading 4 digital input starting from bit 5.

#### Message Analysis:

- Function code matches the request by Modbus Master.
- Byte count is 1 which is correct for 4 coils.
- Data is 4 bit for 4 coils.
- Source and destination of message is also ok.
- Total frame size is 64 bytes.

The image shows the 'Modbus Master' software interface. The 'Modbus Mode' is set to 'TCP'. The 'Unit ID' is 1, and the 'Scan Rate (ms)' is 1000. The 'Function Code' is 'Read Discrete Inputs (0x02)'. The 'Format' is 'Decimal'. The 'Start Address' is 2, and the 'Number of Coils' is 11. The interface displays a table of digital inputs. The first row shows the status of the inputs, with the first four bits (addresses 10001, 10002, 10003, 10004) set to 1, and the remaining bits set to 0.

Address	10001	10002	10003	10004	10005	10006	10007	10008	10009	10010	10011	10012	10013	10014	10015	10016
10001	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10002	0	0	1	x	x	x	x	x	x	x	x	x	x	x	x	x

TCP : 192.168.001.060:502      Packets : 2      Errors : 0



The image shows two windows. The top window is 'MODBUS Eth. TCP/IP PLC - Simulator (port: 502)'. It displays a table of digital inputs. The bottom window is 'Wireshark - Packet 2045', showing a Modbus/TCP packet details.

**MODBUS Eth. TCP/IP PLC - Simulator (port: 502)**

Connected (0/10) : (received/sent) (15/15) Serv. listening.

Address : ☐ Hex ☒ Dec I/O  (100) Fmt:  Prot:  ☐ Clone

Address	+15	+14	+13	+12	+11	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+0	Total
10001-10016	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	2008
10017-10032	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10033-10048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10049-10064	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10065-10080	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10081-10096	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
10097-10112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

**Wireshark - Packet 2045** · wireshark\_pcapng\_AB6B5B5E-EF1C-486E-AF88-7F711D57AA02\_20160406224953\_a08400

> Frame 2045: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0

> Ethernet II, Src: LiteonTe\_6d:85:7b (ac:e0:10:6d:85:7b), Dst: LiteonTe\_c5:b6:d8 (ac:e0:10:c5:b6:d8)

> Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.57

> Transmission Control Protocol, Src Port: 502 (502), Dst Port: 50170 (50170), Seq: 1, Ack: 13, Len: 11

> Modbus/TCP

Modbus

Function Code: Read Discrete Inputs (2)

[Request Frame: 2044]

Byte Count: 2

Data: 0000

No.: 2045 · Time: 735.480108 · Source: 192.168.1.60 · Destination: 192.168.1.57 · Protocol: .../TCP · Length: 68 · Info: Response: Trans: 1; Unit: 1, Func: 2: Read Discrete Inputs

Close Help

**Capture 4. B2: Wireshark response packet for reading 11 digital inputs starting from bit 2.**

Message Analysis:

- Function code matches the request by Modbus Master.
- Byte count is 2 which is correct for 11 coils.
- Data is 0 as all the states of the inputs are 0.
- Source and destination of message is also ok.
- Total frame size is 68 bytes.

#### • 4.c Reading 2<sup>nd</sup> Holding Register

The image shows the 'Modbus Master' software interface. It includes a menu bar (File, Options, Commands, View, Language, Help) and a toolbar. The main configuration area shows 'Modbus Mode' set to 'TCP', 'Unit ID' set to '1', and 'Scan Rate (ms)' set to '1000'. The 'Function Code' is set to 'Read Holding Registers (0x03)', 'Format' is 'Decimal', 'Start Address' is '1', and 'Number of Registers' is '1'. A status bar at the bottom shows '32'.

**Modbus Master**

File Options Commands View Language Help

Modbus Mode  Unit ID  Scan Rate (ms)

Function Code  Format

Start Address  Number of Registers

32

The image shows two windows. The top window is 'MODBUS Eth. TCP/IP PLC - Simulator (port: 502)'. It displays a table of holding registers. The register at address +1 is highlighted with a red box and contains the value 32.

Address	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
40001-40010	0	32	0	0	0	0	0	0	0	2100
40011-40020	0	0	0	732	54	55	0	5	2	12296
40021-40030	0	0	0	0	0	0	0	0	0	0
40031-40040	0	0	0	0	0	0	0	0	0	0
40041-40050	0	0	0	0	0	0	0	0	0	0
40051-40060	0	0	0	0	0	0	0	0	0	0
40061-40070	0	0	0	0	0	0	0	0	0	0

The bottom window is 'Wireshark - Packet 3691'. It shows the details of a Modbus/TCP packet. The packet is a 'Read Holding Registers' request. The function code is 3, the request frame is 3690, the byte count is 2, and the register address is 1 (UINT16). The value 32 is shown in the 'Register 1 (UINT16)' field.

