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:

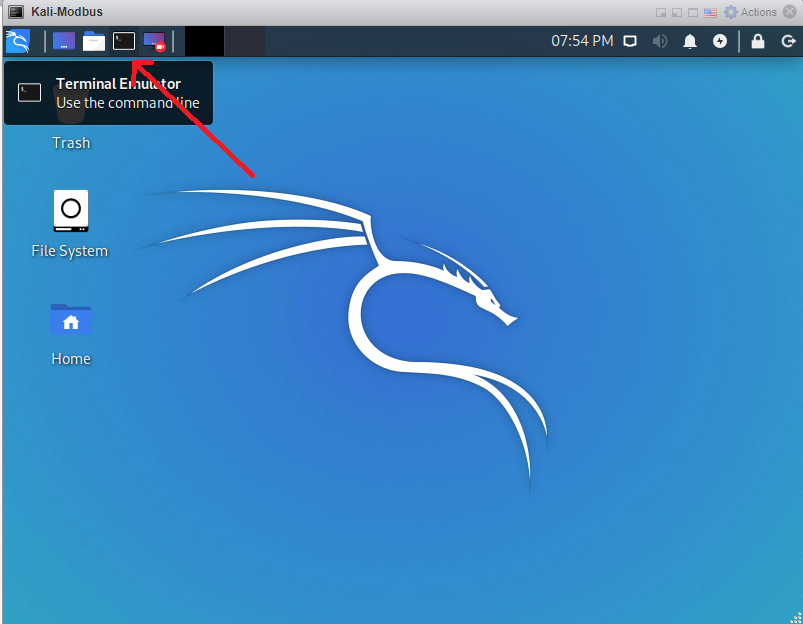
* Security Appliance
* Sensor
* PLC
* OPC
* HMI
* Kali

## 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.



1. Type the command **nmcli connection** to view the available network connections.
2. Notice that the Cell-Area Zone configuration is associated with a device but the Manufacturing Zone configuration is not.
3. Type the letter **q** to stop viewing the network configurations.
4. 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.

1. View the available network configurations by typing the command **nmcli connection**.
2. Notice that now the Manufacturing Zone configuration is associated with a device but the Cell-Area Zone configuration is not.
3. 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.

1. After the Wireshark program starts select the manufact-zone network device to indicate that you wish to capture data on that device.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

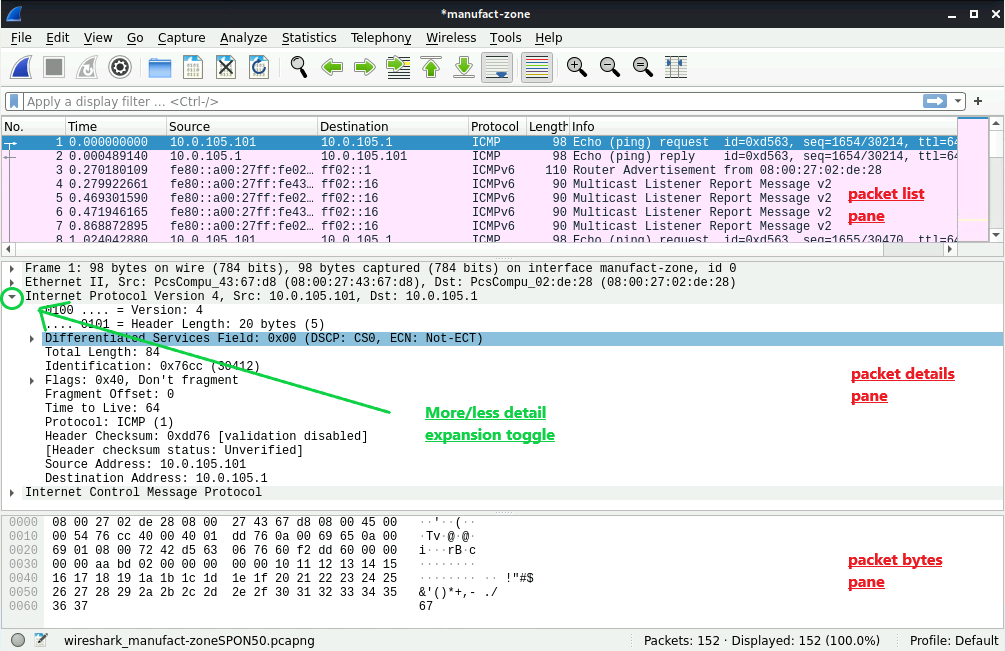
1. Let the system capture data for about 1 minute.
2. Click the Stop Capturing packets button to stop capturing network data.

