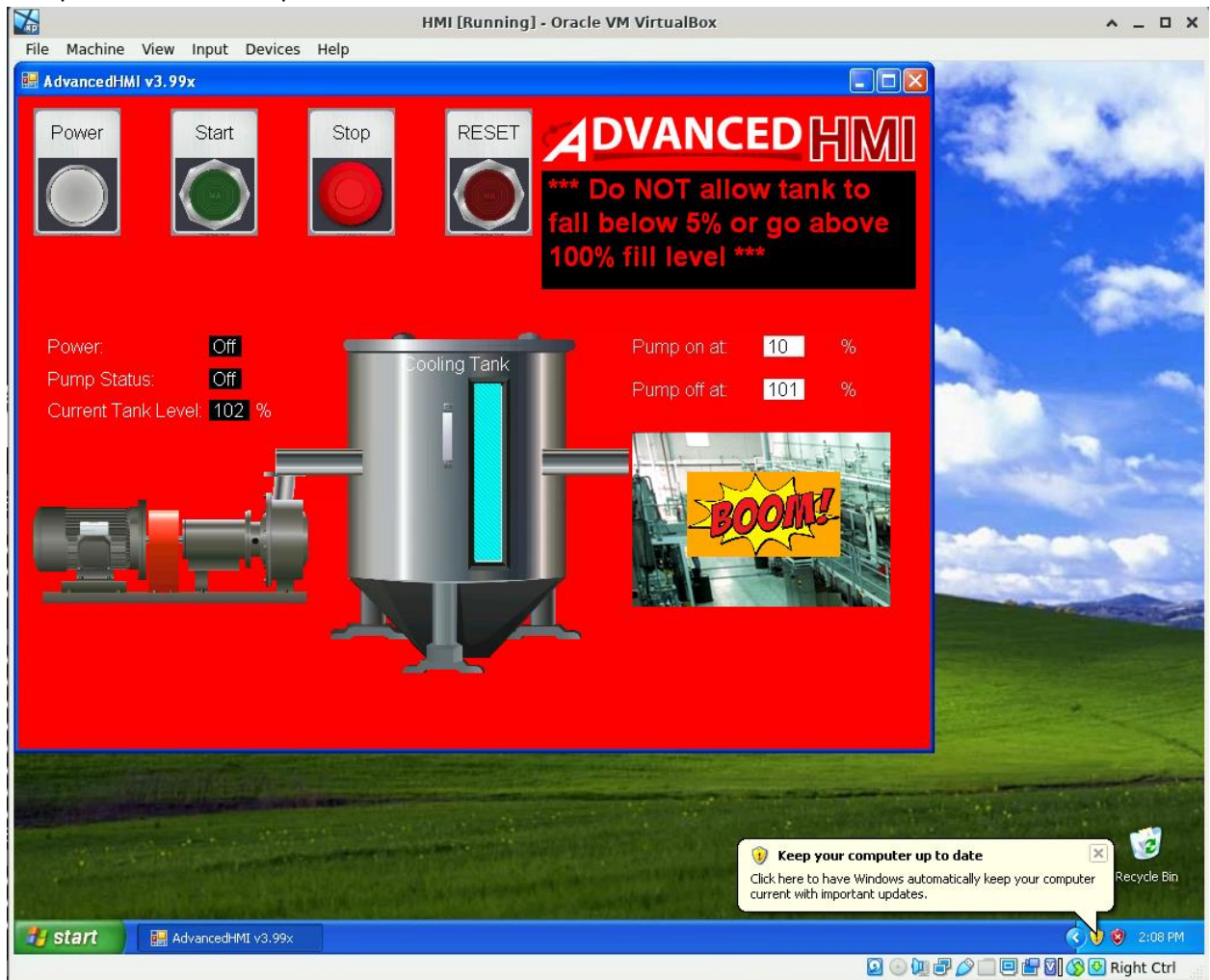


ICS Basics Lab Form

Name:

Date:

1. Paste the screen shot taken in Part 2 – “Use an HMI System to Monitor and Control ICS Components” into this question:



2. Paste the screen shot taken in Part 3 – “Use an OPC Server to Monitor and Control ICS Components” into this question:



The screenshot shows the OPC Quick Client interface. The tree view on the left displays the following structure:

- Keypware.KEPSEverEX.V5
 - _System
 - Channel1._CommunicationSerial
 - Channel1._Statistics
 - Channel1._System
 - Channel1.Cooling_Tank**
 - Channel1.Cooling_Tank._Statist
 - Channel1.Cooling_Tank._System
 - Data Type Examples._Statistics
 - Data Type Examples._System

The table below shows the data points for Channel1.Cooling_Tank:

Item ID	Data Type	Value	Timestamp	Quality	Update Count
Channel1.Cooling_Tank.Power	Boolean	0	08:29:56.608	Good	3
Channel1.Cooling_Tank.Pump_Relay	Boolean	0	08:29:49.597	Good	22
Channel1.Cooling_Tank.Reset_Switch	Boolean	0	08:25:07.201	Good	1
Channel1.Cooling_Tank.Sp_Start_Level	Word	50	08:25:07.201	Good	1
Channel1.Cooling_Tank.Sp_Stop_Level	Word	75	08:25:07.201	Good	1
Channel1.Cooling_Tank.Start_Switch	Boolean	0	08:25:07.201	Good	1
Channel1.Cooling_Tank.Stop_Switch	Boolean	0	08:25:07.201	Good	1
Channel1.Cooling_Tank.Tank_Level	Word	62	08:29:56.608	Good	280

