MODBUS MASTER SIMULATOR

USER GUIDE

Version *<1.1>*

<05/14/2020>

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.1	*Digital Reach Pvt. Ltd.*	*07/14/2020*	*Remaining*	*<mm/dd/yy>*	More features were added

UP Template Version: 12/31/07

TABLE OF CONTENTS

LIST OF FIGURES

1 SOFTWARE DESCRIPTION

1.1 ABOUT MODBUS SLAVE SIMULATOR

Modbus Master Simulator is a software designed to simulate Modbus protocol to test slave device.

1.2 SYSTEM REQUIREMENTS

HARDWARE REQUIRENTS	• 1 Ghz. or faster processor • 512 MB Ram • 2 MB of storage • 800 x 600 display resolution
SOFTWARE REQUIREMENTS	• Runs on Windows platform only. Any windows version: Windows 7/8/8.1/10.

1.3 END-USER LICENSE AGREEMENTS

Visit website https://www.digireach.com/ for License agreement.

2 SOFTWARE INSTALLATION

2.1 INSTALLATION PROCEDURE

1. Download .rar file from website https://www.digireach.com/ under Product Menu.
2. Unzip and run setup.exe.

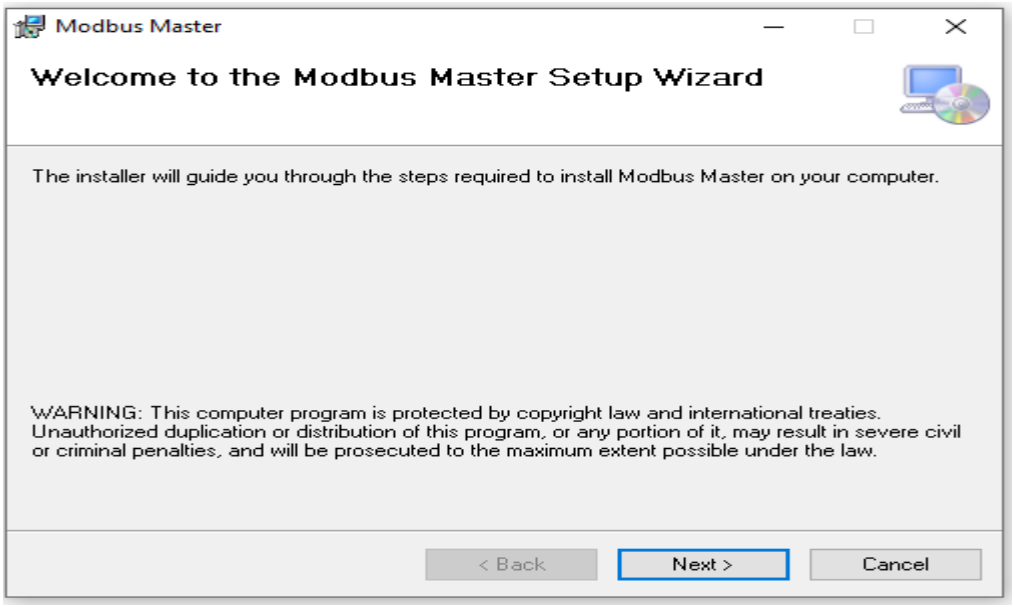

Figure 1 Installation window on running setup.exe

3. Choose destination to install software.

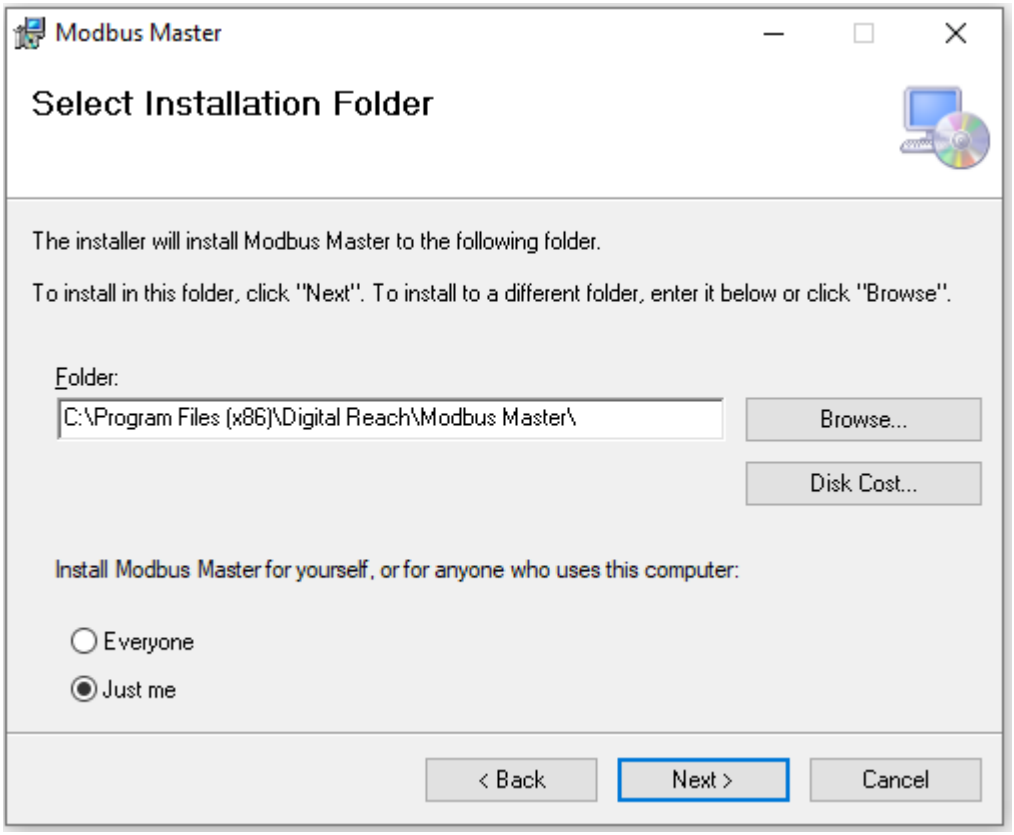

Figure 2 Path selection window where you want to install software

4. Click Next and Close to complete the installation.

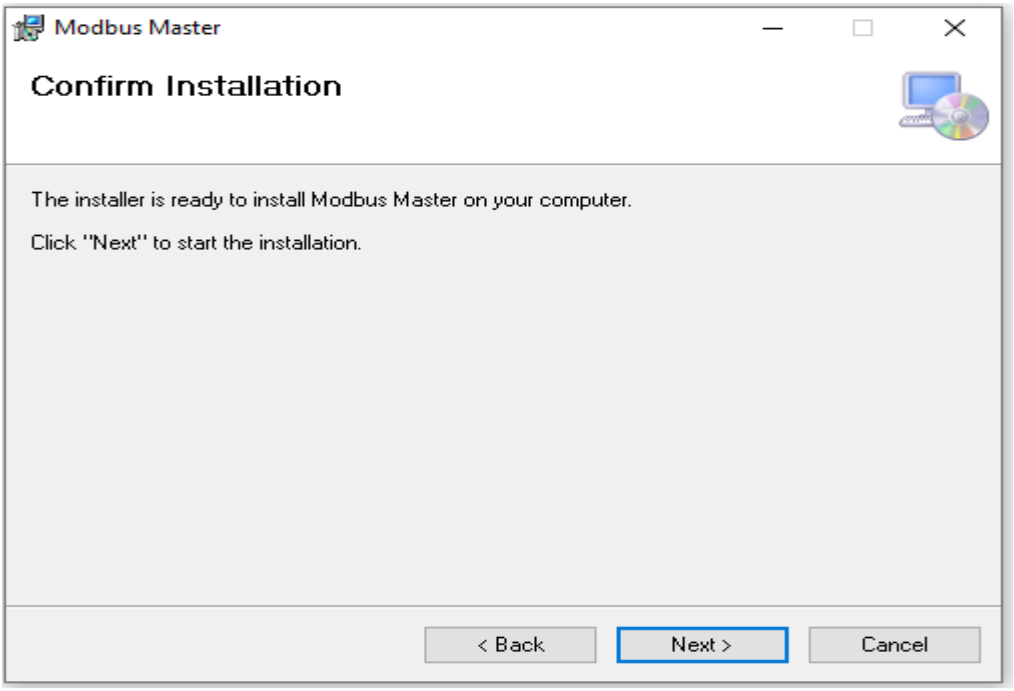

Figure 3 Click Next to install software

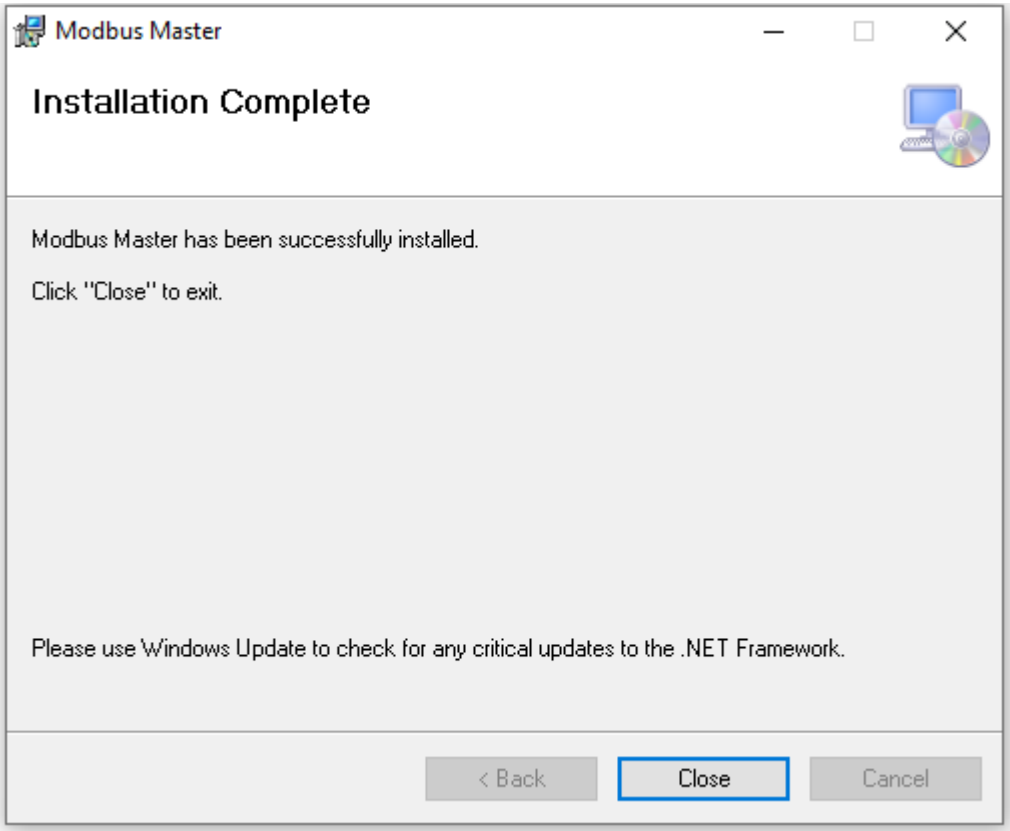

Figure 4 Close to finish installation

2.2 ACTIVATING LICENSE