A screenshot of a computer

Description automatically generated

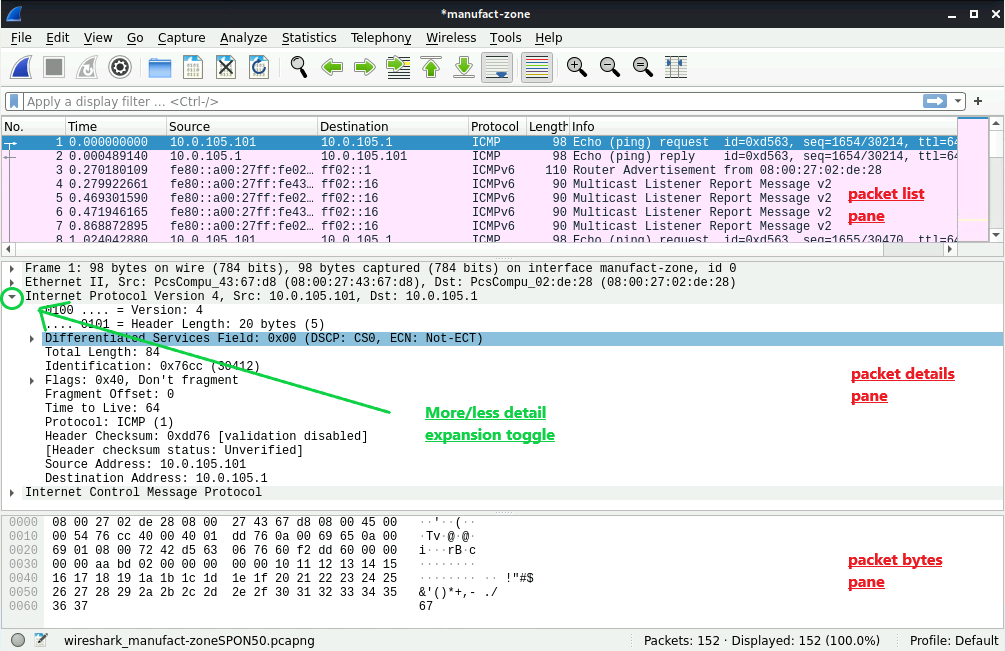
1. Scroll through the list of packets in the top, packet list, pane and observe the type of data shown.

* 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.



