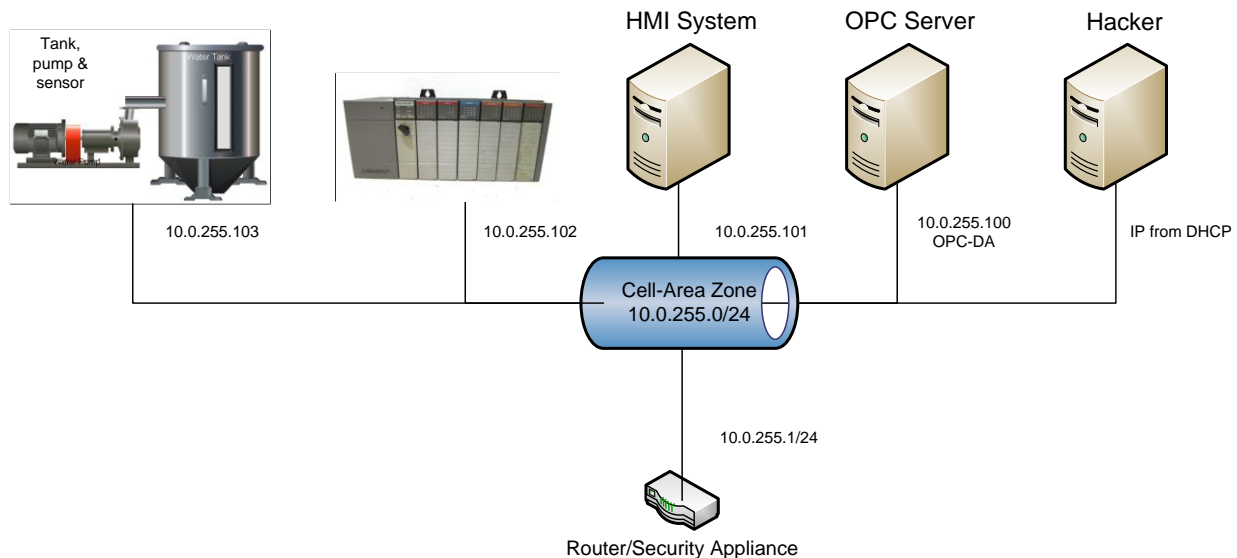


Lab 1

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 you are going to use Wireshark to capture and view typical network traffic. You will observe that Wireshark can present captured data in multiple formats. You will use Wireshark display filters to limit the traffic shown to only that which interests you. Finally, you will use Wireshark's follow stream functionality to demonstrate how to collect, decode and view related network traffic in a single window.

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

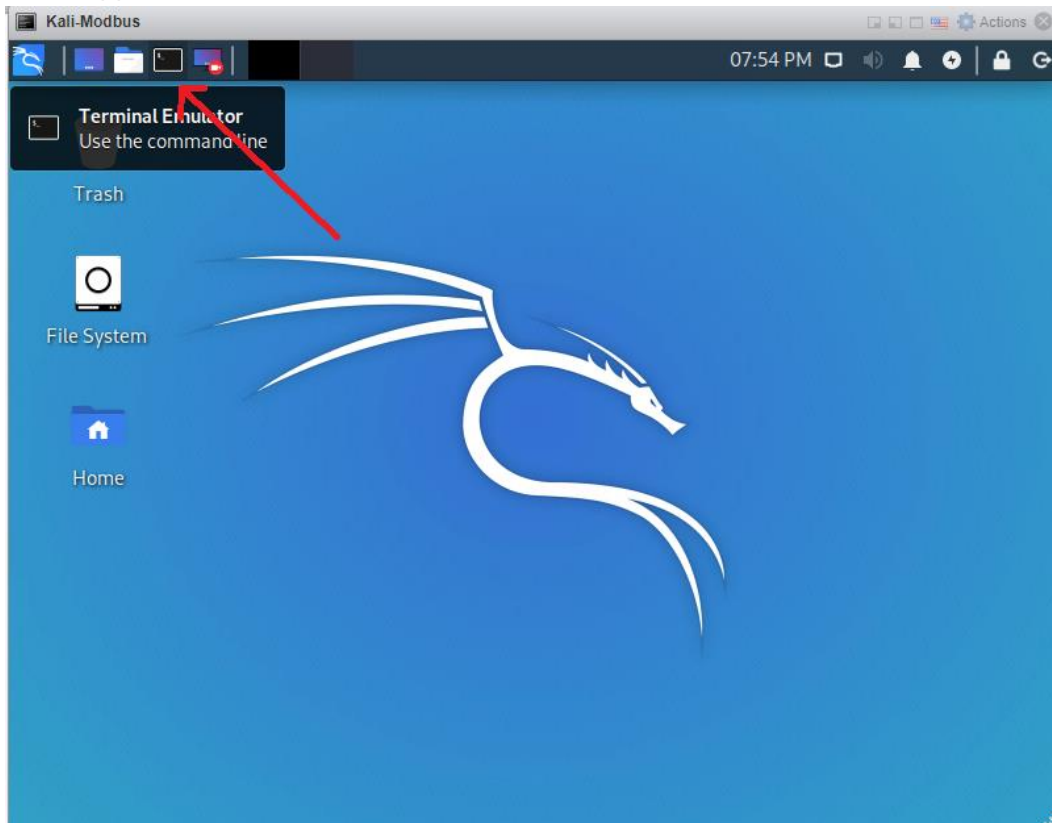
Part 2

Login to Kali and activate the network device connected to the manufacturing network

In this part of the lab you are going to login to the Kali system, view the system's IP address, bring up its second network card then start the ping program to generate typical network 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.