Frame 3691: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0  
Ethernet II, Src: LiteonTe\_6d:85:7b (ac:e0:10:6d:85:7b), Dst: LiteonTe\_c5:b6:d8 (ac:e0:10:c5:b6:d8)  
Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.57  
Transmission Control Protocol, Src Port: 502 (502), Dst Port: 50202 (50202), Seq: 1, Ack: 13, Len: 11  
Modbus/TCP  
Modbus  
Function Code: Read Holding Registers (3)  
[Request Frame: 3690]  
Byte Count: 2  
Register 1 (UINT16): 32

**Capture 4. c: Modbus master request for reading 2<sup>nd</sup> Holding Register and wireshark response packet**

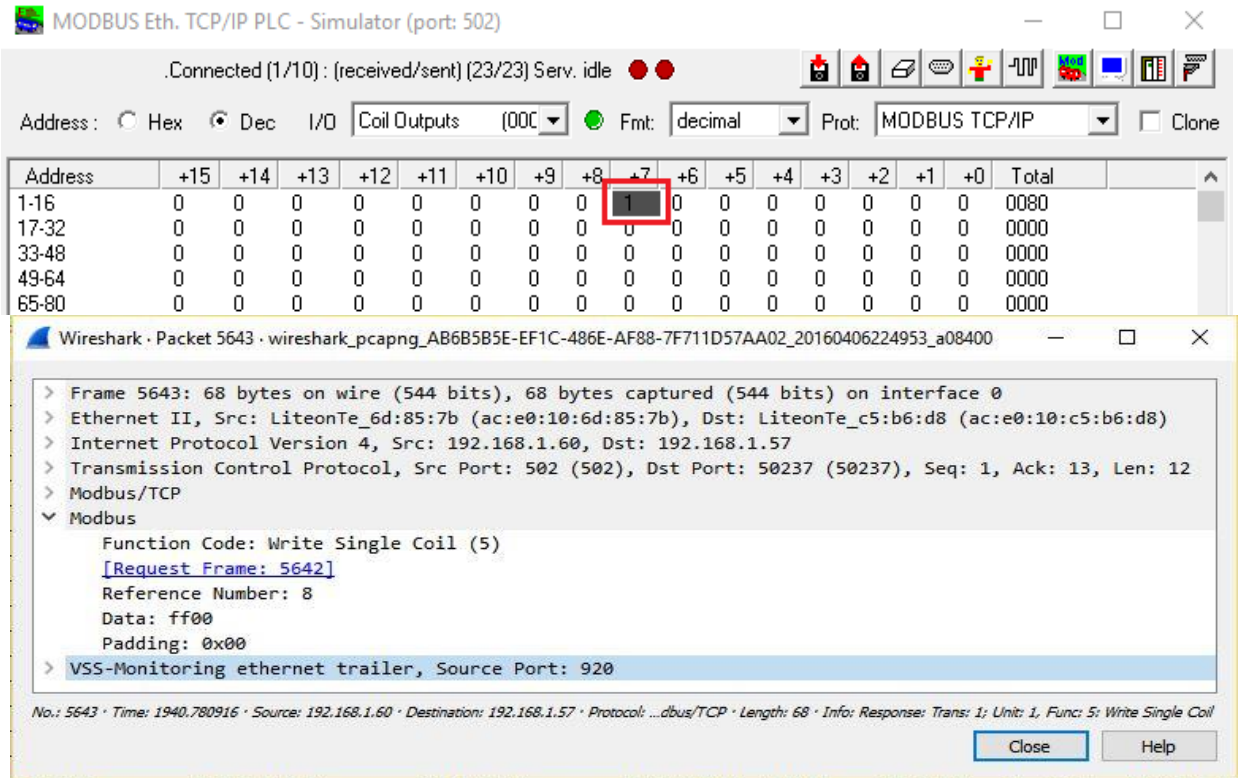
#### Message Analysis:

- Function code matches the request by Modbus Master.
- Byte count is 2 which is correct for a holding register which consumes 16 bit.
- Data is 32.
- Source and destination of message is also ok.
- Total frame size is 68 bytes.