Software once installed will ask for activation on opening for first time.

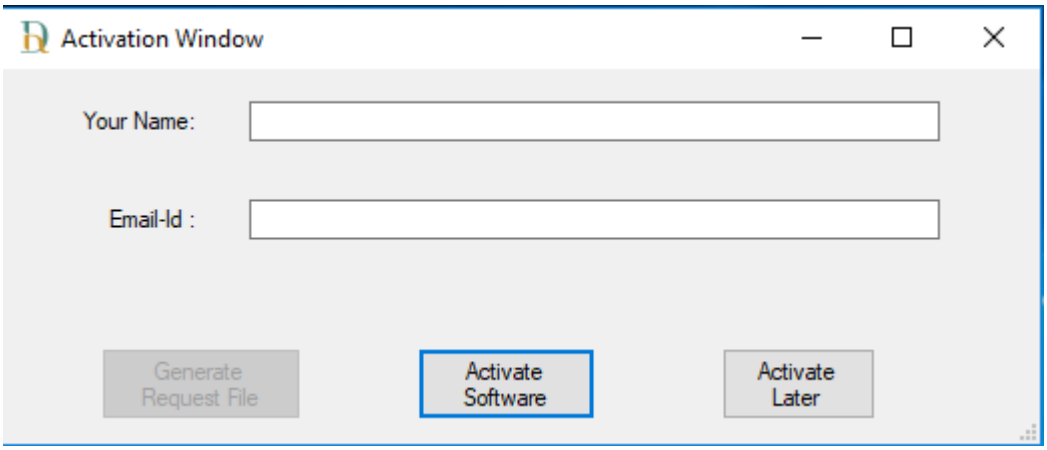

Figure 5 Software Activation Window opened at first time.

Here, if user choose to “Activate Later” it will run for a trial period of 30 days for 10 minutes each time an instance of the software is opened. This can be found in the help window about trial period showing unregistered.

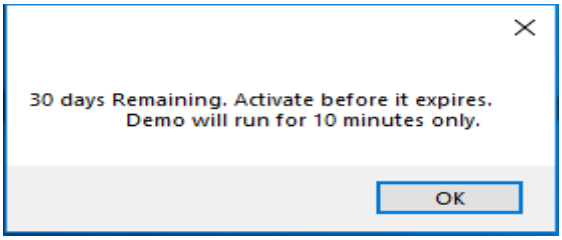

Figure 6 Showing Trial Period

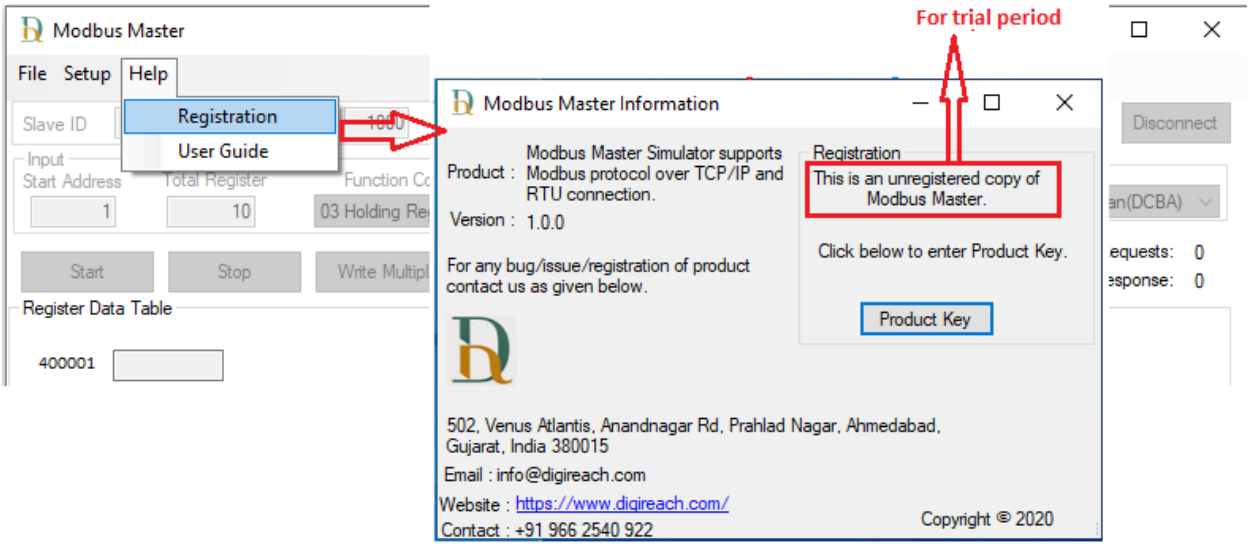

Figure 7 Software information when running in trial mode

If user want to activate software then user need to buy the software and follow below given steps to activate it.

1. If user is in same window as shown in Fig. 5 then fill details. Else click on help button then again click on “Product Key” button to open same window, after that fill details and click on “Generate Request File”. On clicking this button will open File Explorer, save the request file(.req) and mail that request file at provided email address(mail id is given in software information window).

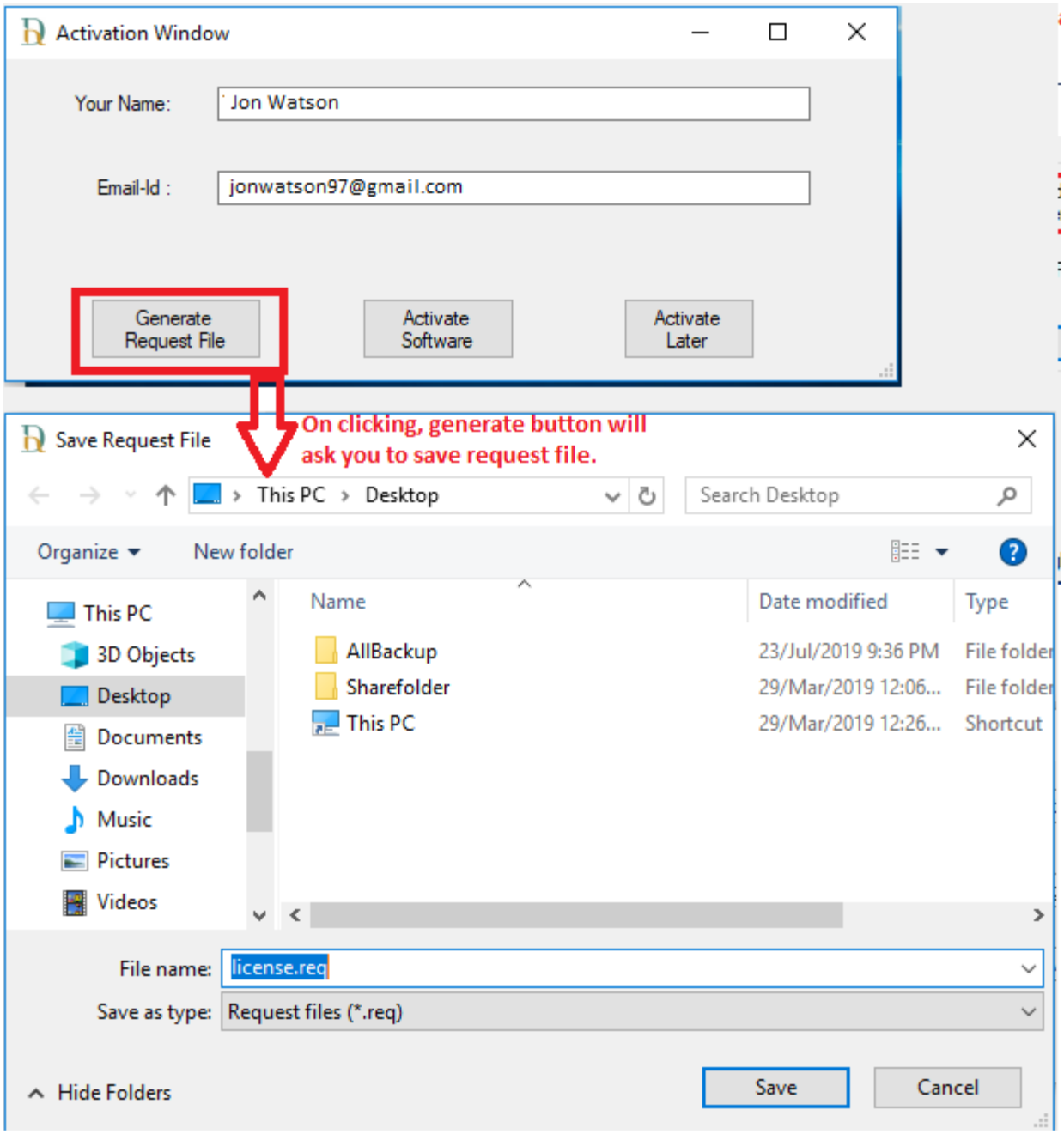

Figure 8 Save request file to send for license activation

2. After user have mailed request file, the company person will revert back with software activation(.act) file. On clicking “Activate Software” a File Explorer will open and here user have to select path of activation file(.act) where user had downloaded.