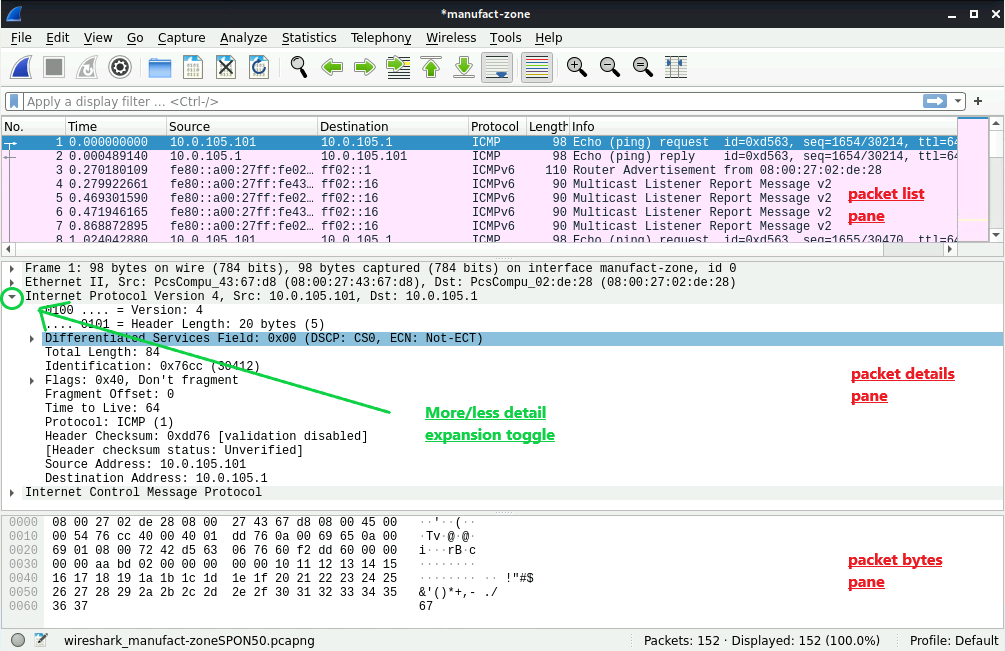
1. Scroll through the list of packets in the middle, packet details, pane and observe the type of data shown.

* 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.

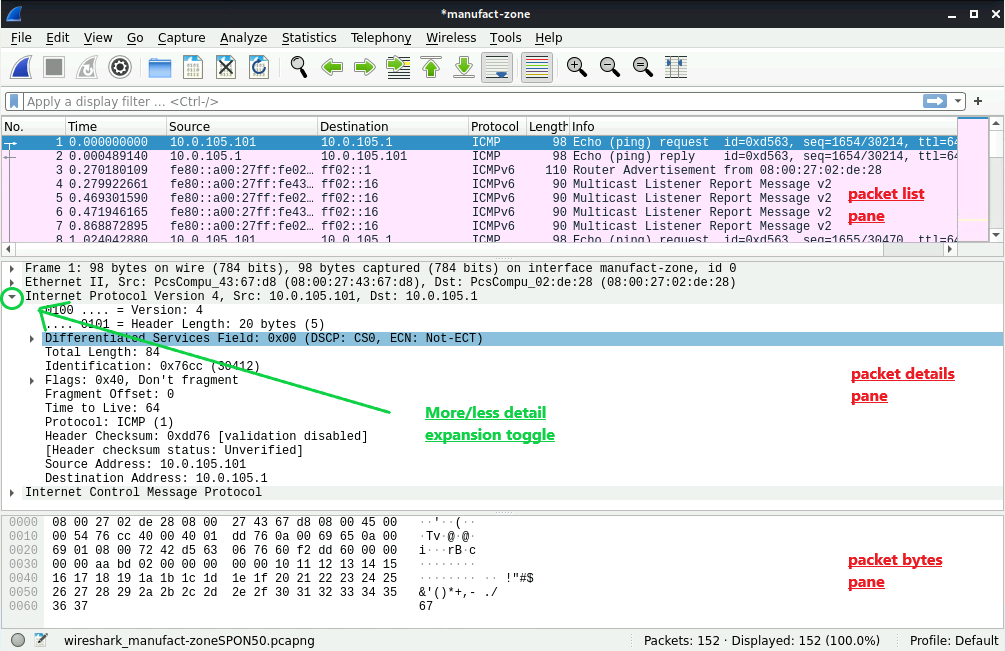


1. Scroll through the list of packets in the bottom, packet bytes, pane and observe the type of data shown (Example).

* 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.



1. 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.
2. Take a screen shot showing the entire Wireshark window (Example) and paste it into the lab form.