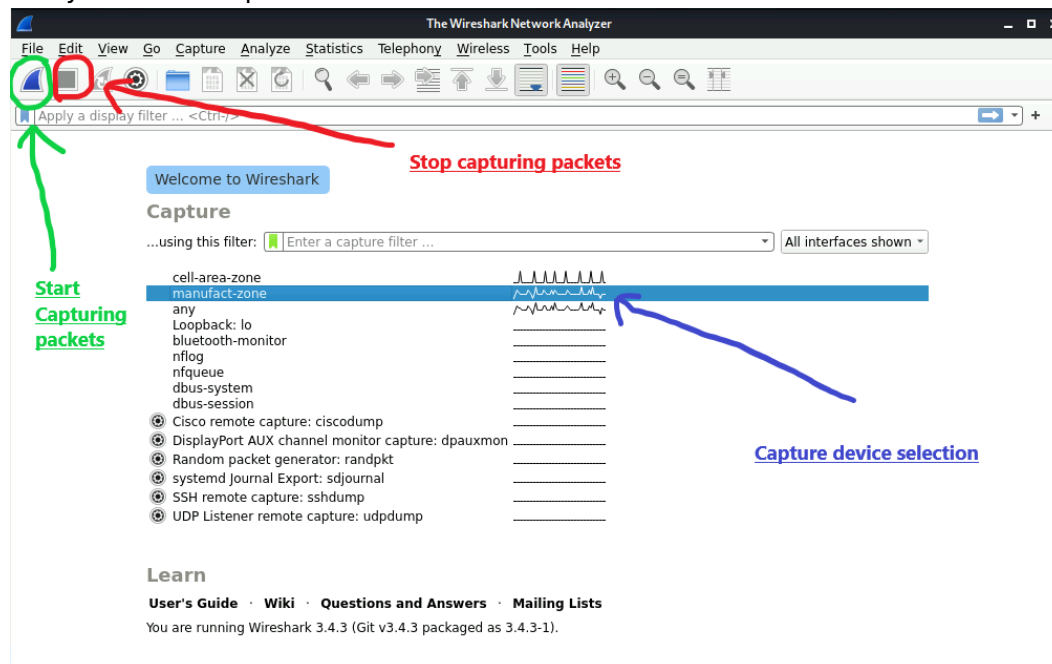
5. Type the command **nmcli connection** to view the available network connections.
6. Notice that the Cell-Area Zone configuration is associated with a device but the Manufacturing Zone configuration is not.
7. Type the letter **q** to stop viewing the network configurations.
8. Switch the zone (network segment) that the Kali system is connected to by typing the command **~/change_network.sh** then providing the student user's password, **Password01** when prompted.
 - To prevent people from looking over your shoulder and writing down the password it is not displayed on the screen as you are typing.
9. View the available network configurations by typing the command **nmcli connection**.
10. Notice that now the Manufacturing Zone configuration is associated with a device but the Cell-Area Zone configuration is not.
11. Type the letter **q** to stop viewing the network configurations.
 - If you restart the Kali system at any point during this lab you will need to redo this section of the lab instructions.

Part 3

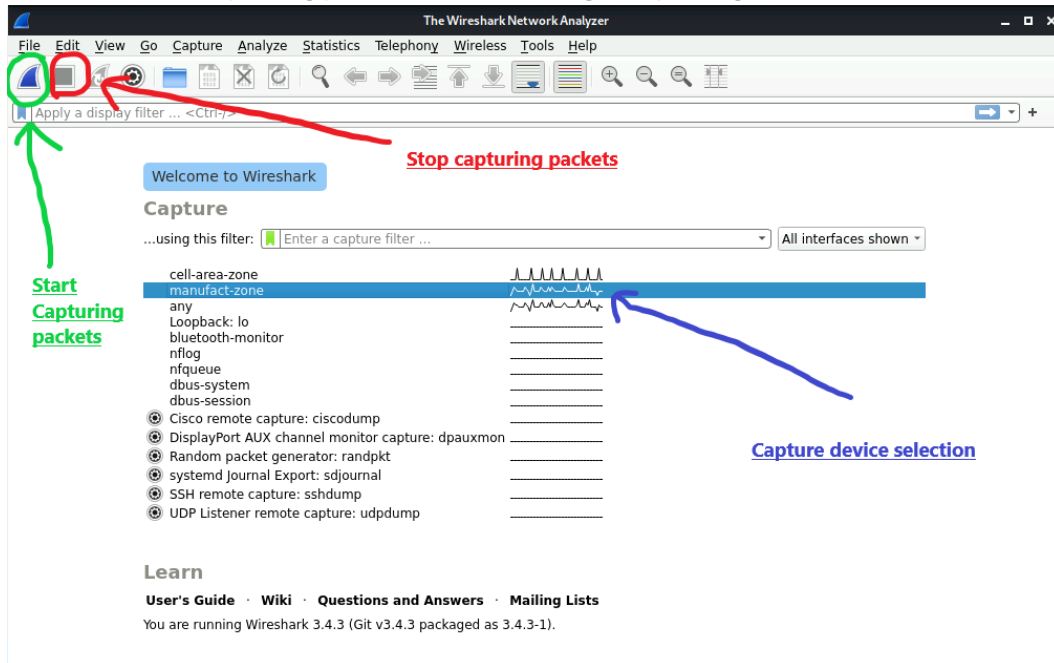
Use Wireshark to capture and view network traffic in different formats

In this part of the lab you are going to use the Wireshark network monitoring software to capture and view typical network data.

