Lab 9.1.3 Using Wireshark to Observe the TCP Three-way Handshake

Objectives

- Use Wireshark to monitor an Ethernet interface for recording packet flows
- Generate a TCP connection using a web browser
- Observe the initial TCP/IP three-way handshake

Background / Preparation

In this lab, you use the Wireshark network packet analyzer (also called a packet sniffer) to view the TCP/IP packets generated by the TCP three-way handshake. When an application that uses TCP first starts on a host, the protocol uses the three-way handshake to establish a reliable TCP connection between two hosts. You will observe the initial packets of the TCP flow: the SYN packet, then the SYN ACK packet, and finally the ACK packet.

Caution: Installing or using a packet sniffer application may be considered a breach of the security policy of an organization, leading to serious legal and financial consequences. It is recommended that permission is obtained before downloading, installing, or running a packet sniffer application.

Note: The term “packet” is used in this lab. Wireshark actually captures Ethernet frames, which contain IP packets. The Wireshark application uses the term “frame” when analyzing captures. The two terms are often used interchangeably, but recall that a frame is a Data Link Layer 2 encapsulation package, and a packet is a Network Layer 3 encapsulation.

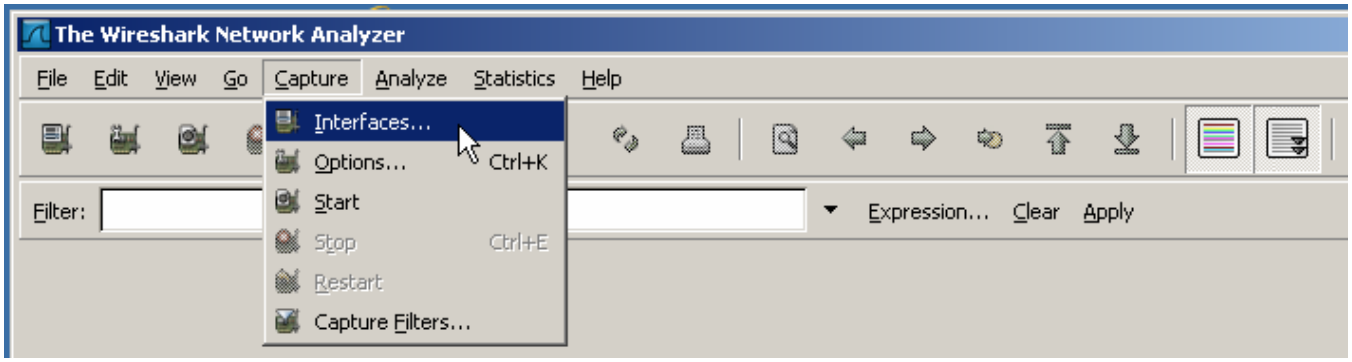
Task 1: Prepare Wireshark to Capture Packets

Step 1: Start Wireshark.

Double-click the Wireshark icon, which is located on the desktop.

Step 2: Select an interface to use for capturing packets.

a. From the Capture menu, choose **Interfaces**.

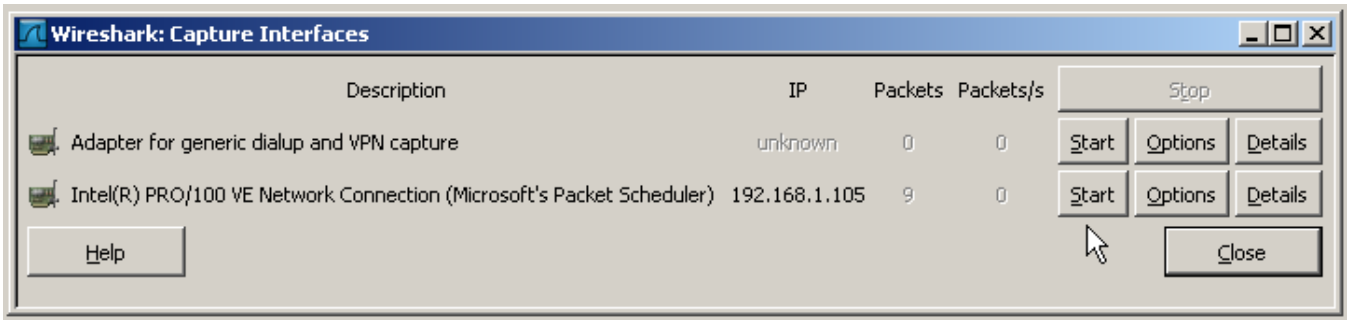


Step 3: Start a network capture.

a. Choose the local network Ethernet interface adapter for capturing network traffic. Click the **Start** button of the chosen interface.

b. Write down the IP address associated with the selected Ethernet adapter, because that is the source IP address to look for when examining captured packets.