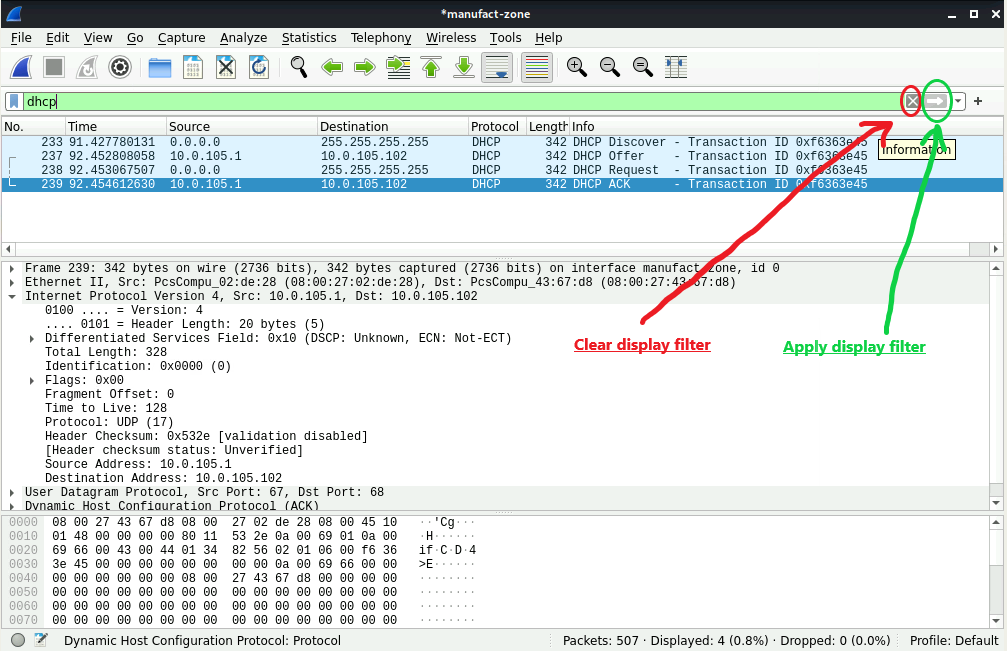


## Part 5

### 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.

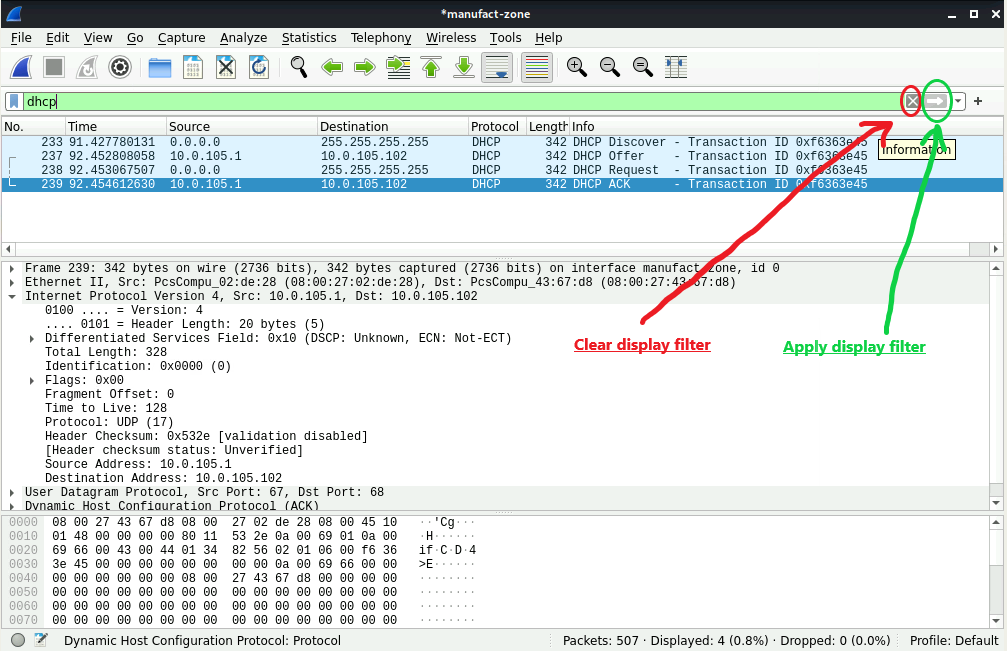
1. Click the Clear display filter button to remove the current display filter.