1. Type the command **ping 10.0.105.1** to generate typical ICMP network traffic.
2. Open a new tab in the Terminal Emulator program by going to the File menu then choosing the option + New Tab
3. Start the Wireshark program by typing the command **sudo wireshark**
 - If you are using sudo and are prompted to authenticate type in the password **Password01** followed by the **<ENTER>** key.
4. After the Wireshark program starts select the manufact-zone network device to indicate that you wish to capture data on that device.

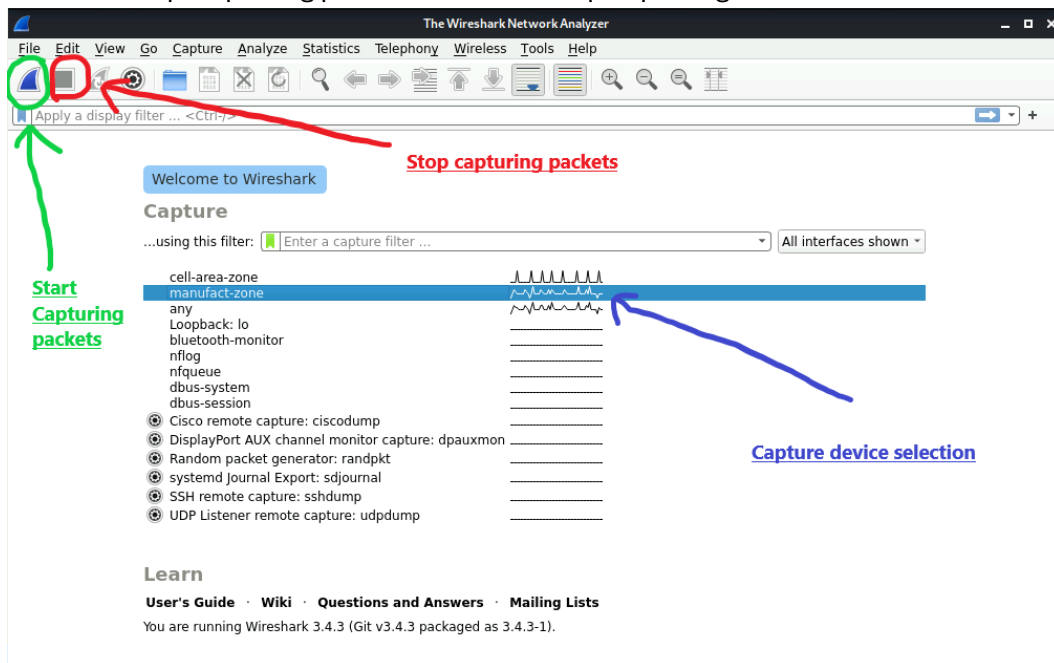


5. Click the Start Capturing packets button to begin capturing network data.

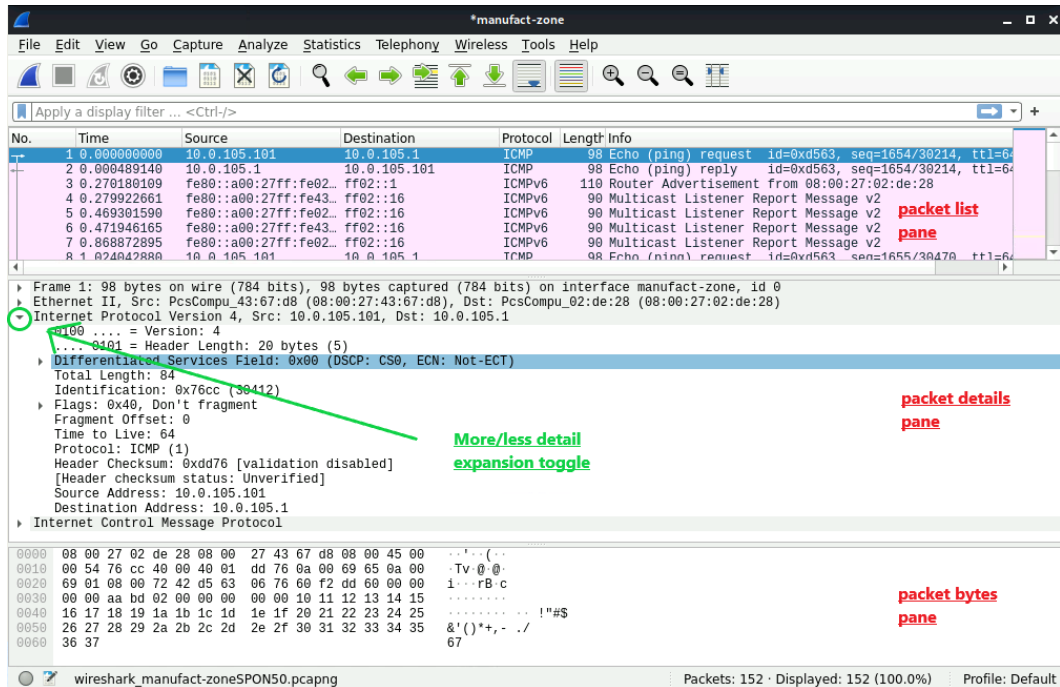


6. Let the system capture data for about 1 minute.

7. Click the Stop Capturing packets button to stop capturing network data.



8. Scroll through the list of packets in the top, packet list, pane and observe the type of data shown.
 - You should see that the data is ordered, contains a time stamp in relation to when the capture started, IP addressing information, the protocol being used, length of the packet and an overview of the data contained in the packet.



9. Scroll through the list of packets in the middle, packet details, pane and observe the type of data shown.

- In the packet details pane you will see detailed and decoded information about the packet selected in the packet list pane.
- You can expand and contract categories shown in the packet detail pane to view more or less detailed data regarding that category.