#### 4.d Writing the 9<sup>th</sup> Coil value to True

The image shows the 'Modbus Master' software interface. The 'Modbus Mode' is set to 'TCP', 'Unit ID' is 1, and 'Scan Rate (ms)' is 1000. The 'Function Code' is 'Write Single Coil (0x05)', 'Format' is 'Hex', 'Start Address' is 8, and 'Number of Coils' is 1. The 'FF00' button is highlighted.





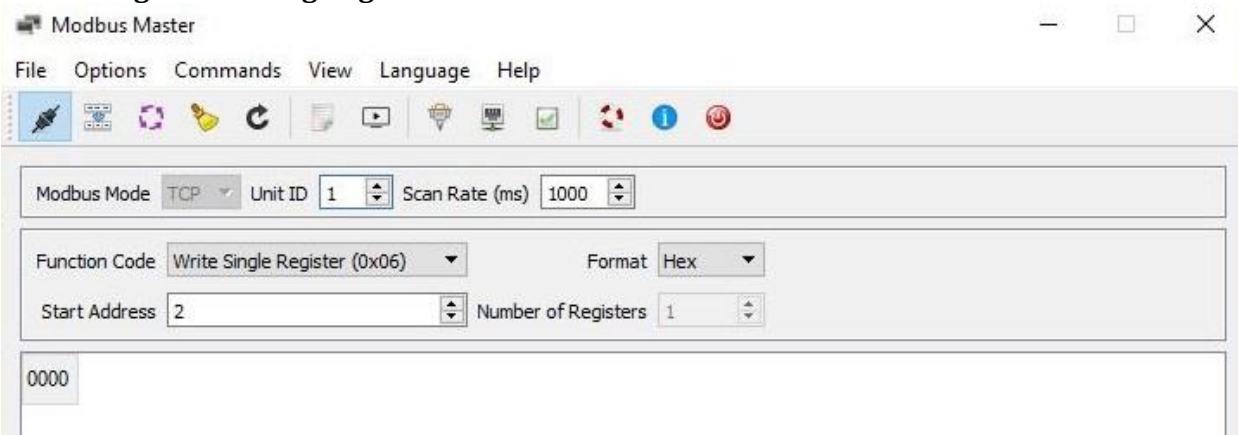
**Capture 4. d: Modbus master request for setting the 9<sup>th</sup> coil to true and wireshark response packet**

Message Analysis:

- Function code matches the request by Modbus Master.
- Reference Number is 8 as the 9<sup>th</sup> coil is set to true.
- Data is FF00 which is used for setting true value of coils.
- Source and destination of message is also ok.
- Total frame size is 68 bytes.

All the experiments tested for the 5 functions codes were observed and they matched with the Master application according to the changes made in the Slave simulator.

#### 4.c Writing 3rd Holding Register to 0



MODBUS Eth. TCP/IP PLC - Simulator (port: 502)

.Connected [0/10] : (received/sent) [31/31] Serv. listening

Address: ☐ Hex ☒ Dec I/O: Holding Registers Fmt: decimal Prot: MODBUS TCP/IP

Address	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
40001-40010	0	32	0	0	0	0	0	0	0	2100
40011-40020	0	0	0	412	40	48	1	5	2	29754
40021-40030	0	0	0	0	0	0	0	0	0	0
40031-40040	0	0	0	0	0	0	0	0	0	0
40041-40050	0	0	0	0	0	0	0	0	0	0

Wireshark · Packet 7280 · wireshark\_pcapng\_AB6B5B5E-EF1C-486E-AF88-7F711D57AA02\_20160406224953\_a08400

> Frame 7280: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0  
> Ethernet II, Src: LiteonTe\_6d:85:7b (ac:e0:10:6d:85:7b), Dst: LiteonTe\_c5:b6:d8 (ac:e0:10:c5:b6:d8)  
> Internet Protocol Version 4, Src: 192.168.1.60, Dst: 192.168.1.57  
> Transmission Control Protocol, Src Port: 502 (502), Dst Port: 50275 (50275), Seq: 1, Ack: 13, Len: 12  
> Modbus/TCP  
    Modbus  
        Function Code: Write Single Register (6)  
        [Request Frame: 7279]  
        Reference Number: 2  
        Data: 0000  
> VSS-Monitoring ethernet trailer, Source Port: 845

No.: 7280 · Time: 2672.109173 · Source: 192.168.1.60 · Destination: 192.168.1.57 · Protocol: Modbus/TCP · Length: 68 · Info: Responder Trans: 1; Unit: 1; Func: 6; Write Single Register

Close Help

**Capture 4. e: Modbus master request for setting the 3rd Holding Register to 0 and wireshark response packet**

**Message Analysis:**

- Function code matches the request by Modbus Master.
- Reference Number is 2 as the 3rd coil is set to 0.
- Data is 0000 which is used for setting the holding register to 0.
- Source and destination of message is also ok.
- Total frame size is 68 bytes.