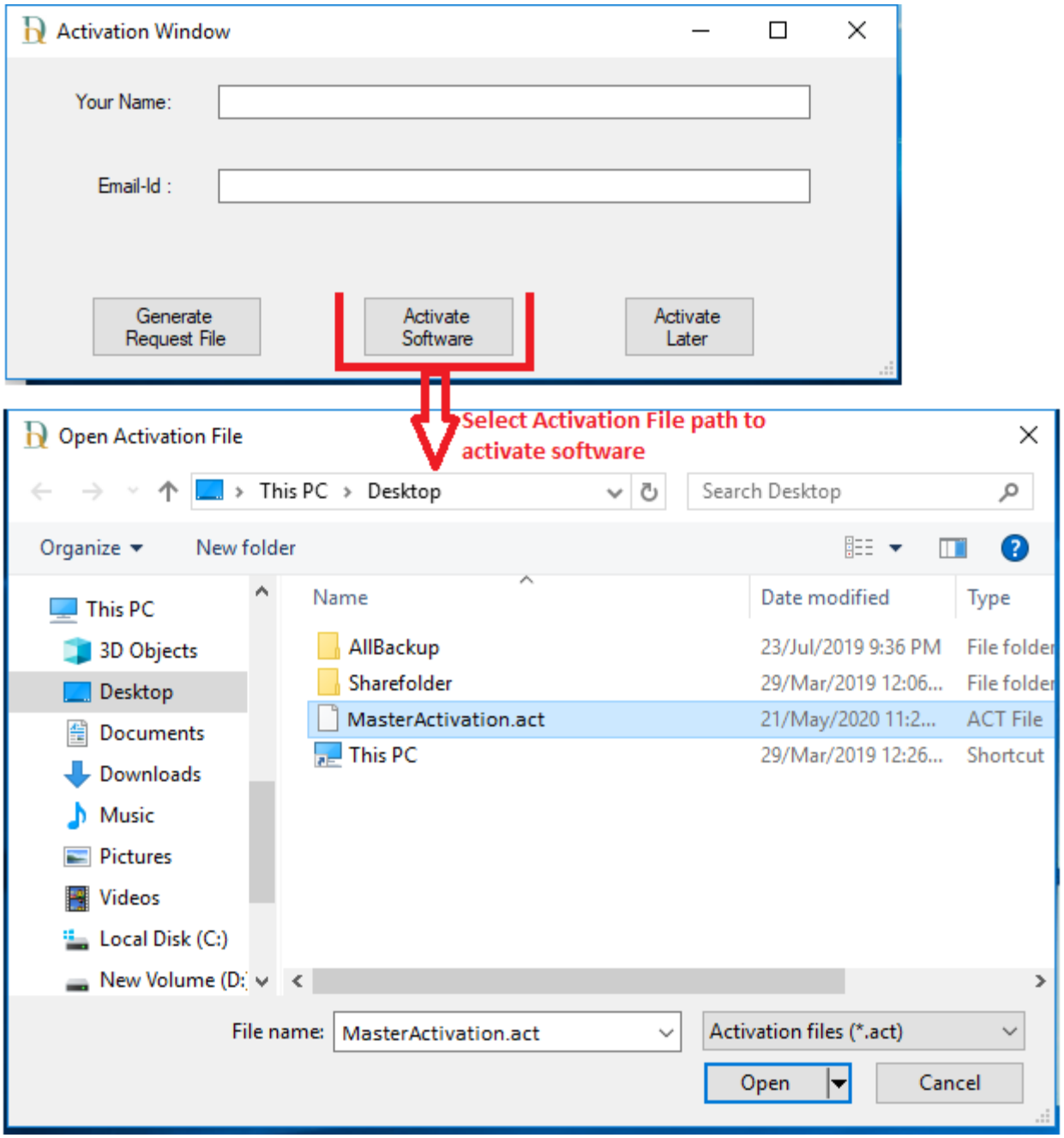

Figure 9 Selecting activation file provided by administrator to activate software

3. On successful activation message will be shown as below. User can also see in software information by clicking Help Menu -> Registration.

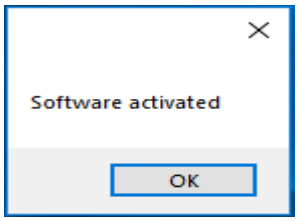

Figure 10 Software Activated pop-up

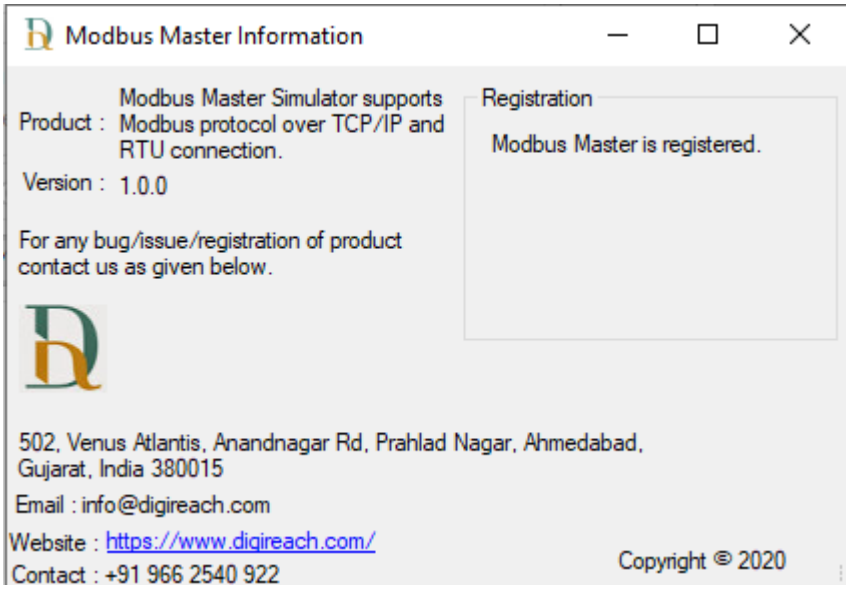

Figure 11 Software activation registration details

3 FEATURES

3.1 CONNECTION SUPPORTED

- Modbus TCP/IP
- Modbus RTU

3.2 FUNCTION CODE SUPPORTED

Function Codes in Decimal Format	Function Codes in Hexadecimal Format	Description / Usage
01	0x01	Read Coil Status
02	0x02	Read Input Status
03	0x03	Read Holding Registers
04	0x04	Read Input Registers
05	0x05	Write / Force Single Coil
06	0x06	Write / Force Single Register
15	0x0F	Write / Force Multiple Coil
16	0x10	Write / Force Multiple Register

3.3 DISPLAY FORMAT

FORMAT	BIG-ENDIAN	LITTLE-ENDIAN	MID-BIG ENDIAN	MID-LITTLE ENDIAN
Hexadecimal	✓	×	×	×
Binary	✓	×	×	×
Signed Integer-16 bit	✓	✓	×	×
Unsigned Integer-16 bit	✓	✓	×	×
Signed Integer-32 bit	✓	✓	✓	✓
Unsigned Integer-32 bit	✓	✓	✓	✓
Float-32 bit	✓	✓	✓	✓

3.4 ADDITIONAL FEATURES

- Slave Response(receive) and poll(request) delay can be set manually. Some baud rates requires different receive delays which software automatically assigns.
- Communication Log for connection status, data transmission(send/receive).
- Data Logging in csv format.

4 MODBUS MESSAGE DEFINITION

4.1 TCP MESSAGE FRAME

Modbus TCP message format is shown as below which contains Modbus Application Protocol Header(6 bytes), unit identifier(slave id), function code and data for request/response through TCP/IP connection.