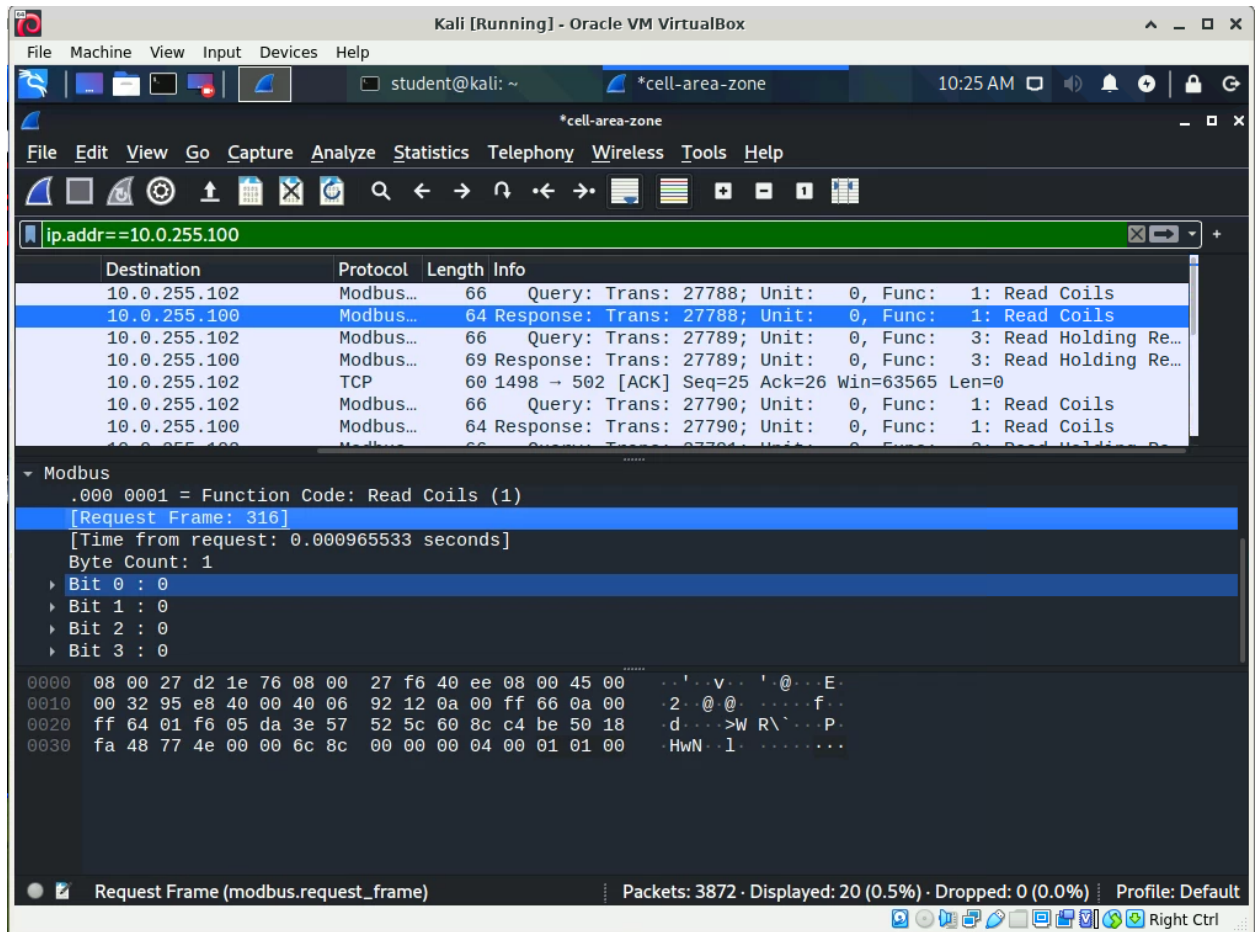
The bottom pane shows a list of events with columns Date, Time, and Event. The events are as follows:

Date	Time	Event
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 9 items to gr...
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 34 items to g...
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 34 items to g...
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 4 items to gr...
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 9 items to gr...
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 44 items to g...
7/14/2021	8:25:07 AM	Added group 'Data ...
7/14/2021	8:25:07 AM	Added 44 items to g...
7/14/2021	8:25:07 AM	Added 4 items to gr...
7/14/2021	8:25:07 AM	Added group 'Simul...
7/14/2021	8:25:07 AM	Added group 'Simul...
7/14/2021	8:25:07 AM	Added 11 items to g...
7/14/2021	8:25:07 AM	Added group 'Simul...
7/14/2021	8:25:07 AM	Added 3 items to gr...
7/14/2021	8:25:07 AM	Added group 'Simul...
7/14/2021	8:25:07 AM	Added 9 items to gr...
7/14/2021	8:25:07 AM	Added 16 items to g...
7/14/2021	8:26:07 AM	Set active state '0' f...
7/14/2021	8:26:17 AM	Set active state '1' f...
7/14/2021	8:29:56 AM	Synchronous write ...