The host IP address: 192.168.1.105



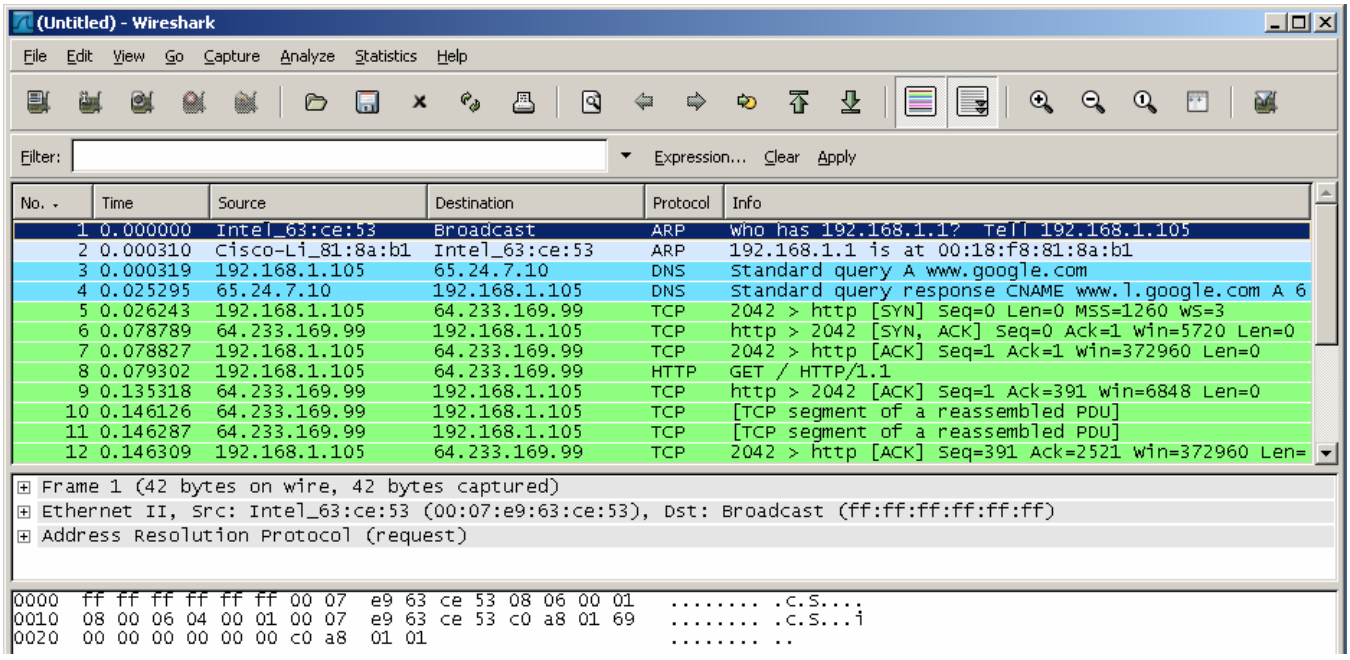
Task 2: Generate and Analyze Captured Packets

Step 1: Open a browser and access a website.

a. Go to www.google.com. Minimize the Google window, and return to Wireshark. You should see captured traffic similar to that shown below.