MBAP Header (6 bytes)	Unit Identifier (1 byte)	Function Code (1 Byte)	Data (As per required)

MBAP Header consist of following parts :-

Fields	Length	Description	Master/Client	Slave/Server
Transaction Identifier	2 Bytes	Identification of a MODBUS Request/Response transaction.	Initialized by the client	Recopied by the server from the received request
Protocol Identifier	2 Bytes	0 = MODBUS protocol	Initialized by the client	Recopied by the server from the received request
Length	2 Bytes	Number of following bytes	Initialized by the client (request)	Initialized by the server (Response)

- Registers / Coils Size:

  Since modbus message size is 256 bytes below are the total number of coils/registers that can be read/write:-

  - For Coils/Discrete Input :- Maximum 2000 coils/discrete input
  - For Holding/Input Register :- Maximum 123 registers

- Example :-

  Request : 00 00 00 00 00 06 01 03 00 05 00 02

  Response : 00 00 00 00 00 06 01 03 04 02 1C 03 0A

4.2 RTU MESSAGE FRAME

In Modbus RTU frame instead of MBAP header, CRC(2 bytes)is added at the end of frame which can be seen below:-

Unit Identifier (1 byte)	Function Code (1 byte)	Data (As per required)	CRC (2 bytes)

Here, in CRC field the lower byte is taken first followed by higher byte.

- Registers / Coils Size:

Since modbus message size is 256 bytes below are the total number of coils/registers that can be read/write:-

- For Coils/Discrete Input :- Maximum 2000 coils/discrete input
- For Holding/Input Register :- Maximum 125 registers

- Example :-

  Request : 01 03 00 07 00 02 75 CA

  Response : 01 03 04 47 2B 00 00 9E 8F

4.3 ADDRESSING

Address must be between 0 to 65536. The start address must be entered by adding 1 to original address(data address defined inside slave device). For instance, if start address is 120 then 121 must be entered inside start address textbox.

5 CONNECTION SETTINGS

To open connection settings go to Setup Menu->Connect. It will open pop-up for setting up slave for TCP/IP or Serial connection.

Listen button is used for quick connection i.e. it will connect automatically with configuration set inside Setup Menu -> Connect. Window.

5.1 TCP/IP CONNECTION

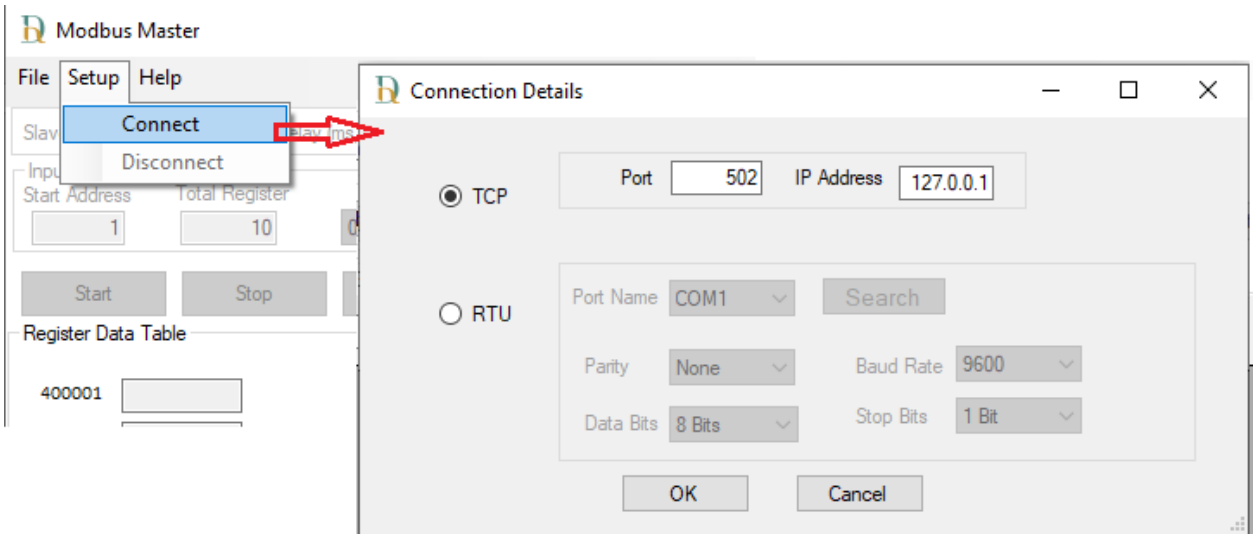

Figure 12 TCP / IP Connection Settings

TCP/IP connection consists of two components, (a) IP Address (b) Port, to which any external device can connect in the network.

a) IP Address:- Local IP address is needed to be specified to for connection. This gives the device to easily identify slave. By default the address is set to 127.0.0.1
b) Port :- Port number for listening client request. By default port number is set to 502.

5.2 SERIAL CONNECTION

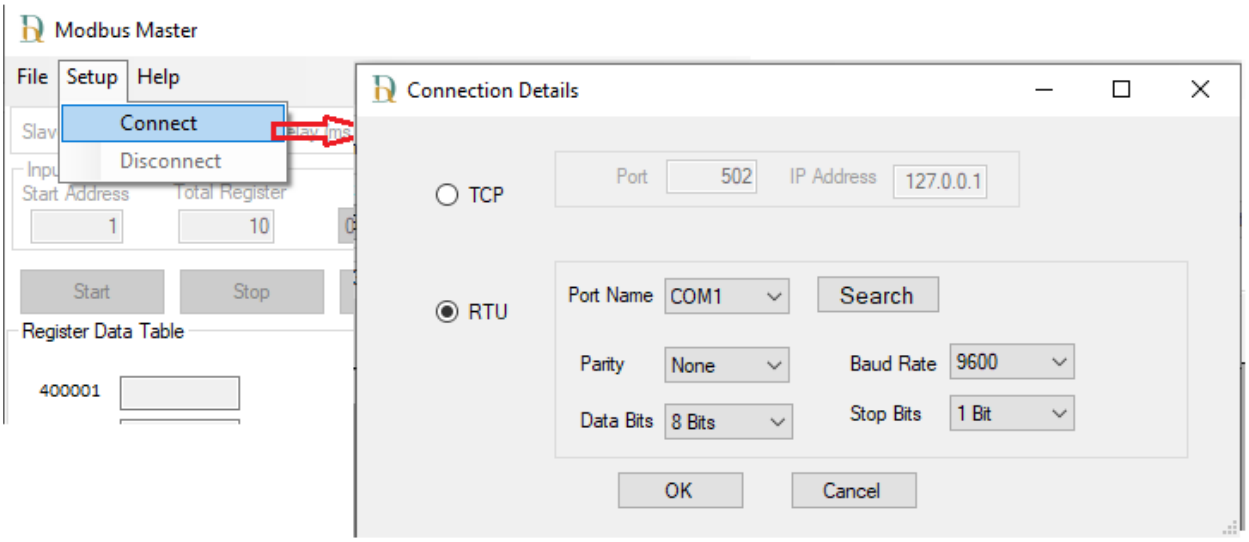

Figure 13 Serial Connection Properties

As shown in Fig. 13 following components are needed to set before slave is ready for serial connection:-

1. Port Name:- User have to select communication port from the available ports in dropdown section. Select only those port that are serial port which can be found out from under “Device Manager -> Ports(COM & LPT)”.
2. Parity:- It is used for detecting errors in transmission. Available values in dropdown:-
   - None (Default)
   - Odd
   - Even
   - Mark
   - Space
3. Data bits: This value is used for sending number of data bits in binary at a time. Available Values:
   - 8 (Default) :- or most kinds of data, as this size matches the size of a byte.
   - 7
4. Baud Rate:- It is the rate at which information is transferred in a communication channel. Following rates are available for serial port transmission.

150	1200	4800	14400	57600
300	1800	7200	19200	115200
600	2400	9600 (Default)	38400	128000

5. Stop Bits:- Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronise with the character stream. Available values:
    - None (Default)
    - 1 Bit
    - 1.5 Bits
    - 2 Bits

5.3 DELAY SETTINGS

- Request Delay :- Delay between each request. Minimum delay is 500ms. If receive delay is higher than request delay then software will consider receive delay.
- Receive Delay :- This delay is used before software starts reading data from input buffer to avoid data loss. Minimum delays are automatically set according to baud rates to avoid data loss. E.g. for baud rate 1200ms minimum receive delay is set to 1450, but user can set receive delay more than or equal to 1450 ms.

Figure 14 Delay example

6 USING MODBUS SIMULATOR

6.1 SENDING READ REQUEST

After successful connection, connection type and name will be shown at bottom, only those fields required for read/write request and DISCONNECT button would be visible/editable as you can see in Figure 15