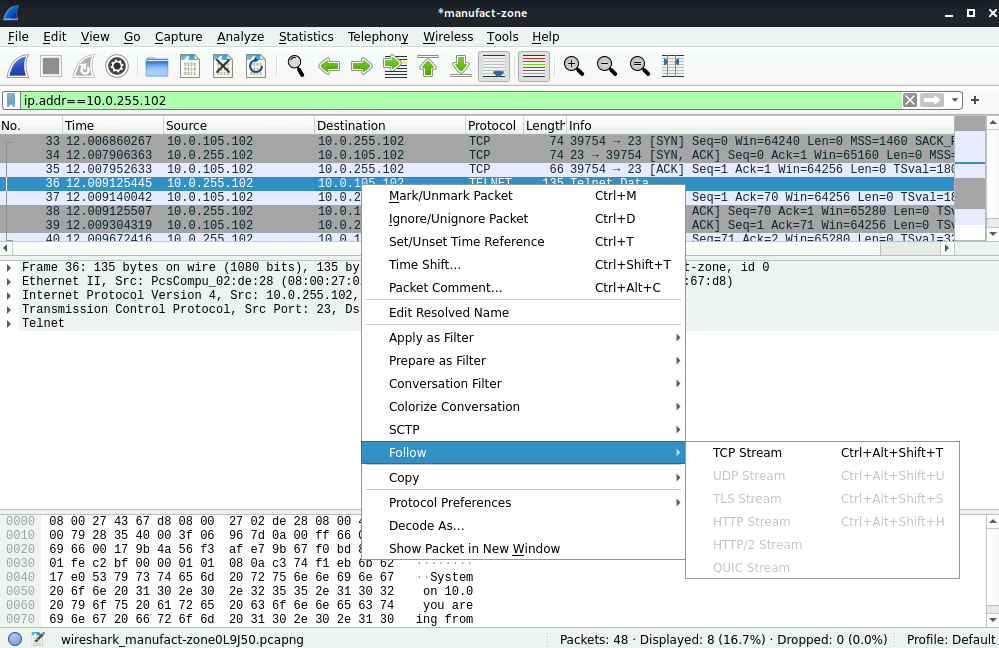
1. Start capturing network traffic by clicking on the Start Capturing packets button then clicking the Continue without Saving button.
2. Open a new terminal (command prompt) window by clicking the Terminal Emulator button found at the upper left hand corner of the window.
3. Connect to the PLC by typing 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.

1. Type the command **exit** to end the terminal session.
2. Return to the Wireshark window.
3. Stop capturing network traffic by clicking on the Stop Capturing packets button.
4. 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).