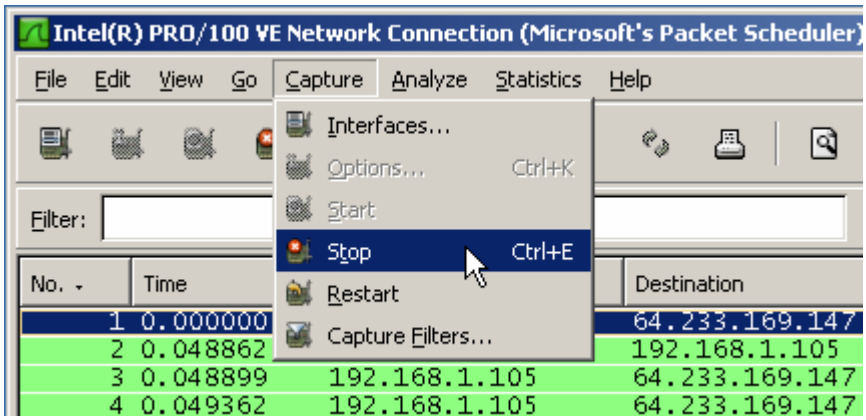
Note: Your instructor may provide you with a different website. If so, enter the website name or address here:
www.google.com

b. The capture windows are now active. Locate the Source, Destination, and Protocol columns on the Wireshark display screen. The HTTP data that carries web page text and graphics uses TCP for reliability.



Step 2: Stop the capture.

From the Wireshark Capture menu, choose **Stop**.



Step 3: Analyze the captured output.

If the computer was recently started and there has been no activity in accessing the Internet, you can see the entire process in the captured output, including ARP, DNS, and the TCP three-way handshake.

The capture screen in Task 2, Step 1 shows all the packets the computer needs to get to a website, starting with the initial ARP for the gateway router interface MAC address. (Your screen capture may vary.)

a. In the screen capture, the process starts with frame 1, which is an ARP broadcast from the source computer to determine the MAC address of the router default gateway. The gateway is the local LAN Fast Ethernet interface on the router. The computer needs to resolve the default gateway IP address to the interface MAC address before it can send the first frame or packet to the router.

   What is the IP address of the router default gateway? 192.168.1.1

b. The second frame is the reply from the router telling the computer the MAC address of its Fast Ethernet interface.

   What is the MAC address? 00:18:f8:81:8a:ba

c. The third frame is a DNS query from the computer to the configured DNS server, attempting to resolve the domain name www.google.com to the IP address of the web server. The computer must have the IP address before it can send the first frame to the web server.

   What is the IP address of the DNS server that the computer queried? 65.24.7.10

d. The fourth frame is the response from the DNS server with the IP address of www.google.com. You need to scroll to the right to see the IP address of the Google server in the DNS response, but you can see it in the next frame.

e. The fifth frame is the start of the TCP three-way handshake [SYN].

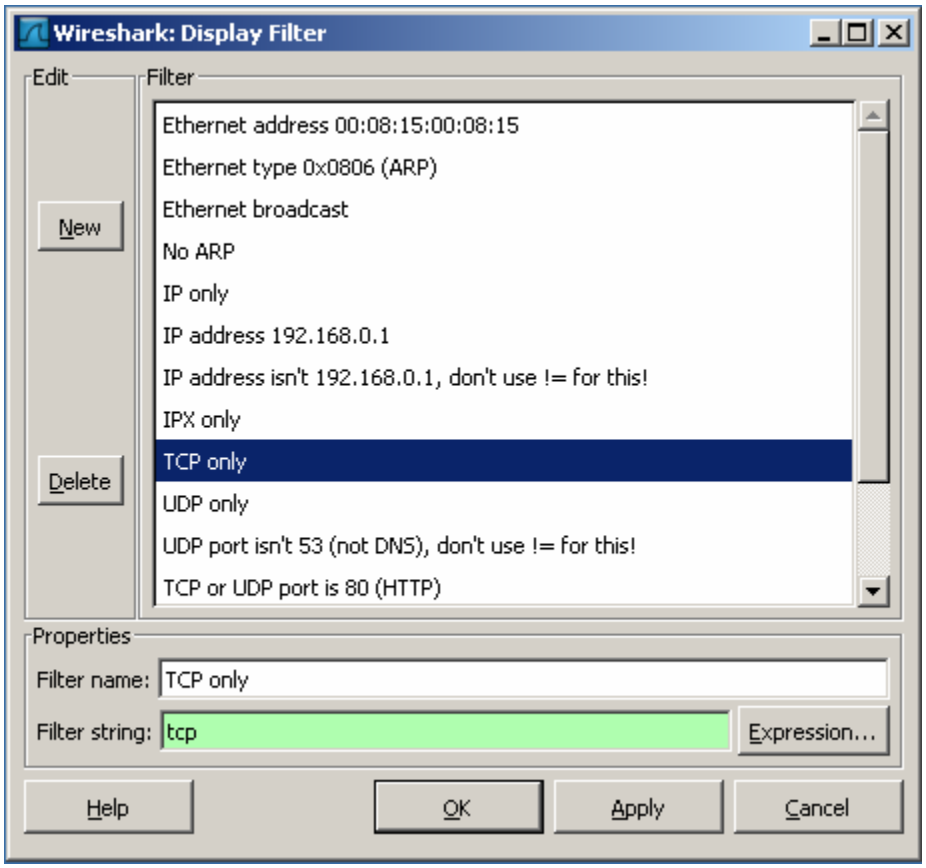
   What is the IP address of the Google web server? 64.233.169.99