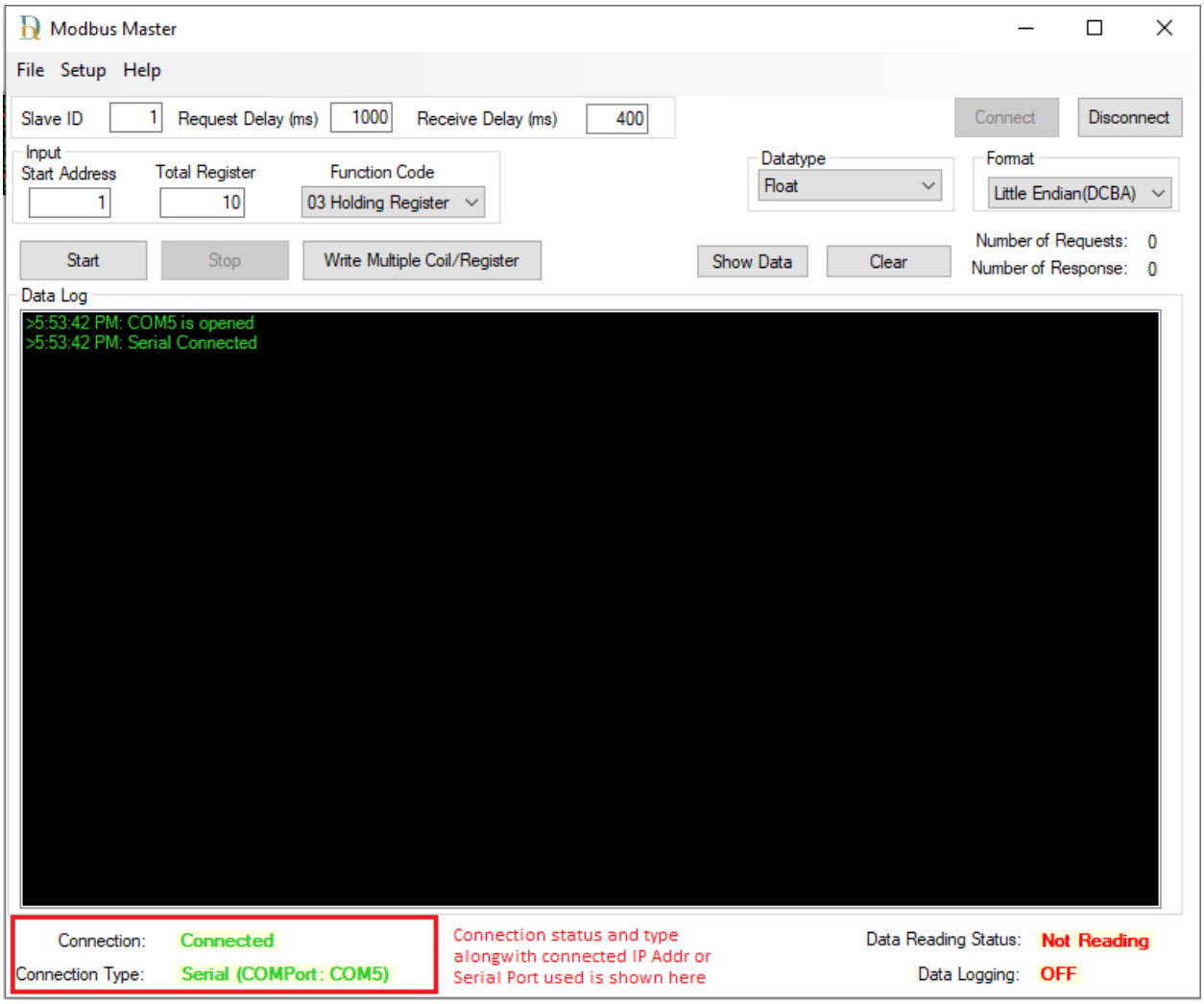

Figure 15 Initiating read request for slave device

On setting these values and clicking on START button will start reading data for selected function code at time interval defined in REQUEST DELAY textbox. If correct response is received then “Data Reading Status ” will show “Success” else shows error.

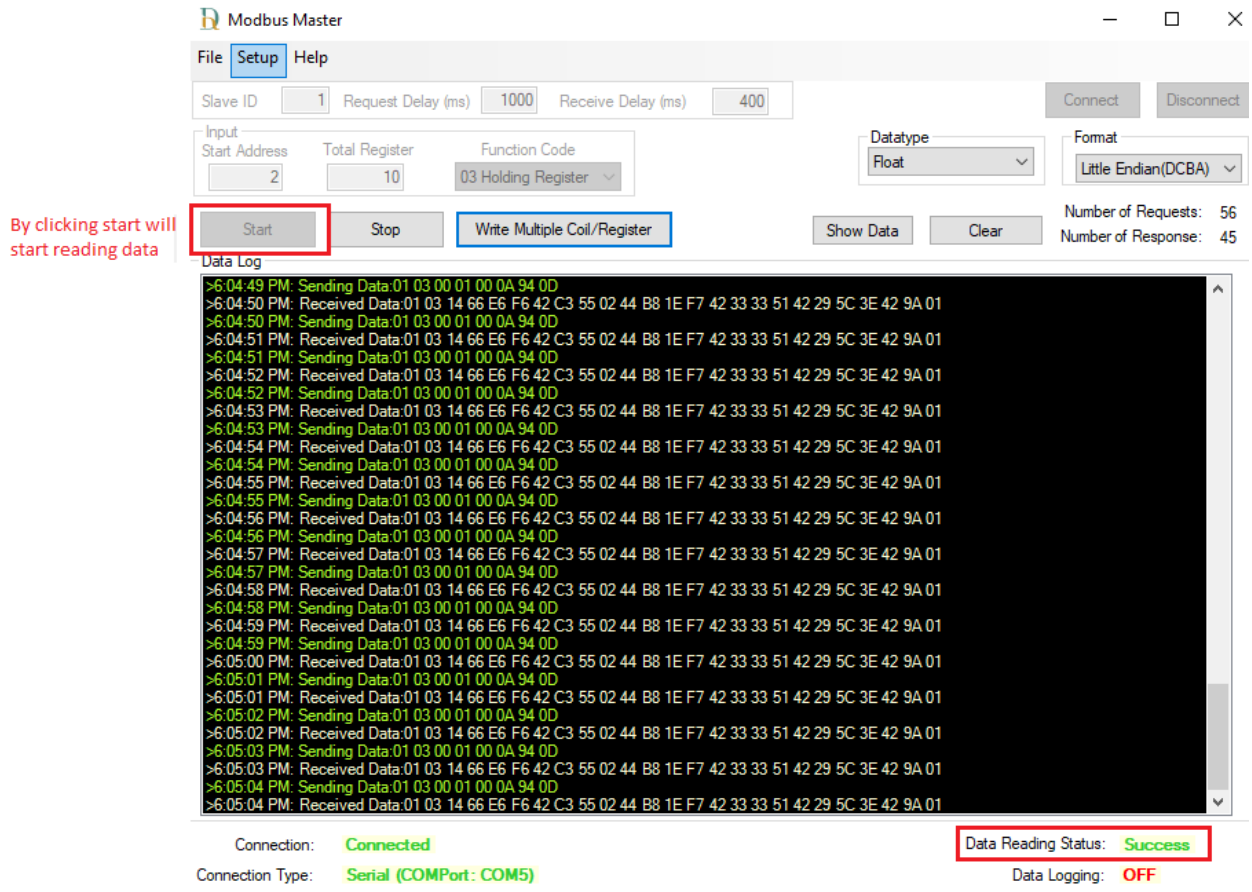

Figure 16 Start reading data from slave device

You cannot change any values while request is ongoing for this you have to click STOP button to stop sending request and then you can change input values and start again.

6.2 SENDING WRITE REQUEST

- Sending Write Single Coil/Register Request:-

  For sending write single register/coil data, double-click on textbox/led inside REGISTER DATA TABLE box which will open a window for entering data. Here, whatever datatype and format is selected the data will be represented in that format inside textbox(see Fig.18) in case of registers and coil status in case of coil(see Fig.19).

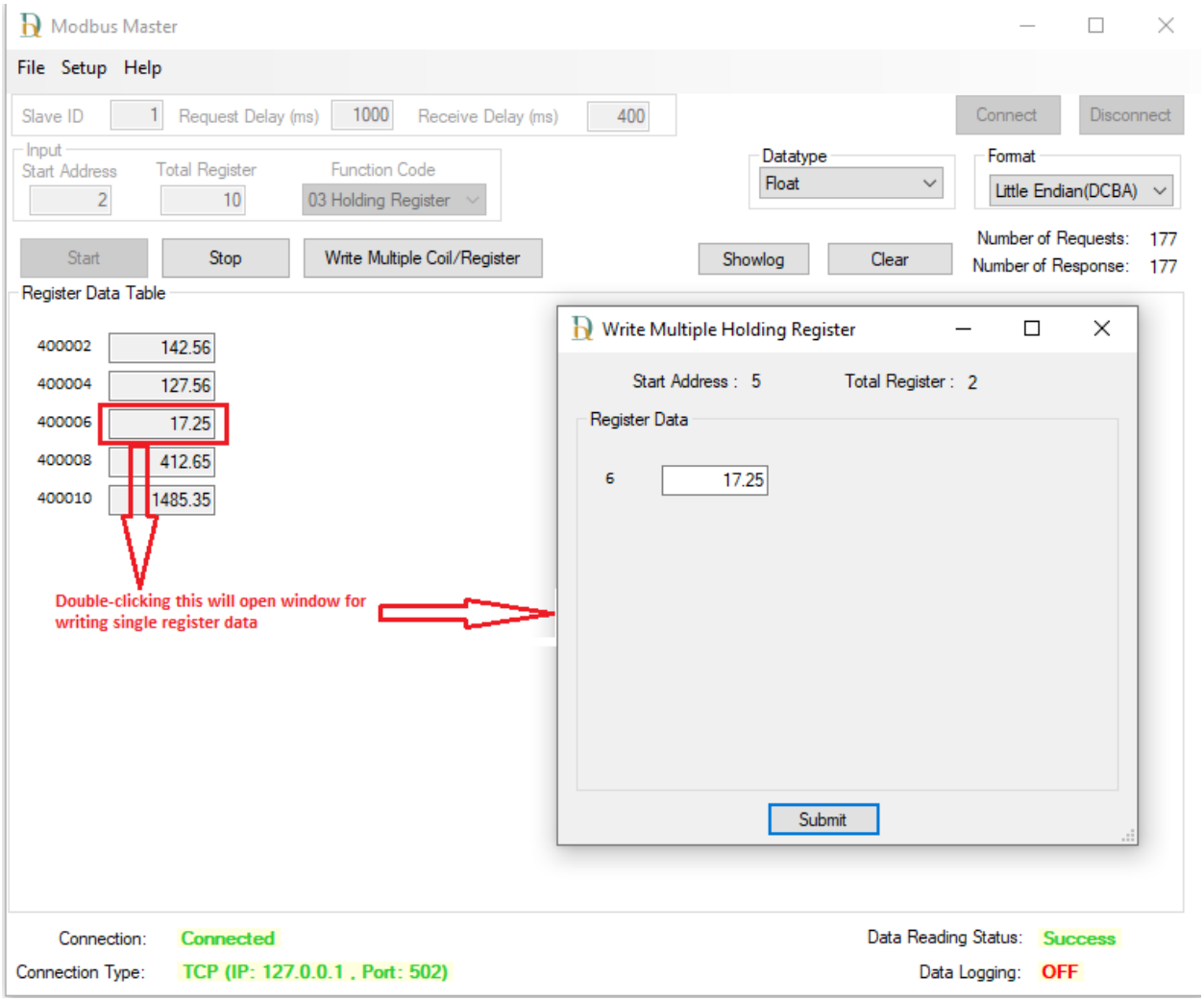

Figure 17 Window for editing data of single register (single register write)