**Analyzing protocol level from Wireshark packet:**

Wireshark · Packet 2044 · wireshark\_pcapng\_AB6B5B5E-EF1C-486E-AF88-7F711D57AA02\_20160406224953\_a08400

Frame 2044: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Interface id: 0 (\Device\NPF\_{AB6B5B5E-EF1C-486E-AF88-7F711D57AA02})  
Encapsulation type: Ethernet (1)  
Arrival Time: Apr 6, 2016 23:02:10.062318000 FLE Daylight Time  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1459972930.062318000 seconds  
[Time delta from previous captured frame: 0.788447000 seconds]  
[Time delta from previous displayed frame: 257.772802000 seconds]  
[Time since reference or first frame: 735.438721000 seconds]  
Frame Number: 2044  
Frame Length: 66 bytes (528 bits)  
Capture Length: 66 bytes (528 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:mbtcp:modbus]  
[Coloring Rule Name: TCP]  
[Coloring Rule String: tcp]

In this level the data that are encoded are:

- Transmission time for receiving this packet from slave to master.
- Frame size
- Frame Number
- Frame protocol: Ethernet

```
▼ Ethernet II, Src: LiteonTe_c5:b6:d8 (ac:e0:10:c5:b6:d8), Dst: LiteonTe_6d:85:7b (ac:e0:10:6d:85:7b)
  ▼ Destination: LiteonTe_6d:85:7b (ac:e0:10:6d:85:7b)
    Address: LiteonTe_6d:85:7b (ac:e0:10:6d:85:7b)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  ▼ Source: LiteonTe_c5:b6:d8 (ac:e0:10:c5:b6:d8)
    Address: LiteonTe_c5:b6:d8 (ac:e0:10:c5:b6:d8)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

- Destination and source address

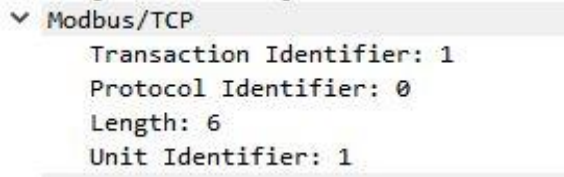
```
▼ Internet Protocol Version 4, Src: 192.168.1.57, Dst: 192.168.1.60
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x2416 (9238)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  > Header checksum: 0x52e8 [validation disabled]
    Source: 192.168.1.57
    Destination: 192.168.1.60
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