Step 4: Filter the capture to view only TCP packets.

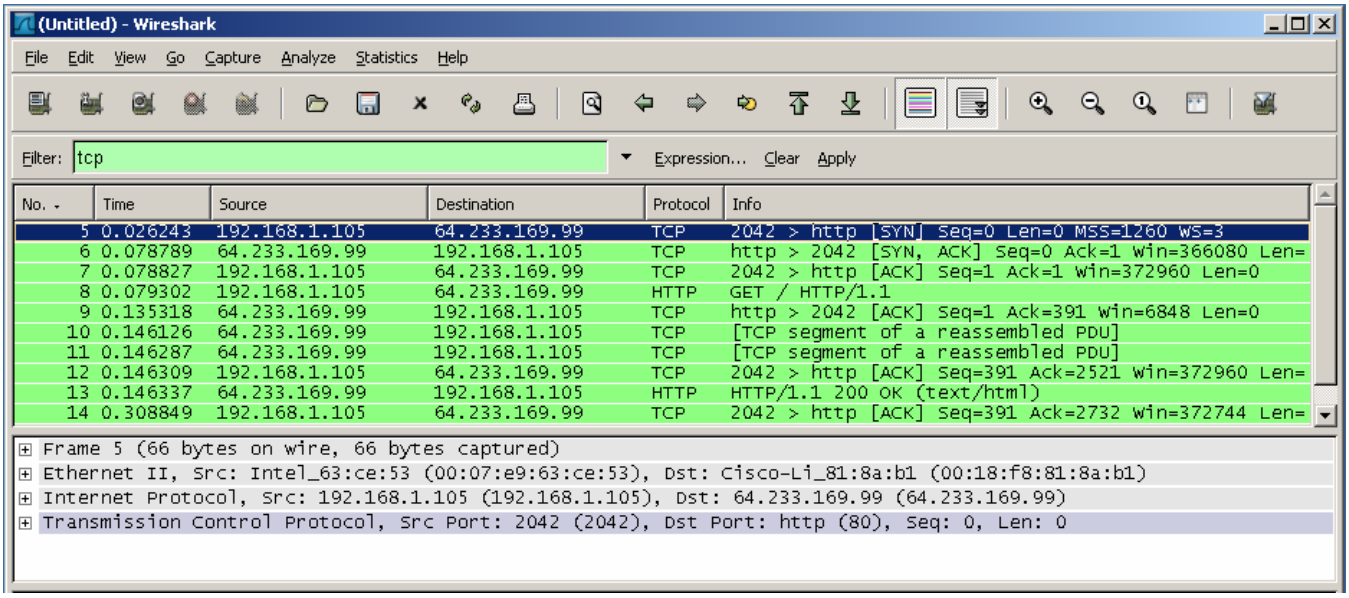
If you have many packets that are unrelated to the TCP connection, it may be necessary to use the Wireshark filter capability.

a. To use a preconfigured filter, click the **Analyze** menu option, and then click **Display Filters**.

b. In the **Display Filter** window, click **TCP only**, and then click **OK**.



c. In the Wireshark window, scroll to the first captured TCP packet. This should be the first packet in the flow.



d. In the Info column, look for three packets similar to the first three shown in the window above. The first TCP packet is the [SYN] packet from the initiating computer. The second is the [SYN, ACK]

response from the web server. The third packet is the [ACK] from the source computer, which completes the handshake.