The image shows the Wireshark network protocol analyzer interface. The top pane, 'packet list pane', displays a list of captured packets. The middle pane, 'packet details pane', shows the hierarchical structure of the selected packet (Frame 1: 98 bytes on wire). The bottom pane, 'packet bytes pane', shows the raw data of the selected packet in hexadecimal and ASCII. A green arrow points to the 'More/less detail expansion toggle' in the packet details pane.

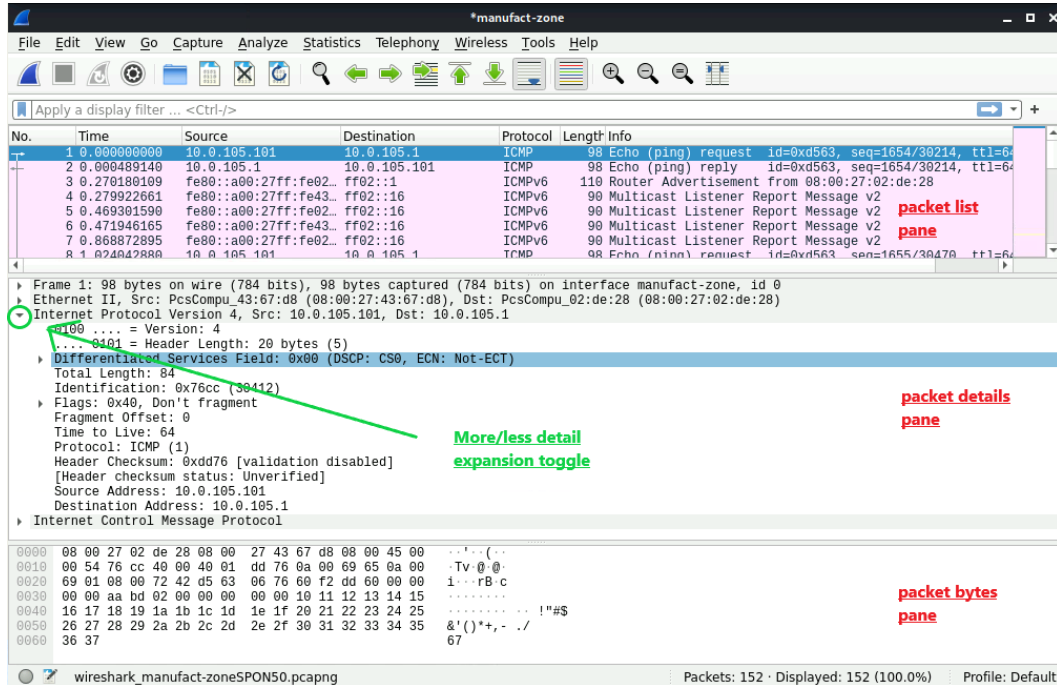
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.105.101	10.0.105.1	ICMP	98	Echo (ping) request id=0xd563, seq=1654/30214, ttl=64
2	0.000489140	10.0.105.1	10.0.105.101	ICMP	98	Echo (ping) reply id=0xd563, seq=1654/30214, ttl=64
3	0.270180109	fe80::a00:27ff:fe02::1	ff02::1	ICMPv6	118	Router Advertisement from 08:00:27:02:de:28
4	0.279922661	fe80::a00:27ff:fe02::1	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
5	0.469301590	fe80::a00:27ff:fe02::1	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
6	0.471946165	fe80::a00:27ff:fe02::1	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
7	0.868872895	fe80::a00:27ff:fe02::1	ff02::1	ICMPv6	90	Multicast Listener Report Message v2
8	1.024042880	10.0.105.101	10.0.105.1	ICMP	98	Echo (ping) request id=0xd563, seq=1655/30470, ttl=64

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface manufact-zone, id 0
Ethernet II, Src: PcsCompu_43:67:d8 (08:00:27:43:67:d8), Dst: PcsCompu_02:de:28 (08:00:27:02:de:28)
Internet Protocol Version 4, Src: 10.0.105.101, Dst: 10.0.105.1
... = Version: 4
... = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x76cc (30412)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xdd76 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.105.101
Destination Address: 10.0.105.1
Internet Control Message Protocol