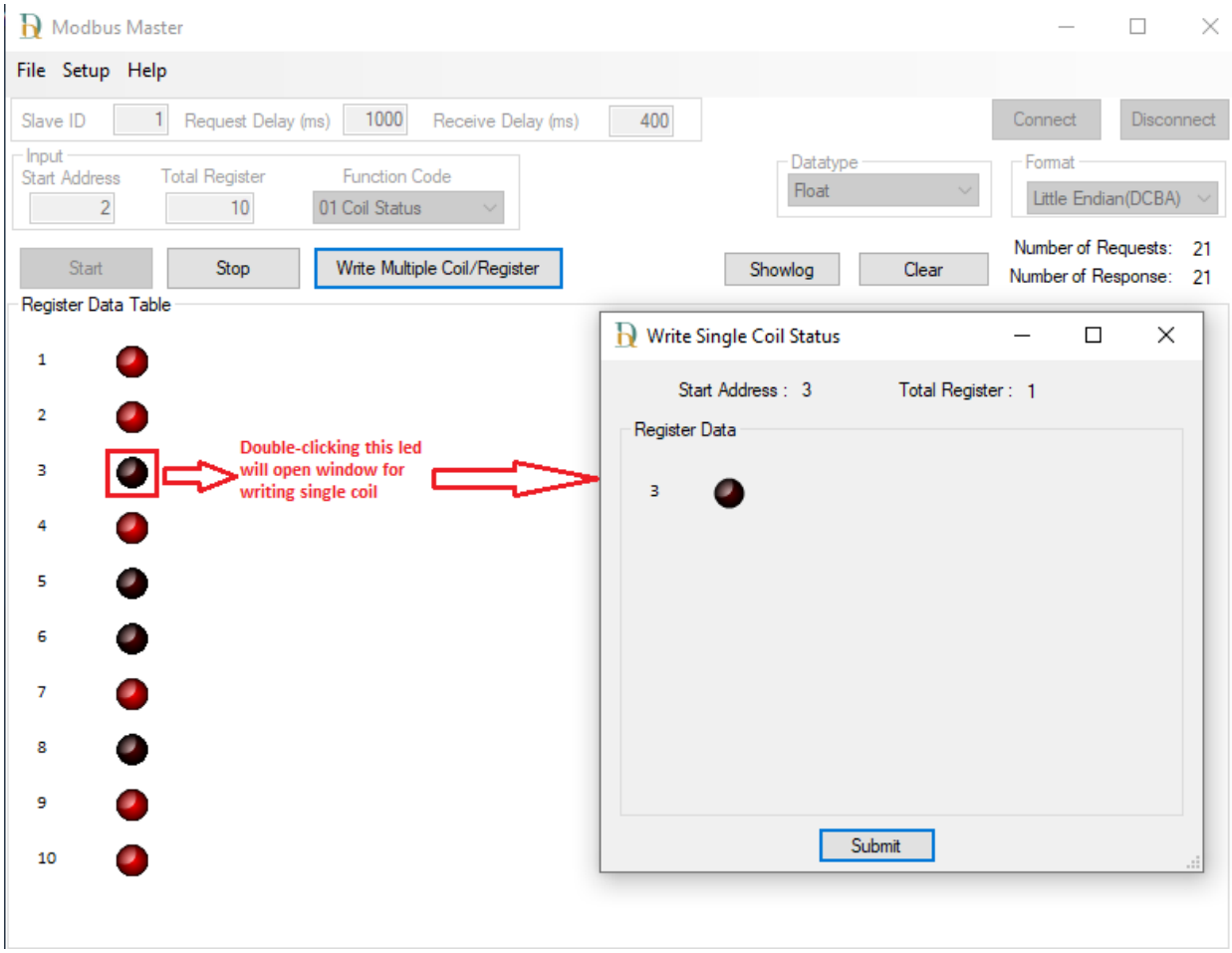

Figure 18 Window for editing data of single coil(single coil write)

After editing on clicking SUBMIT button will send request and update data at specified register/coil address.

- Sending Write Multiple Coil/Register Request:-

  For sending write multiple register/coil data, click on WRITE MULTIPLE COIL/REGISTER button which will open a window asking to select option for multiple register/coil, enter start address(insert address by adding 1) and total register (see Fig. 20).

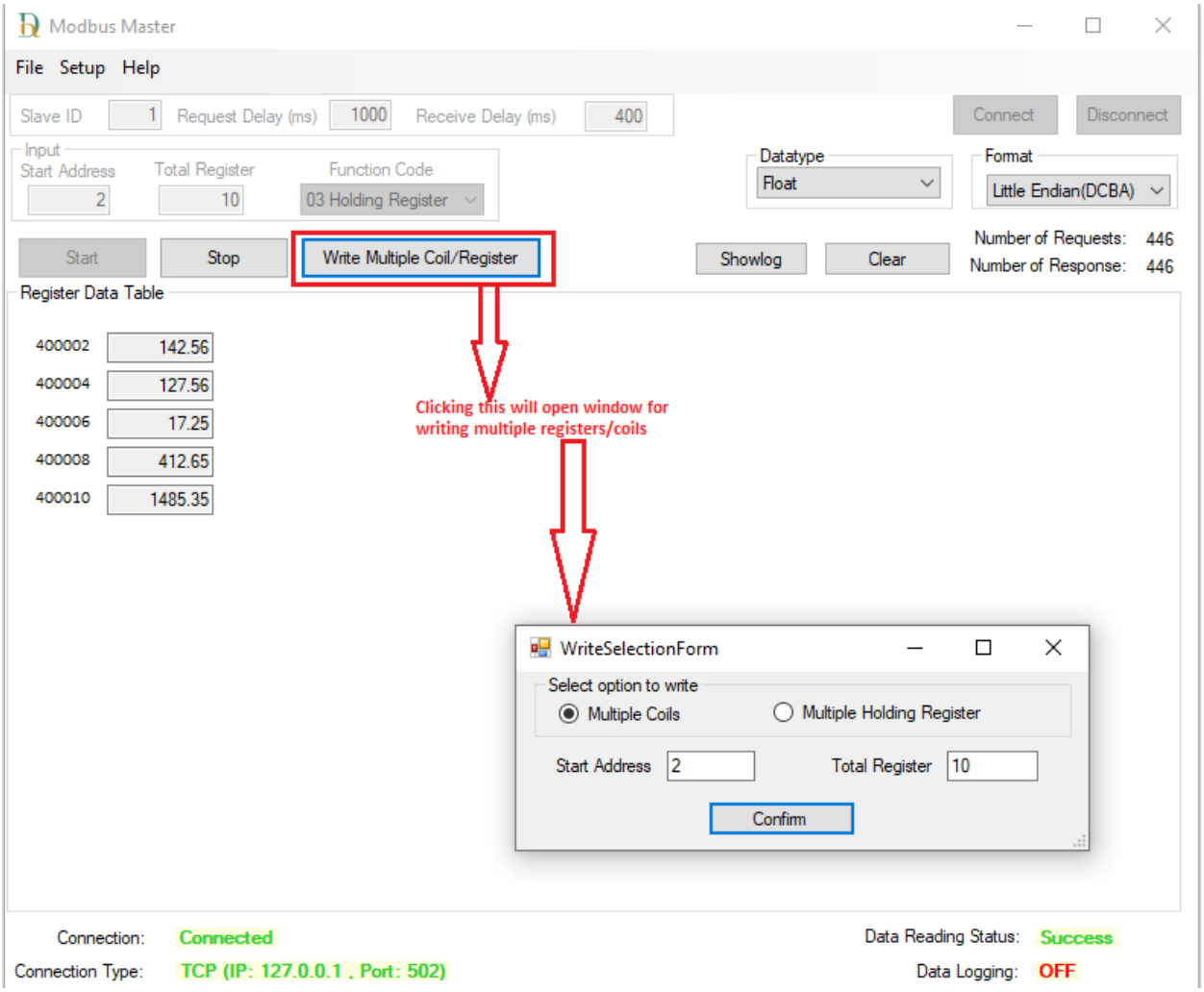

Figure 19 Coil Status / Input Status view for function code 01 / 02 selection

On clicking confirm will open another window showing start address and total register on top side and multiple textbox(in same format and datatype as defined for read request) for registers (see Fig. 21) and for led (see Fig. 22) inside REGISTER DATA box to update data.