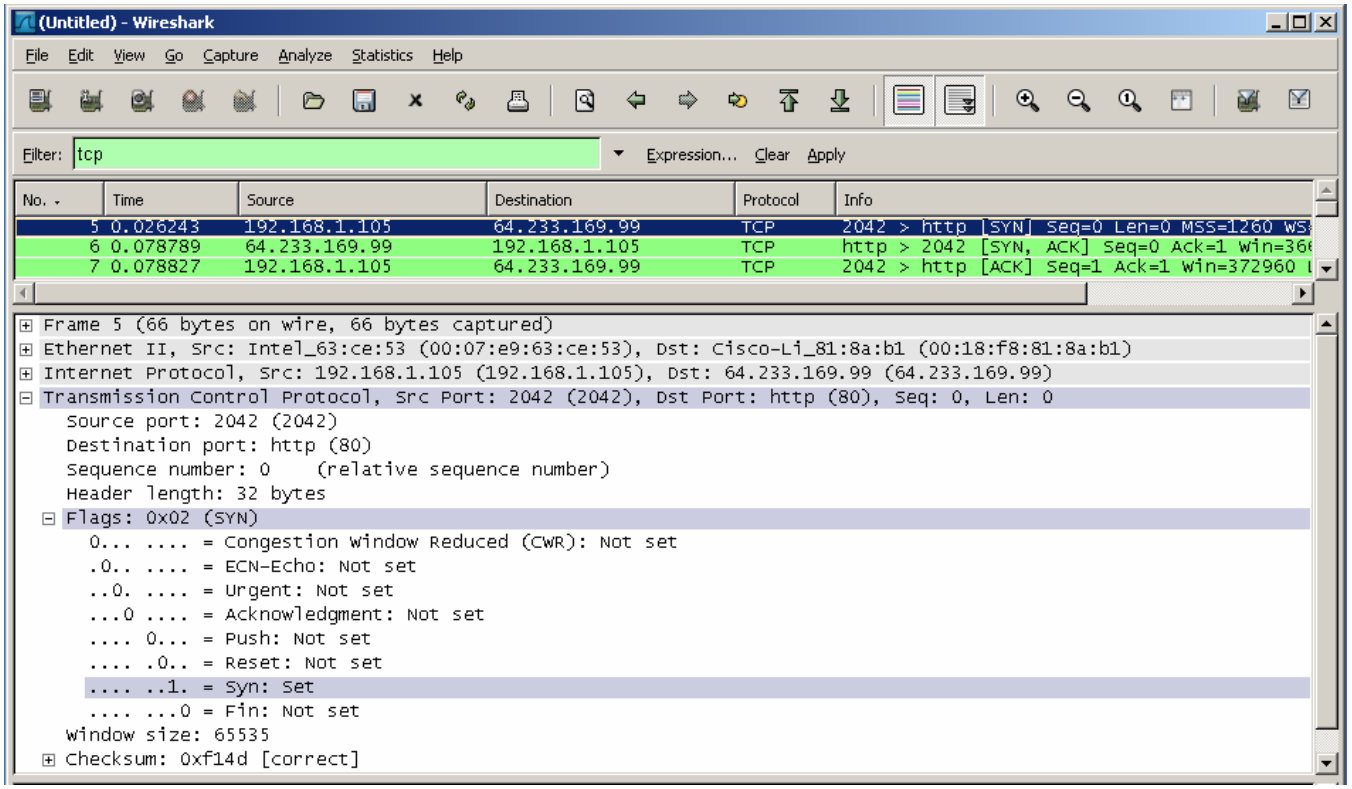
Step 5: Inspect the TCP initialization Sequence

a. In the top Wireshark window, click on the line containing the first packet identified in Step 4. This highlights the line and displays the decoded information from that packet in the two lower windows fill.