0000 08 00 27 02 de 28 08 00 27 43 67 d8 08 00 45 00 ...
0010 00 54 76 cc 40 00 40 01 dd 76 8a 00 69 65 0a 00 -Tv @ @
0020 69 01 08 00 72 42 d5 63 06 76 60 f2 dd 60 00 00 1...rB c
0030 00 00 aa bd 02 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !"#
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./
0060 36 37 67

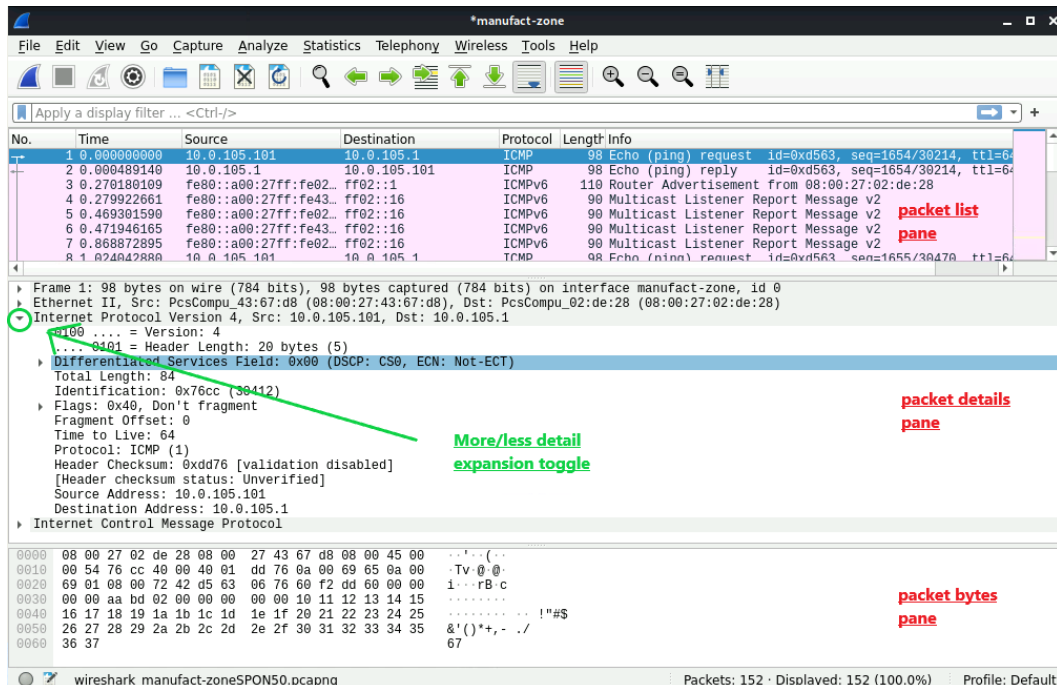
10. Scroll through the list of packets in the bottom, packet bytes, pane and observe the type of data shown (Example).

- The packet bytes pane shows the raw binary data shown in hexadecimal format.
- The packet bytes pane automatically highlights the raw data associated with any decoded detail data selected in the packet detail pane.



11. Note that you can use the bar separating the packet list, packet details and packet bytes panes to resize the pane and control how much data is shown in each pane.