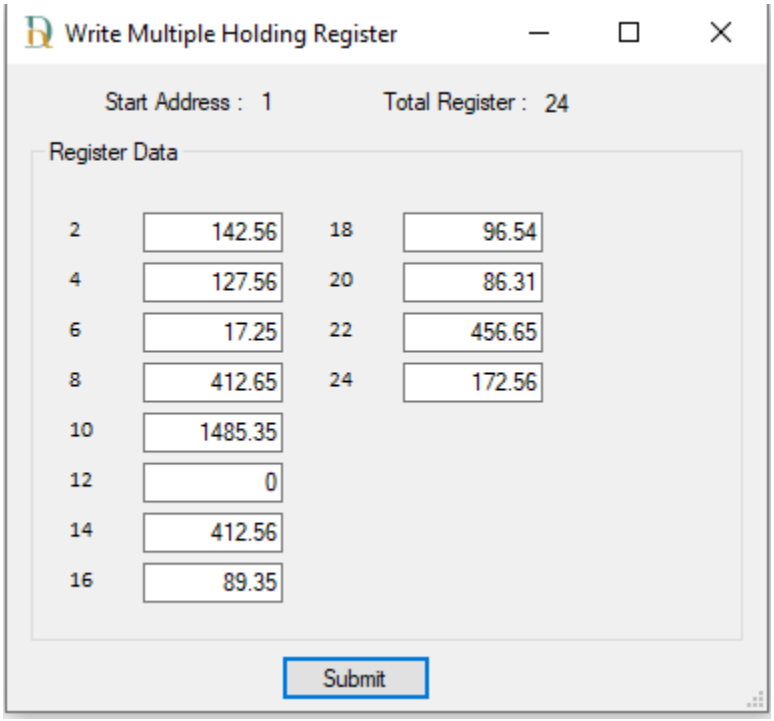

Figure 20 Multiple Register Write window

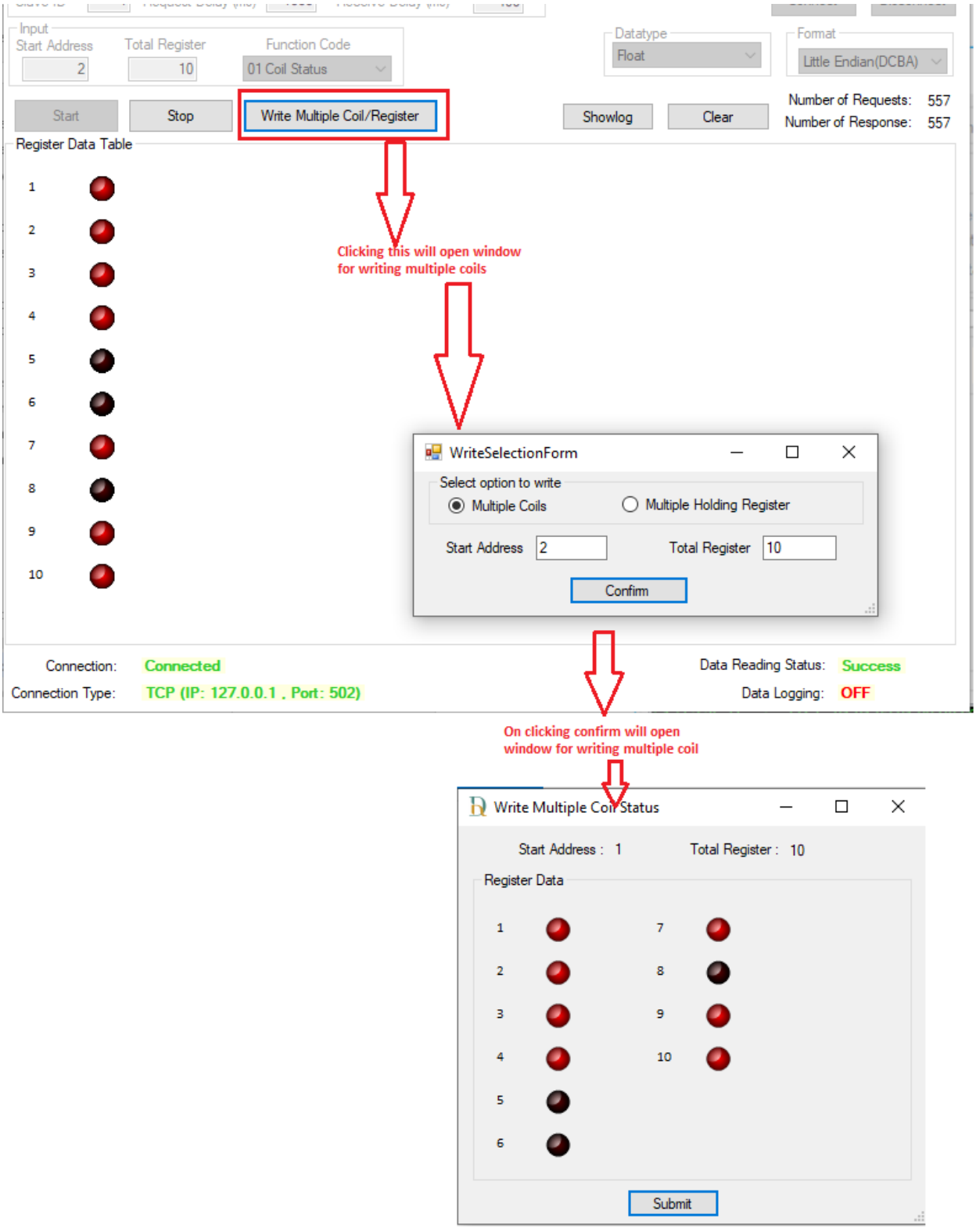

Figure 21 Multiple Coil Write window

By submitting will send write multiple register/coil request to the slave device.

6.3 DATA LOGGING/ EXPORTING DATA AS CSV

This software provides feature of data capturing i.e. saving data in csv format along with timestamp. It can be used for analyzing or monitoring analog / digital values of PLC device.

This feature can be enabled by going to File Menu->select DataLog On which will open pop-up for selecting path to start logging in csv file.

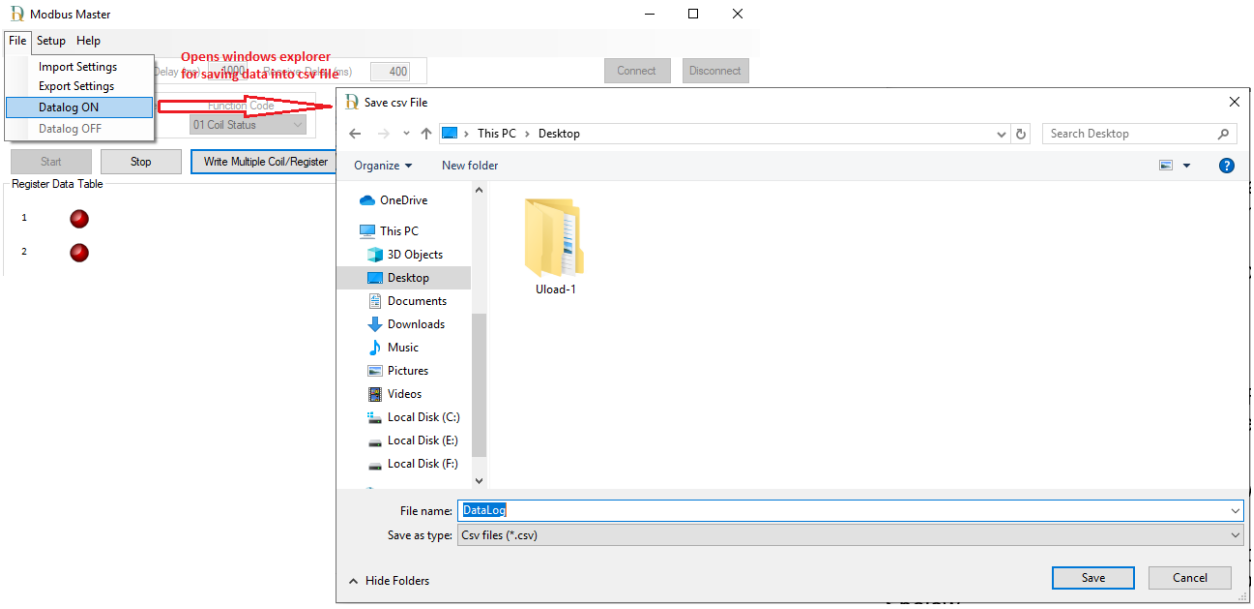

Figure 22. Selecting path for saving data

After file selection is done it will ask to select time interval at which user wants to log data. Here, there are two option for selecting time interval:-

1. Save Every Scan :- Means it will log data each and every response software receives.
2. Save Selected Scan :- It will log data at particular time defined across Frequency which will automatically enabled when selecting this option

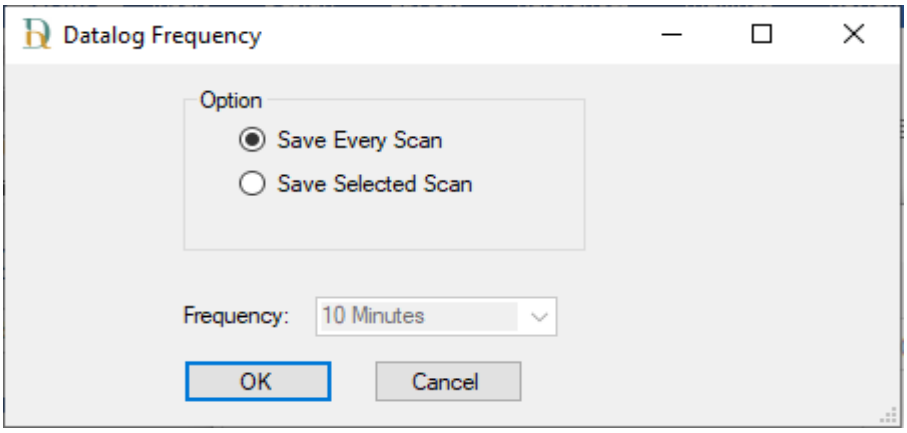

Figure 23 Option for logging data at specific time interval

On clicking OK will start logging data. Data logging status can be seen in the bottom section of software.