- IP Addresses of source and destination
- CRC
- Flags

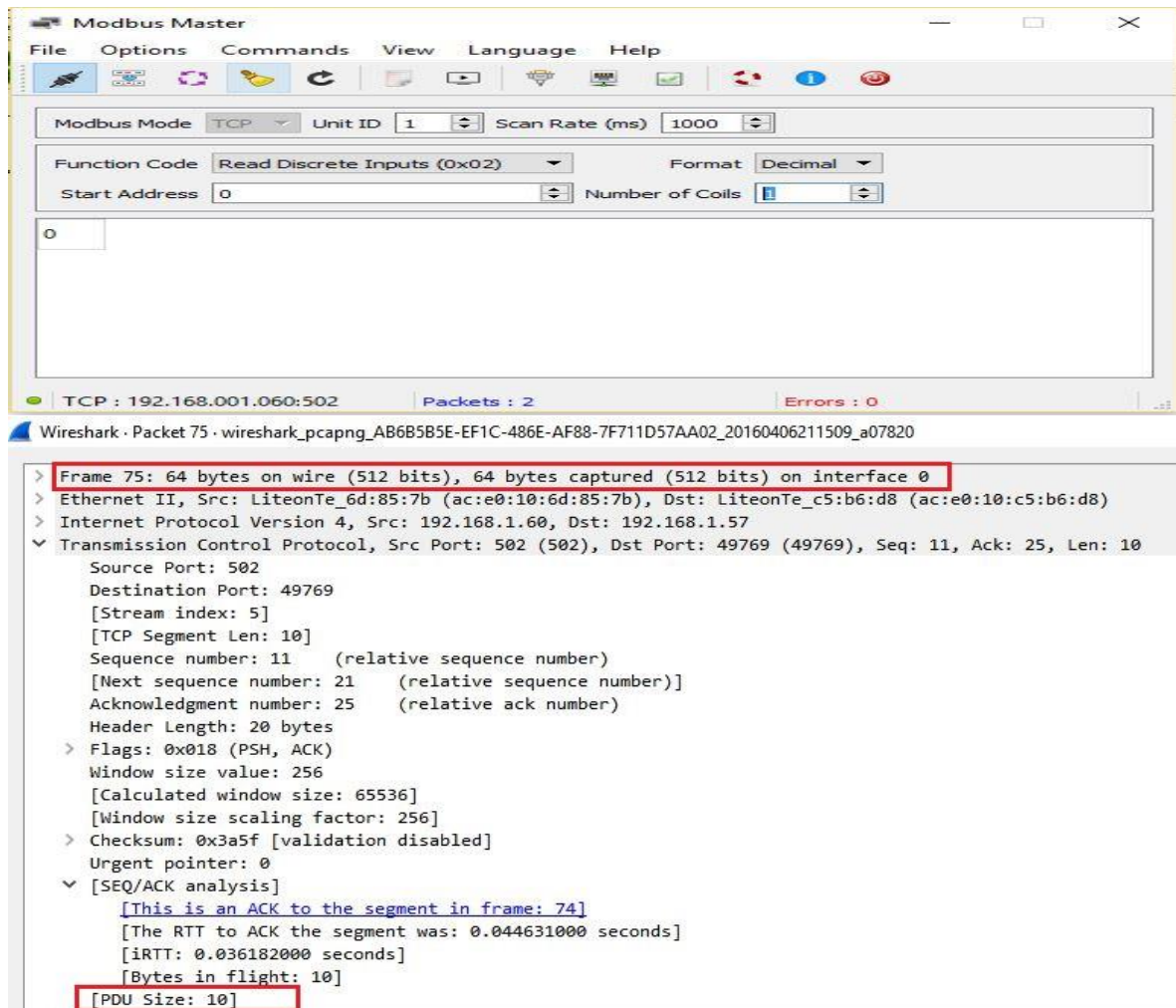
```
▼ Transmission Control Protocol, Src Port: 50170 (50170), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
  Source Port: 50170
  Destination Port: 502
  [Stream index: 44]
  [TCP Segment Len: 12]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 13 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x018 (PSH, ACK)
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
  > Checksum: 0x4f54 [validation disabled]
    Urgent pointer: 0
  ▼ [SEQ/ACK analysis]
    [iRTT: 0.032925000 seconds]
    [Bytes in flight: 12]
    [PDU Size: 12]
```

- Source port & destination port

- Acknowledgement No.
- Flags
- Checksum
- PDU Size



- MBAP Header description.
- Protocol Identifier 0 = Modbus Protocol.
- Communication Overhead for reading one discrete input:



**Capture 4: Reading one discrete input request by Modbus Master & Wireshark response packet analysis**



From the Wireshark message, it is shown that the data frame size is 64 bytes and the PDU size is 10 bytes.

So, the overhead for reading one discrete input is  $(64-10) = 54$  Bytes.

- **Function Code 0\*04: Read Input Register**

It is a Public Function code. Using this Function code, the master client can read the value of the input registers from the slave. It uses 16 bits to store a value. Its starting address can be 0\*0000 to 0\*FFFF. And the quantity of input registers can be 0\*0001 to 0\*007D.

Request & Response PDU:

Request PDU:

- Function Code 1 Byte = 0\*04
- Starting Address = 2 Bytes [0\*0000 to 0\*FFFF]
- Quantity of Input Registers = 2 Bytes [\*0001 to 0\*007D]

Response PDU:

- Function Code 1 Byte = 0\*04
- Byte Count = 1 Byte [2\*Number of Registers]
- Input Registers = Number of Registers \*2 Bytes

- **Transmission Time for 10 Mbps:**

From Wireshark packet the average request data frame got was 64 Bytes and response data frame was 66 bytes. So for this amount of data the transmission time would be

$$\begin{aligned} (66+64) * 8 \text{ Bits} / 10 \text{ Mbps} &= 0.000104 \text{ s} \\ &= 104 \mu\text{s} \end{aligned}$$

- The average transmission time was 0.04138700 seconds.

From Wireshark message for Modbus TCP/IP the transmission time can be found.

```
▼ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 2044]
  [The RTT to ACK the segment was: 0.041387000 seconds]
  [iRTT: 0.032925000 seconds]
  [Bytes in flight: 11]
  [PDU Size: 11]
```