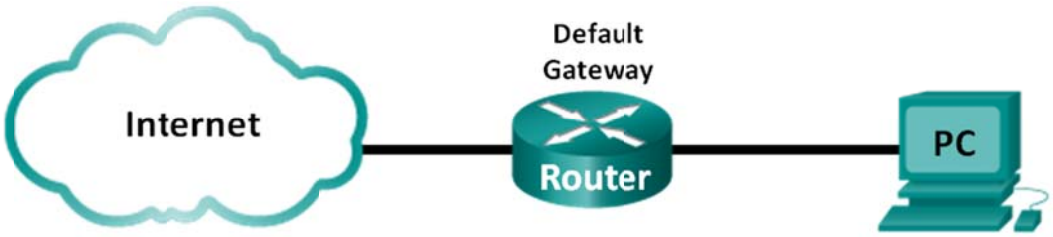
Lab - Using Wireshark to Observe the TCP 3-Way Handshake

Topology



Objectives

Part 1: Prepare Wireshark to Capture Packets

- Select an appropriate NIC interface to capture packets.

Part 2: Capture, Locate, and Examine Packets

- Capture a web session to www.google.com.
- Locate appropriate packets for a web session.
- Examine information within packets, including IP addresses, TCP port numbers, and TCP control flags.

Background / Scenario

In this lab, you will use Wireshark to capture and examine packets generated between the PC browser using the HyperText Transfer Protocol (HTTP) and a web server, such as www.google.com. When an application, such as HTTP or File Transfer Protocol (FTP) first starts on a host, TCP uses the three-way handshake to establish a reliable TCP session between the two hosts. For example, when a PC uses a web browser to surf the Internet, a three-way handshake is initiated and a session is established between the PC host and web server. A PC can have multiple, simultaneous, active TCP sessions with various web sites.

Note: This lab cannot be completed using Netlab. This lab assumes that you have Internet access.

Required Resources

1 PC (Windows 7, Vista, or XP with a command prompt access, Internet access, and Wireshark installed)

Part 1: Prepare Wireshark to Capture Packets

In Part 1, you start the Wireshark program and select the appropriate interface to begin capturing packets.

Step 1: Retrieve the PC interface addresses.