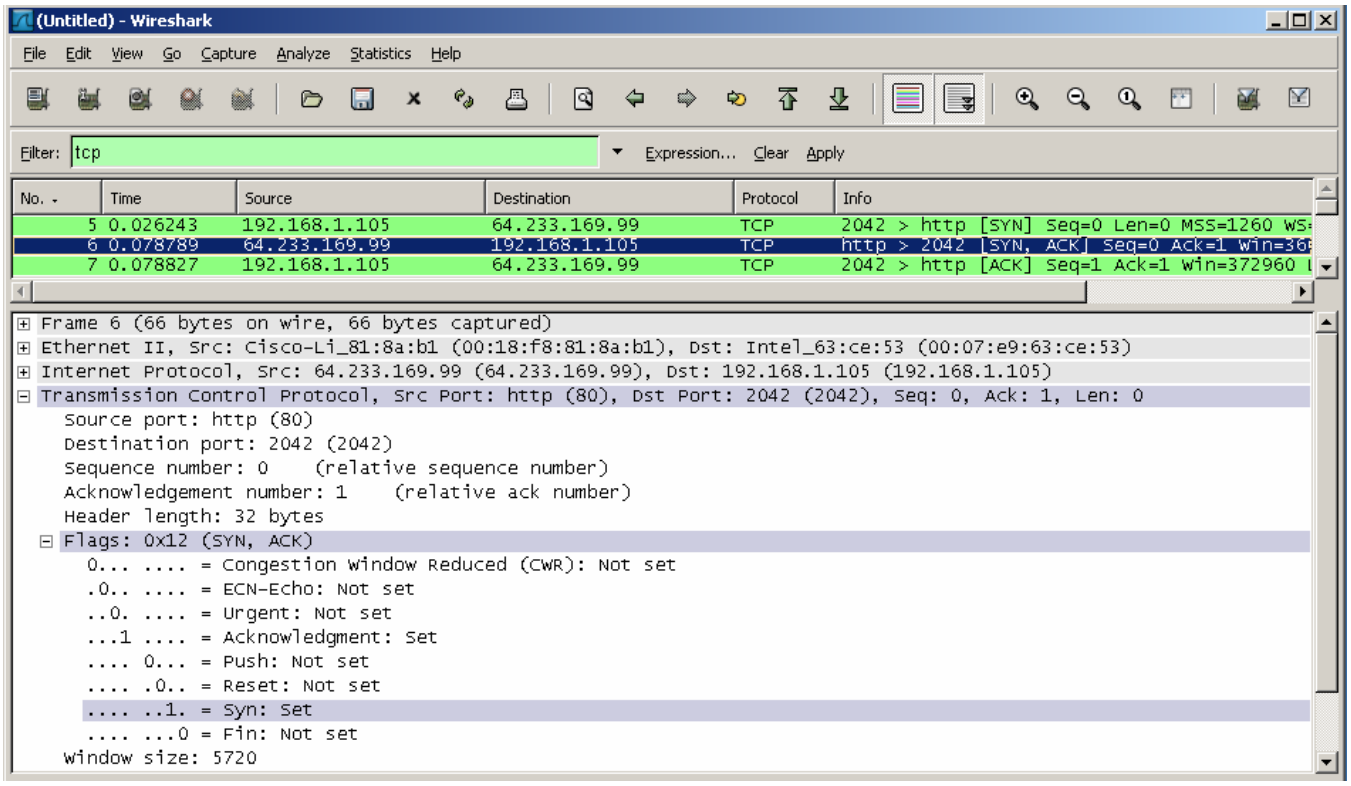
Note: The Wireshark windows below were adjusted to allow the information to be viewed in a compact size. The middle window contains the detailed decoding of the packet.

b. Click the **+** icon to expand the view of the TCP information. To contract the view, click the **–** icon.