12. Take a screen shot showing the entire Wireshark window (Example) and paste it into the lab form.

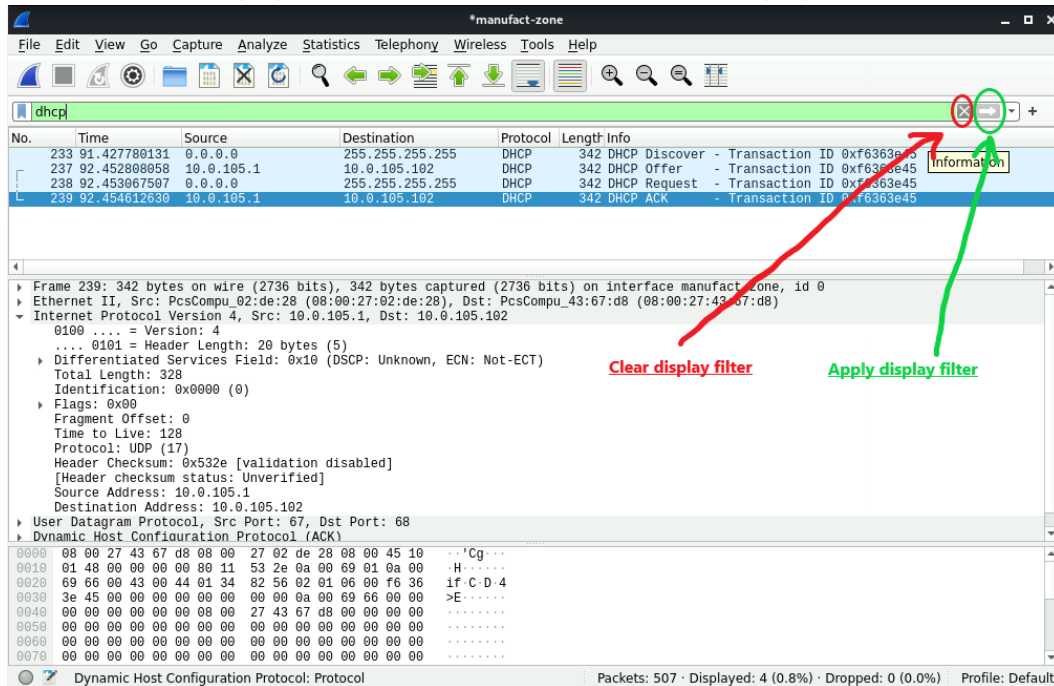


Part 5

Use Wireshark's protocol follow stream option to capture plain text data

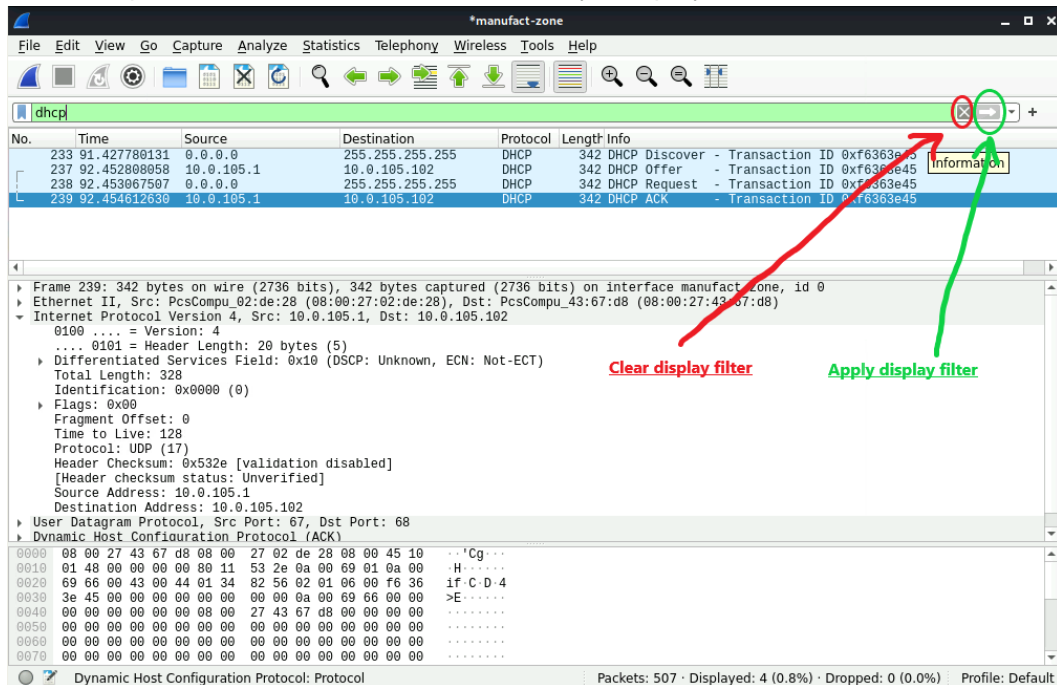
In this part of the lab, you will use Wireshark's follow stream functionality to demonstrate how to collect, decode and view related network traffic in a single window.