The bottom status bar shows 'Ready' and 'Item Count: 314'.

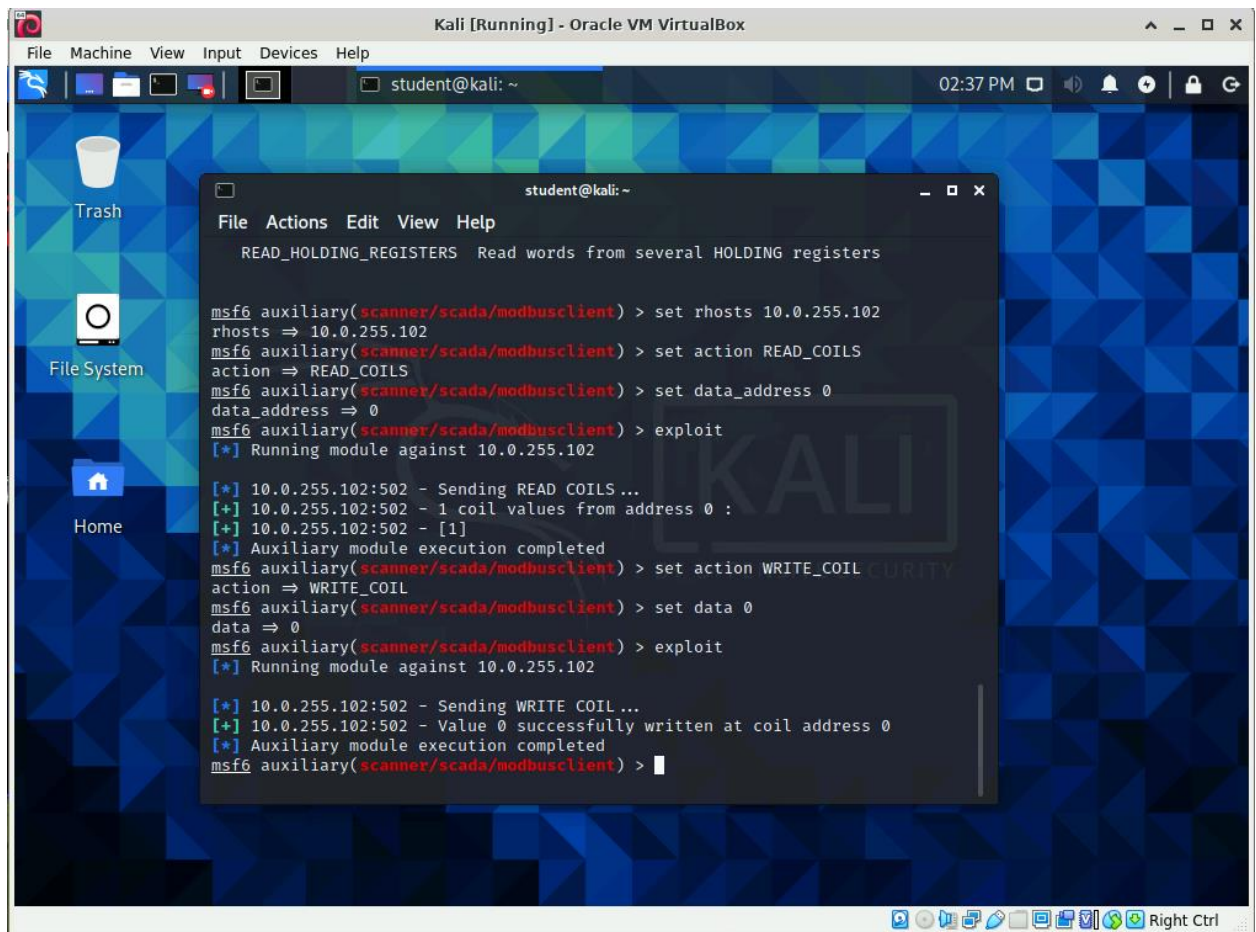
The screen show submitted by the student should show a different time and/or some other difference from this and the reference example.

- Paste the screen shot taken in Part 4 – “Use Wireshark to view Modbus/TCP traffic” into this question:



The screen show submitted by the student should show a different time and/or some other difference from this and the reference example.

4. Paste the screen shot taken in Part 5 – “Use Metasploit to exploit Modbus/TCP vulnerabilities” into this question:



The screen show submitted by the student should show a different time and/or some other difference from this and the reference example.

5. What is the status of the system power and the pump power when the packets containing the protocol data unit reference 1909 were captured?

The byte of data read from memory area Q0.0 contained the hexadecimal value 01. This converts into 0000 0001 in binary. The Power tag is assigned address Q0.0 which maps to the least significant binary bit containing the value 1. The Pump tag is assigned address Q0.1 which maps to the second least significant binary bit containing the value 0. This means that power to the pump is off and power to the system is on.