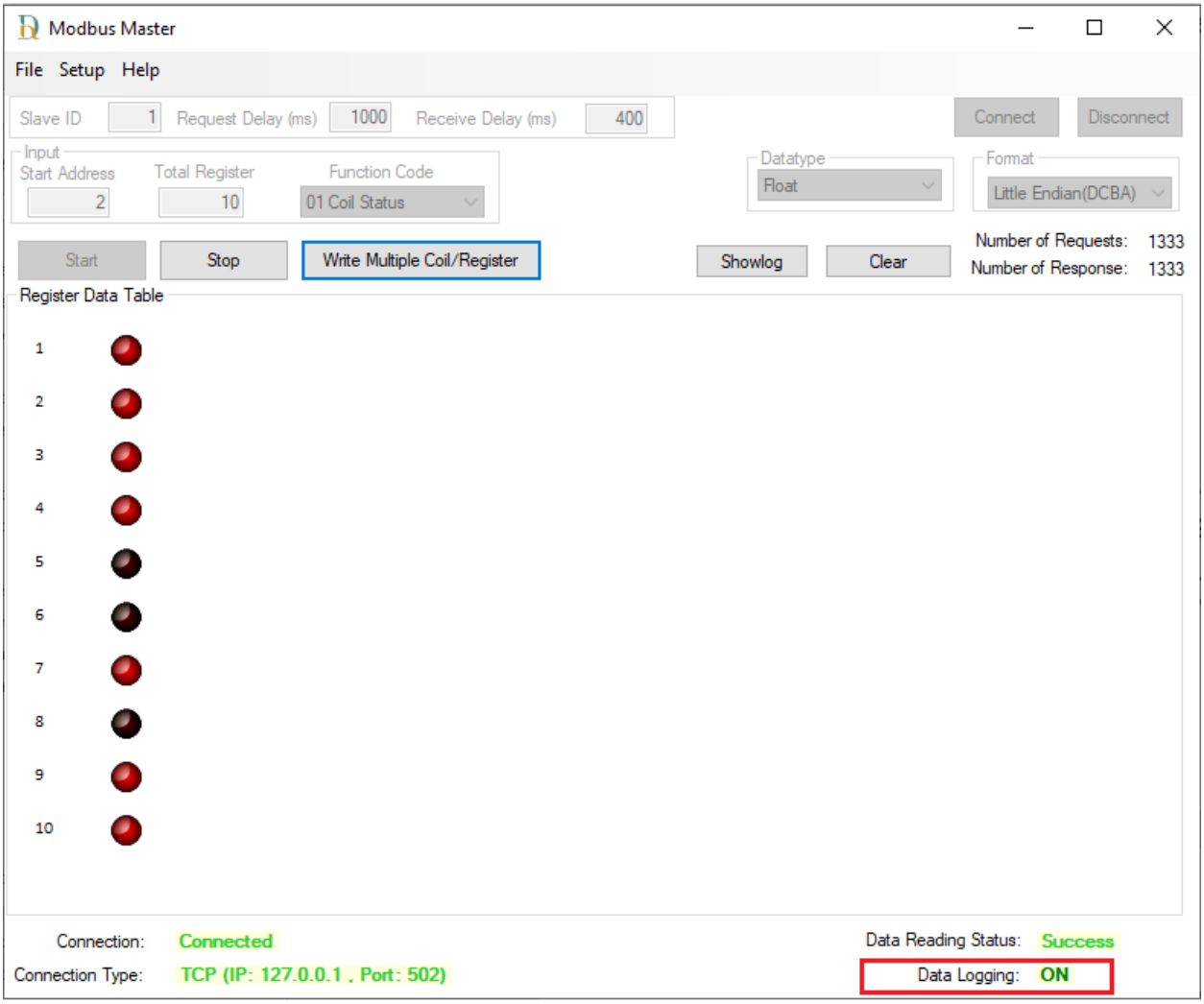

Figure 24 Data Logging started status

The .csv file created can be seen in Fig.

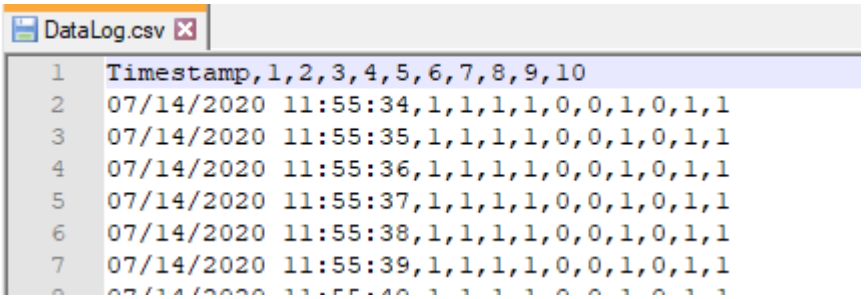

Figure 25 Data Log .csv file visualization(open in Notepad)

Data Logging can be stopped from File Menu ->DataLog Off.

7 MODBUS DISPLAY FORMAT

7.1 FLOAT-32 BIT

Here, floating point value of 4 byte(32 bit) is stored in 2 Register of 2 byte i.e. 16-bit Register and can be visualized in 4 different formats, each giving different value based on their arrangement.

To understand this, consider floating point value 204.56 which can be displayed in different format as shown below:-

204.56 in hexadecimal would be 43 4c 8f 5c. Here byte order is Big-Endian which can be shown in Fig.21. Similarly, arranging this in other format would show different values shown below.

- Float Big-Endian (ABCD) :-
  Byte Order:- 43 4C 8F 5C
  Value :- 204.56
- Float Little Endian (DCBA):-
  Byte Order:- 5C 8F 4C 43
  Value :- 3.22678e+17
- Float Mid-Big Endian (BADC):-
  Byte Order:- 4C 43 5C 8F
  Value :- 5.12129e+07
- Float Mid-Little Endian (CDAB)
  Byte Order:- 8F 5C 43 4C
  Value :- -1.08598e-29

7.2 SIGNED INTEGER-32 BIT

Similar to float-32 bit, this format also uses 2 16-bit registers to form 32-bit signed integer and can be represented in 4 different format.

For e.g., consider value -939257913 which is C8 04 0F C7
in hexadecimal(Big-Endian format)

- Signed Integer-32 Big-Endian (ABCD) :-
  Hexadecimal format:- C8 04 0F C7
  Value :- -939257913
- Signed Integer-32 Little Endian (DCBA):-
  Byte Order:- C7 0F 04 C8
  Value :- -955317048
- Signed Integer-32 Mid-Big Endian (BADC):-

Byte Order:- 04 C8 C7 0F
Value :- 80267023

- Signed Integer-32 Mid-Little Endian (CDAB)
  Byte Order:- 0F C7 C8 04
  Value :- 264751108

7.3 UNSIGNED INTEGER-32 BIT

Here,2 16-bit registers collectively form 32-bit unsigned integer and can be represented in 4 different format.

For e.g., consider value 67124491 which is 04 00 3D 0B in hexadecimal(Big-Endian format)

- Unsigned Integer-32 Big-Endian (ABCD) :-
  Hexadecimal format:- 04 00 3D 0B
  Value :- 67124491
- Unsigned Integer-32 Little Endian (DCBA):-
  Byte Order:- 0B 3D 00 04
  Value :- 188547076
- Unsigned Integer-32 Mid-Big Endian (BADC):-
  Byte Order:- 00 04 0B 3D
  Value :- 265021
- Unsigned Integer-32 Mid-Little Endian (CDAB):-
  Byte Order:- 3D 0B 04 00
  Value :- 1024132096

7.4 SIGNED INTEGER-16 BIT

In this format only 1 16-bit register is used to form signed 16-bit integer and can be represented in 2 different formats.

Take value -14332 whose hexadecimal value is C8 04(Big-Endian).

- Signed Integer-16 Big-Endian (ABCD) :-
  Hexadecimal format:- C8 04
  Value :- -14332
- Signed Integer-16 Little Endian (DCBA):-
  Byte Order:- 04 C8
  Value :- 1224

7.5 UNSIGNED INTEGER-16 BIT

In this format only 1 16-bit register is used signed 16-bit unsigned integer and can be represented in 2 different formats.

Take value 4039 whose hexadecimal value is 0F C7 (Big-Endian).

- Signed Integer-16 Big-Endian (ABCD) :-
  Hexadecimal format:- 0F C7
  Value :- 4039
- Signed Integer-16 Little Endian (DCBA):-
  Byte Order:- C7 0F
  Value :- 50959

7.6 HEXADECIMAL

Here, value stored in 16-bit register will be shown in hex format. For e.g., for a given value 204.56 (43 4c 8f 5c in hexadecimal), In 1st register it will show 43 4c then 8f 5c in next register.

7.7 BINARY

The value stored in 16-bit register is shown in binary i.e. 0 and 1 format.