1. Click the Clear display filter button to remove the current display filter.

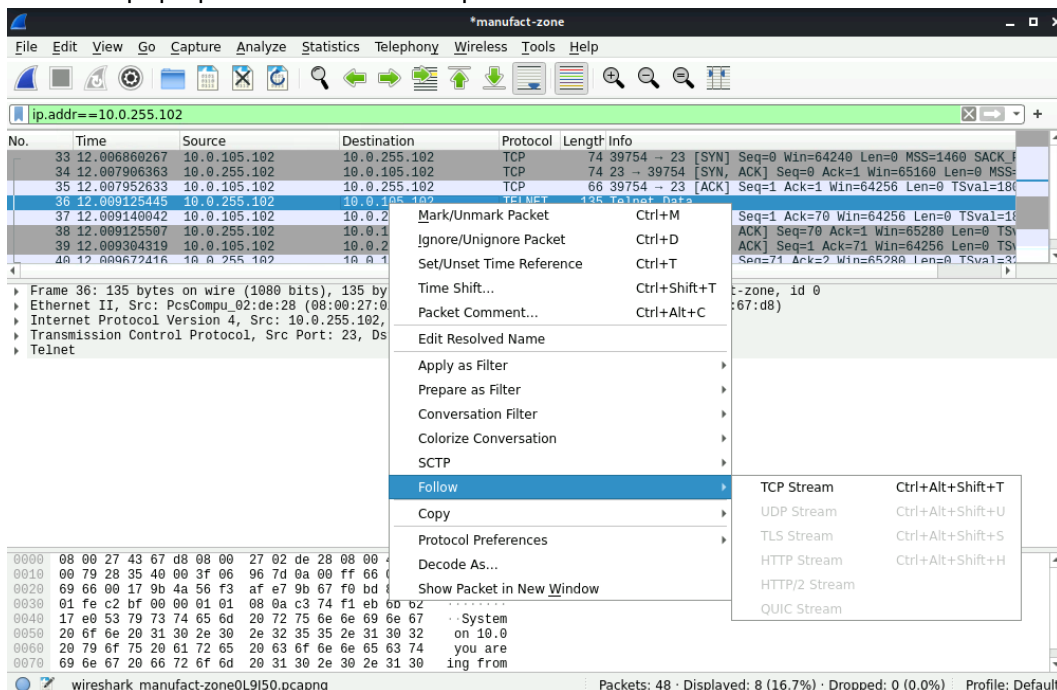


2. Start capturing network traffic by clicking on the Start Capturing packets button then clicking the Continue without Saving button.
3. Open a new terminal (command prompt) window by clicking the Terminal Emulator button found at the upper left hand corner of the window.
4. Connect to the PLC by typing the command **nc 10.0.255.102 23**.
 - The nc command starts the netcat program which is useful network utility that allows a quick connection to network services. In this case netcat is connecting to the telnet service running on the PLC.
5. Type the command **exit** to end the terminal session.
6. Return to the Wireshark window.
7. Stop capturing network traffic by clicking on the Stop Capturing packets button.

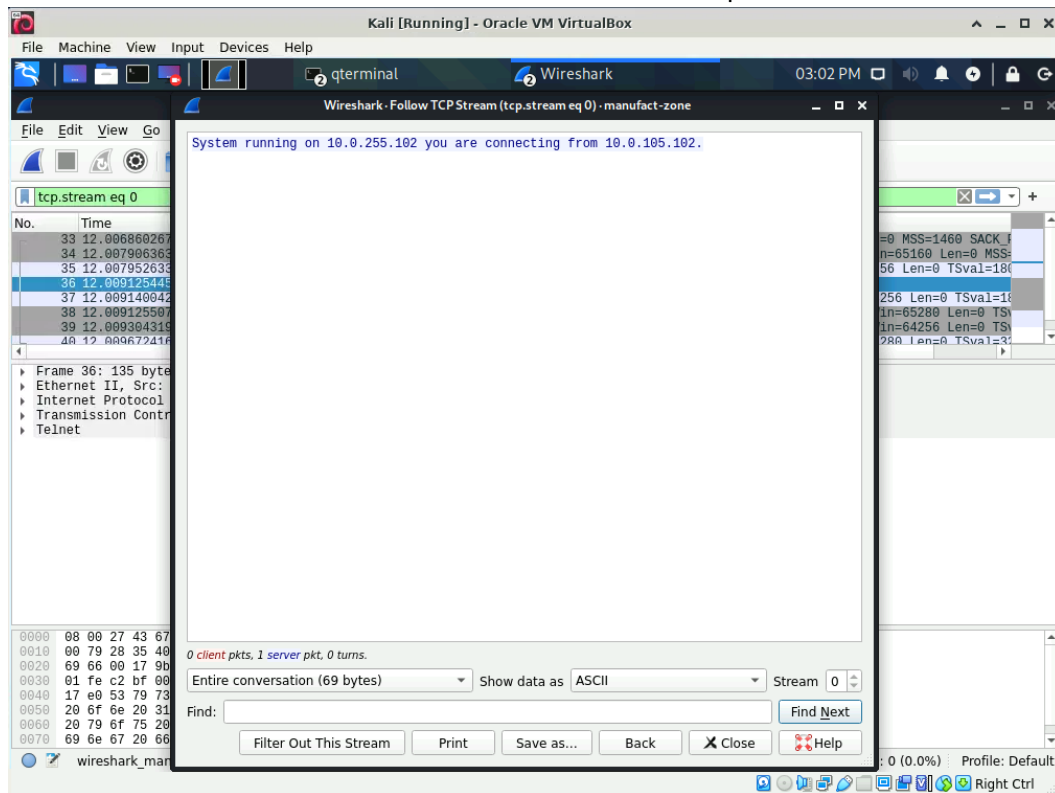
8. Click in the display filter field, type `ip.addr==10.0.255.102` then click the Apply display filter button or press <ENTER> to activate the filter (Example).



9. Right click any packet in the packet list pane which is using the TELNET protocol.
10. From the pop up menu choose the option Follow -> TCP Stream.



