

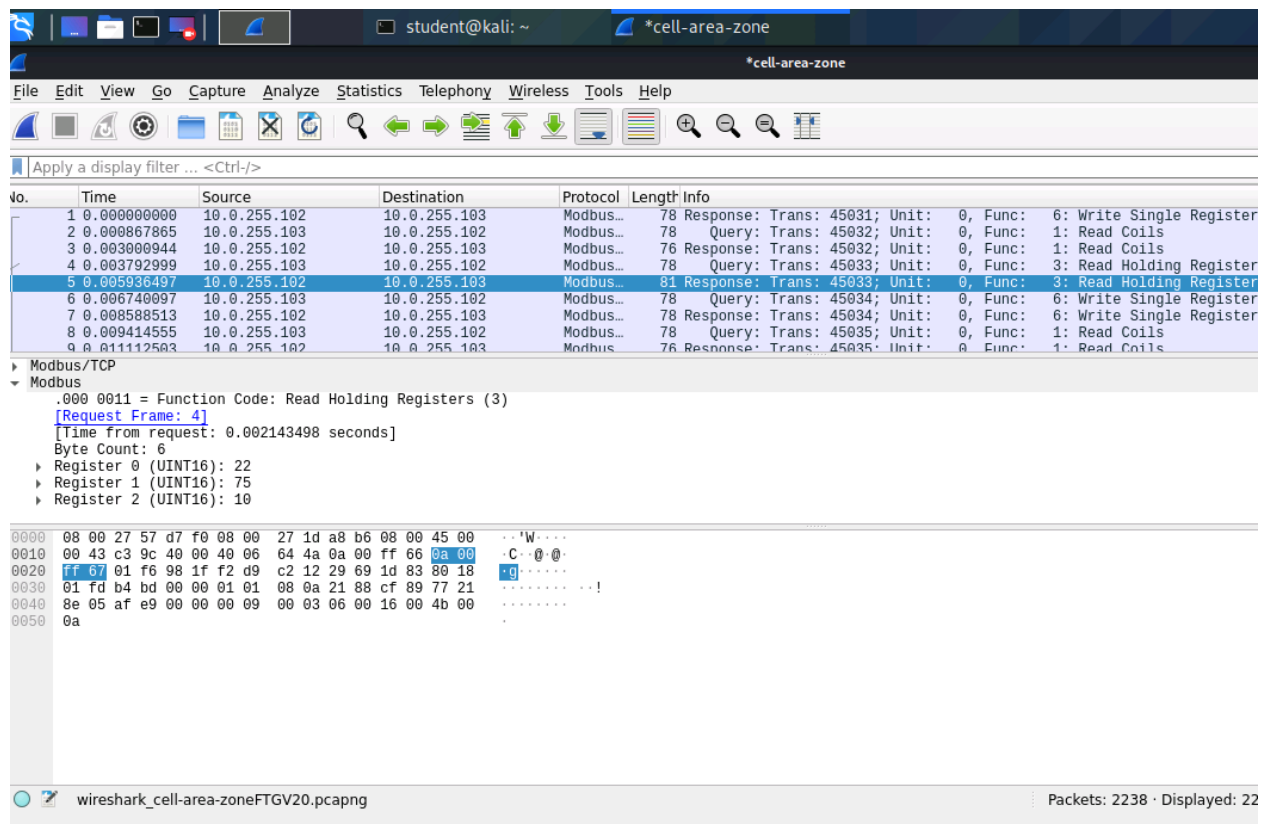
# Zoning Lab Form

7 questions at 4 points a piece – 28 total points

Name: | |

Date: | |

1. Paste the screen shot taken in the “Capture and view data transmitted in the Cell-Area zone” part of the lab into this question:



2. What does the value in Register 0 probably represent?

**(-4) The value in register 0 represents the current tank level. You can determine this by looking at the HMI and noting that the values in the Pump on at and pump off at fields match what is shown in registers 1 and 2. The only other value in the system that is something other than true/false is the current tank level.**