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



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

A screenshot of a computer

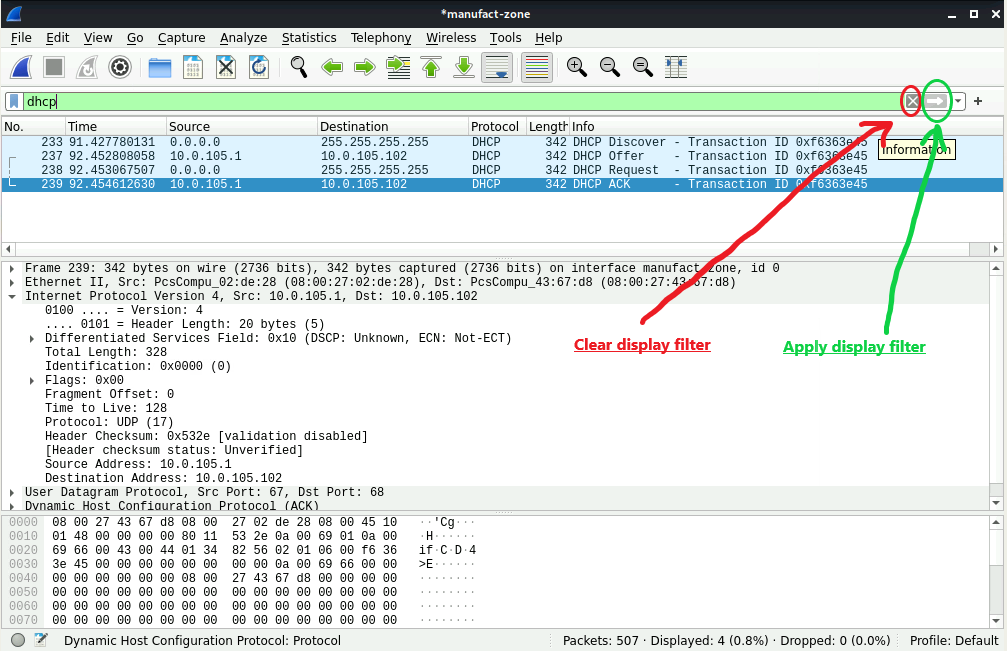
Description automatically generated

## 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.

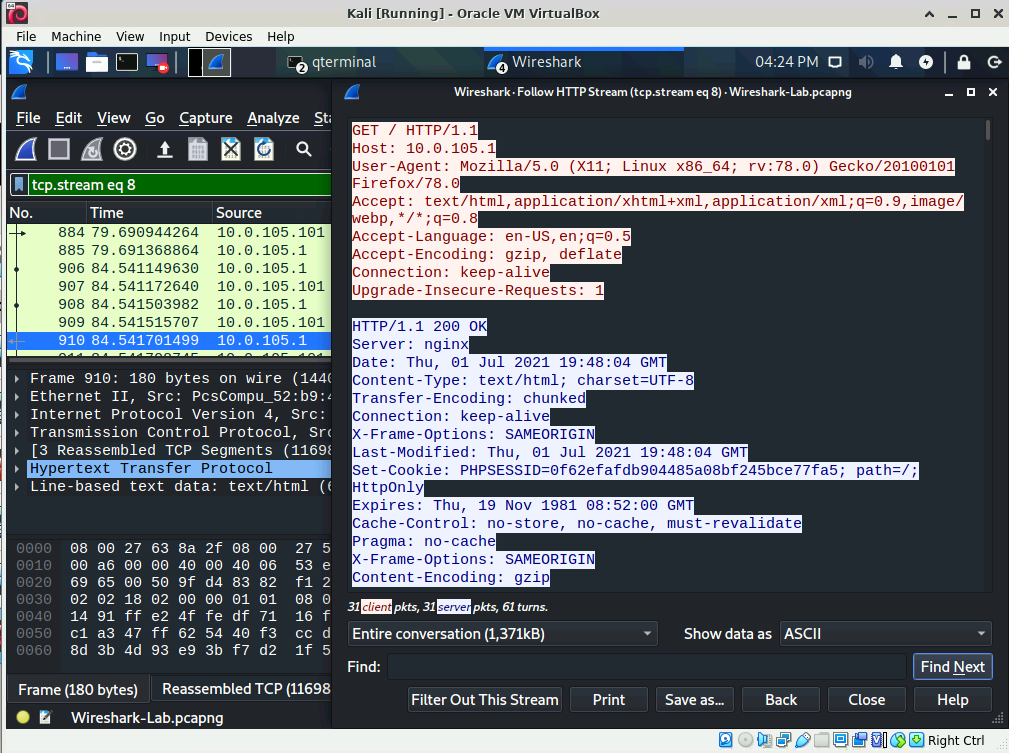
1. Close the Follow TCP Stream window
2. Click the Clear display filter button to remove the current display filter.



1. From the File menu in Wireshark choose the Open option.
2. Navigate to the /home/student/labs/wireshark directory then open the Wireshark-Lab.pcapng capture file.
3. Click the Continue without Saving button.
4. Create and apply a display filter which will show only http traffic.
5. 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.

1. Take a minute or two and view the data displayed.
2. 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.



1. Close the Follow HTTP Stream window.
2. Remove the current display filter.
3. 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

1. 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.
2. Take a minute or two and view the data displayed.
3. Answer the final question found in the lab form.
4. 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.