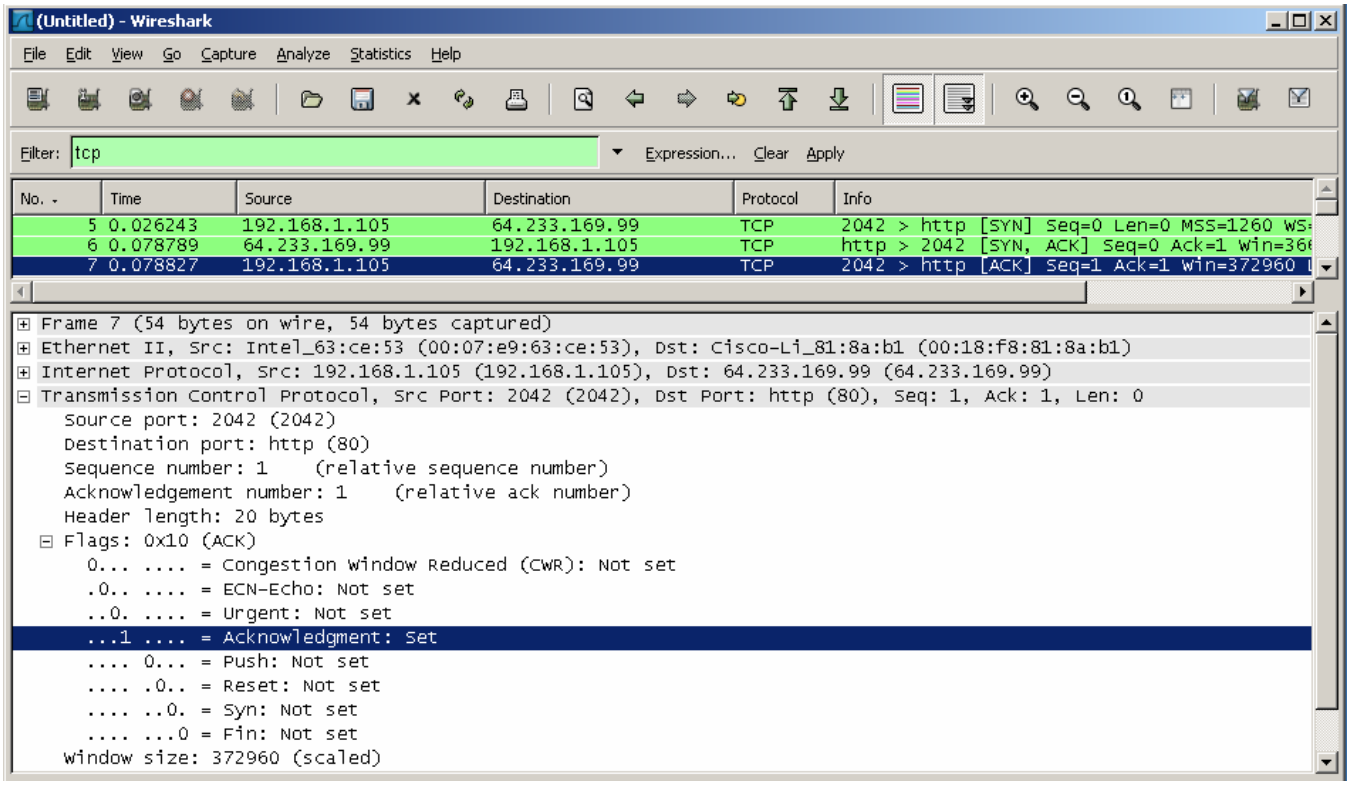
c. Notice in the first TCP packet that the relative sequence number is set to 0, and the SYN bit is set to 1 in the Flags field.



d. Notice in the second TCP packet of the handshake that the relative sequence number is set to 0, and the SYN bit and the ACK bit are set to 1 in the Flags field.



e. In the third and final frame of the handshake, only the ACK bit is set, and the sequence number is set to the starting point of 1. The acknowledgement number is also set to 1 as a starting point. The TCP connection is now established, and communication between the source computer and the web server can begin.



f. Close Wireshark.

Task 3: Reflection

a. There are hundreds of filters available in Wireshark. A large network could have numerous filters and many different types of traffic. Which three filters in the list might be the most useful to a network administrator? Wireshark's IP filters (isolating specific hosts), Protocol filters (TCP, DNS, ARP) and Port filters (TCP, UDP) would be most useful to a network administrator as the information would be useful for extensive troubleshooting

b. Is Wireshark a tool for out-of-band or in-band network monitoring? out-of-band

Explain your answer.

Wireshark is out-of-band as it does not interfere with actual traffic. It captures and analyzes copies of the network packets it listens to. As such performance and latency of the network are not negatively impacted.