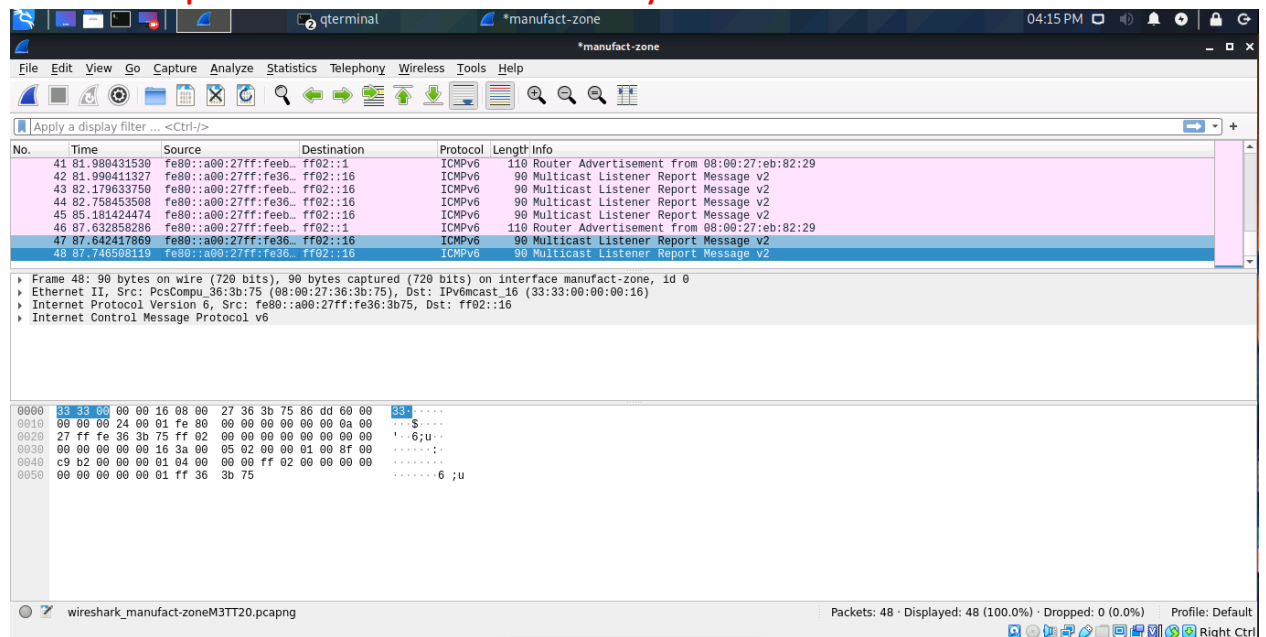


3. What does the value in Register 1 probably represent?

**(-4) The value in register 2 indicates when the pump should be turned off. This matches the pump off at field from the HMI.**

4. Paste the screen shot taken in the “Capture and view data transmitted in the Manufacturing zone” part of this lab into this question:

**Sound have captured ICMP and broadcast traffic only.**



5. Why was the network ping traffic between the Kali-Modus system and the PLC captured but the data between the PLC and other ICS systems was not?

**(-4) Devices can only sniff data from networks they are attached to or that is addressed to or from their own MAC address. The Kali-Modus system was moved to a different network then the PLC system. This allowed it to view ping traffic from itself to the PLC but prevented it from viewing traffic between the PLC and OPC server.**

6. If using proper zoning techniques is more secure why might companies not configure their systems using this technique?



**(-4) The main reason companies might not choose to secure their networks using zoning is because it is more complicated and expensive then just putting all of the systems on the same network.**

|

7. If you were to capture data on the Cell-Area zone and you consistently observed the following data what might you conclude regarding the functionality of the cooling system?

The screenshot shows a Wireshark capture of Modbus data on the cell-area-zone interface. The packet list shows a sequence of Read Coils and Read Holding Registers requests and responses. The packet details pane shows a Read Holding Registers request for registers 0, 1, and 2. The packet bytes pane shows the raw data for the request frame.

No.	Time	Source	Destination	Protocol	Length	Info
68	0.000000	10.0.255.102	10.0.255.100	Modbus/TCP	69	Query: Trans: 13502; Unit: 0, Func: 1: Read Coils
69	0.000000	10.0.255.100	10.0.255.102	Modbus/TCP	69	Response: Trans: 21104; Unit: 0, Func: 3: Read Holding Registers
70	0.000000	10.0.255.102	10.0.255.100	Modbus/TCP	69	Query: Trans: 13503; Unit: 0, Func: 1: Read Coils
71	0.000000	10.0.255.100	10.0.255.102	Modbus/TCP	69	Response: Trans: 13503; Unit: 0, Func: 1: Read Coils
72	0.000000	10.0.255.102	10.0.255.100	Modbus/TCP	69	Query: Trans: 13504; Unit: 0, Func: 1: Read Coils
73	0.000000	10.0.255.100	10.0.255.102	Modbus/TCP	69	Response: Trans: 13504; Unit: 0, Func: 1: Read Coils
74	0.000000	10.0.255.102	10.0.255.100	Modbus/TCP	69	Query: Trans: 13505; Unit: 0, Func: 1: Read Coils
75	0.000000	10.0.255.100	10.0.255.102	Modbus/TCP	69	Response: Trans: 13505; Unit: 0, Func: 1: Read Coils
76	0.000000	10.0.255.102	10.0.255.100	Modbus/TCP	69	Query: Trans: 13506; Unit: 0, Func: 1: Read Coils

Frame 1571: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface cell-area-zone, id 0  
 Ethernet II, Src: VMware\_01:91:89 (00:0c:29:01:91:89), Dst: VMware\_cd:19:3f (00:0c:29:cd:19:3f)  
 Internet Protocol Version 4, Src: 10.0.255.102, Dst: 10.0.255.100  
 Transmission Control Protocol, Src Port: 502, Dst Port: 1114, Seq: 36, Ack: 49, Len: 15  
 Modbus/TCP  
 Modbus  
 .000 0011 = Function Code: Read Holding Registers (3)  
 [Request Frame: 1568]  
 [Time from request: 0.000905231 seconds]  
 Byte Count: 6  
 Register 0 (UINT16): 0  
 Register 1 (UINT16): 60  
 Register 2 (UINT16): 10

0000 00 0c 29 cd 19 3f 00 0c 29 01 91 89 08 00 45 00 ..?)...E.  
 0010 00 37 16 4b 40 00 40 06 11 ab 0a 00 ff 66 0a 00 7.K@...f..  
 0020 ff 64 01 f6 04 5a 56 01 b9 bc e2 f3 ca da 50 18 .d.ZV....P..  
 0030 fa 48 40 50 00 00 52 70 00 00 00 09 00 03 06 00 .H@P..Rp.....

wireshark\_cell-ar...102\_iRmCDa.pcapn Packets: 2684 · Displayed: 2684 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

(-4) This screen shot probably means that the pump has failed or has been turned off, and the cooling tank is empty. The settings show that the pump should turn on when the cooling level gets down to 10% of the tank and should turn on when it gets up to 60% of the tank. The current level of the tank is 0% showing that it is empty.