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



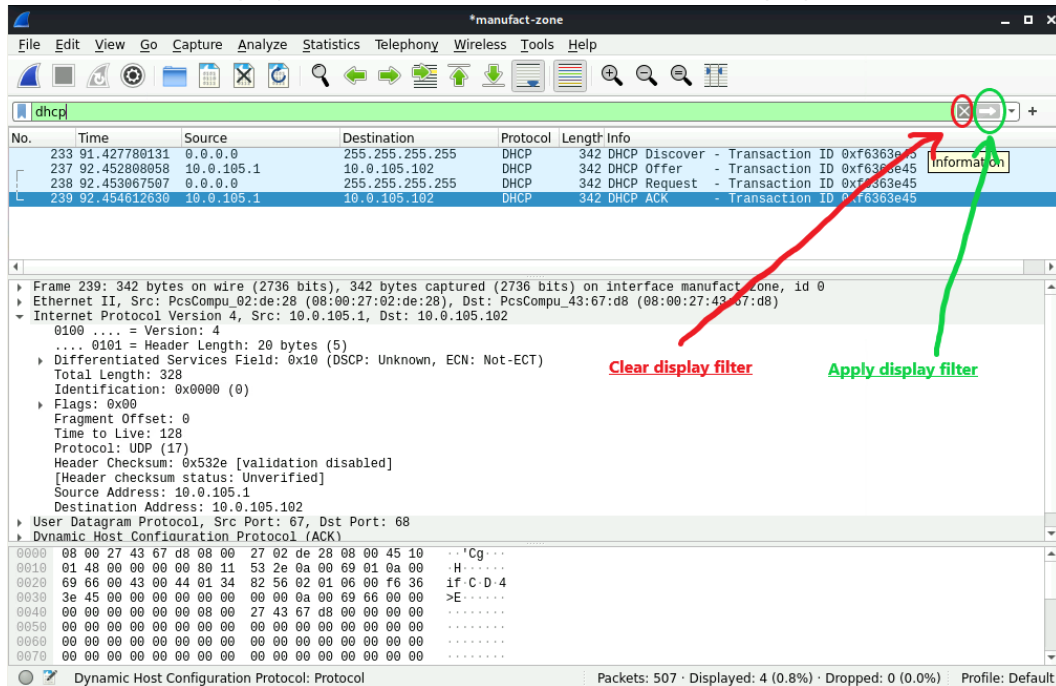
Part 6

Use Wireshark to analyze a previously saved data capture

In this part of the lab, you will use Wireshark to analyze a pcap data file which contains a connection to a web server using the HTTP and HTTPS protocols.

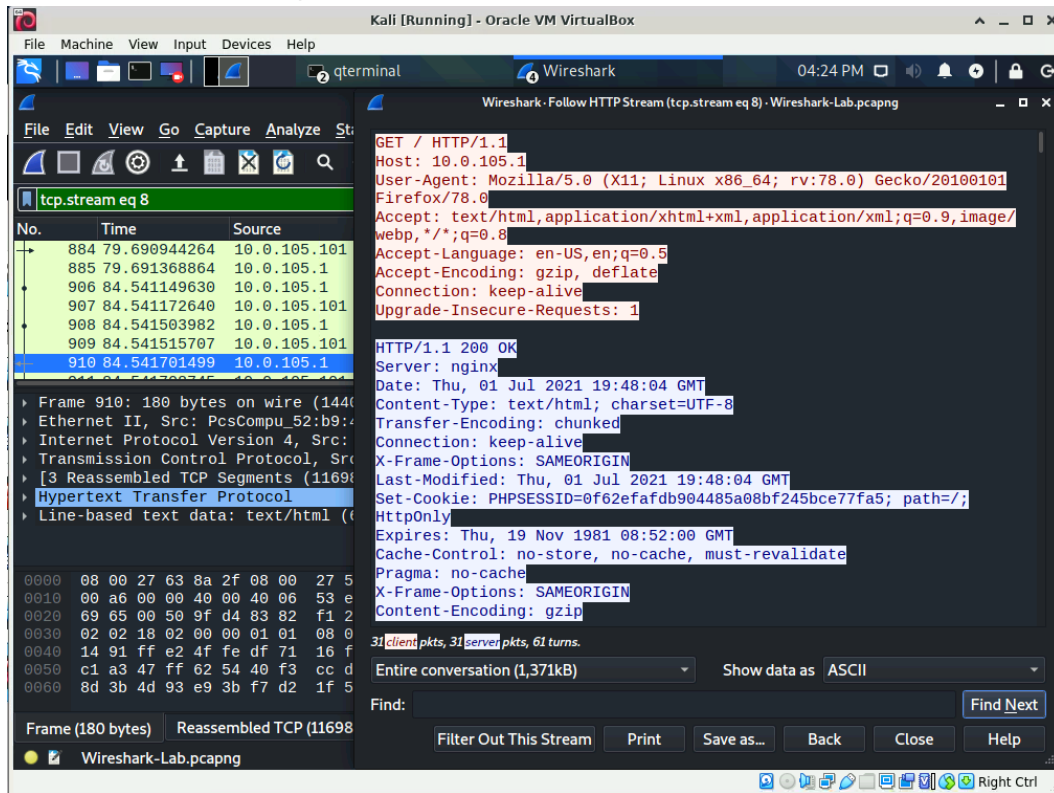
1. Close the Follow TCP Stream window

- Click the Clear display filter button to remove the current display filter.



- From the File menu in Wireshark choose the Open option.
- Navigate to the /home/student/labs/wireshark directory then open the Wireshark-Lab.pcapng capture file.
- Click the Continue without Saving button.
- Create and apply a display filter which will show only http traffic.
- Use the follow HTTP Stream option to follow the stream associated with any of the filtered packets going to or coming from the IP address 10.0.105.1 which also uses the HTTP protocol.
 - Make certain to follow the HTTP protocol and not the OCSP protocol.
- Take a minute or two and view the data displayed.

9. Ensure that some data from the http stream is shown, take a screen shot that shows the entire Kali window and paste it into the lab form.



10. Close the Follow HTTP Stream window.
11. Remove the current display filter.
12. Create and apply a display filter which will show only traffic associated with HTTPS traffic using TCP port 443.
 - The filter you should use is tcp.port==443
13. Use the follow TCP Stream option to follow the stream associated with any of the filtered packets going to or coming from the IP address 10.0.105.1 which also uses the TCP protocol.
14. Take a minute or two and view the data displayed.
15. Answer the final question found in the lab form.
16. To end the lab, restart the ICS Lab Control program from the Desktop if necessary, select the Pause/End Lab option, click the OK button then wait for the systems to stop.