For this lab, you need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

a. Open a command prompt window, type **ipconfig /all** and then press Enter.

```
Physical Address. . . . . : C8-0A-A9-FA-DE-0D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.130(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 01, 2012 1:43:35 PM
Lease Expires . . . . . : Sunday, December 02, 2012 1:43:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

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

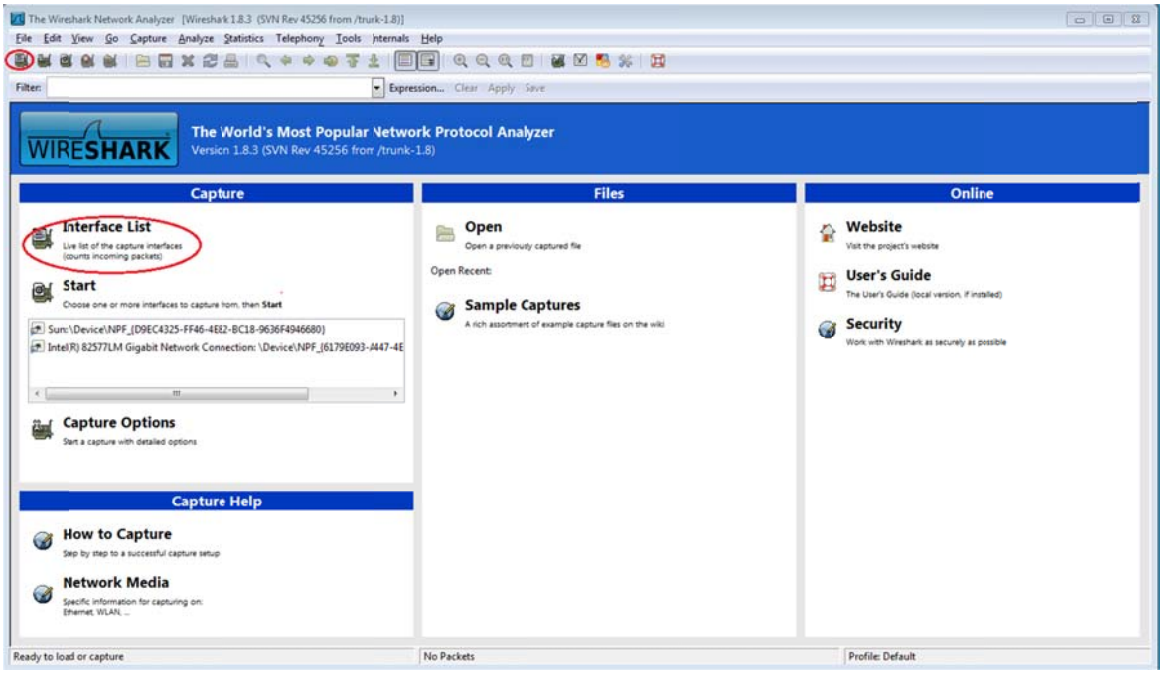
The PC host IP address:

The PC host MAC address:

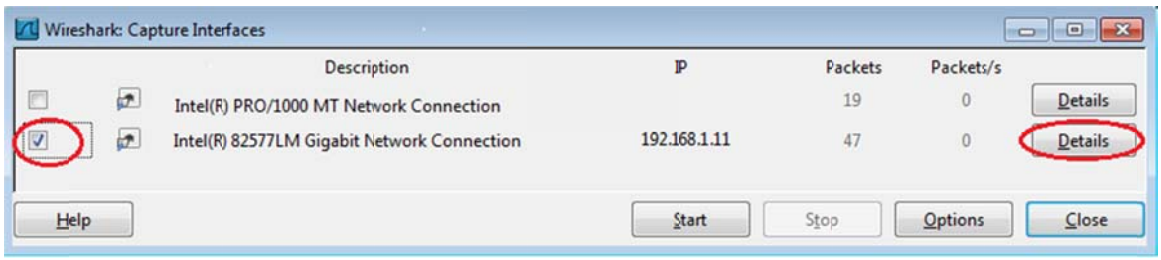
Step 2: Start Wireshark and select the appropriate interface.

a. Click the Windows **Start** button and on the pop-up menu, double-click **Wireshark**.

b. After Wireshark starts, click **Interface List**.



c. In the **Wireshark: Capture Interfaces** window, click the check the box next to the interface connected to your LAN.



Note: If multiple interfaces are listed and you are unsure which interface to check, click **Details**. Click the **802.3 (Ethernet)** tab, and verify that the MAC address matches what you wrote down in Step 1b. Close the Interface Details window after verification.

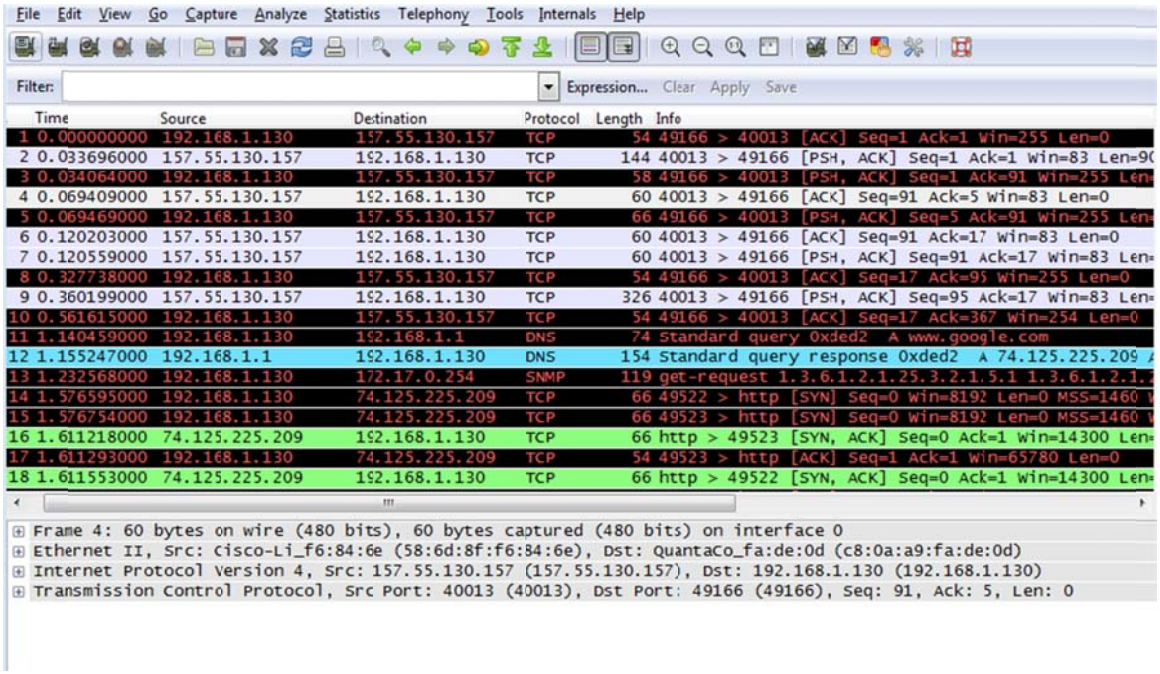
Part 2: Capture, Locate, and Examine Packets

Step 1: Click the Start button to start the data capture.

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

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

b. The capture window is now active. Locate the **Source**, **Destination**, and **Protocol** columns.



Step 2: Locate appropriate packets for the web session.

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 the Address Resolution Protocol (ARP), Domain Name System (DNS), and the TCP three-way handshake. The capture screen in Part 2, Step 1 shows all the packets the computer must get to www.google.com. In this case, the PC already had an ARP entry for the default gateway; therefore, it started with the DNS query to resolve www.google.com.

a. Frame 11 shows the DNS query from the PC to the DNS server, attempting to resolve the domain name, www.google.com to the IP address of the web server. The PC must have the IP address before it can send the first packet to the web server.

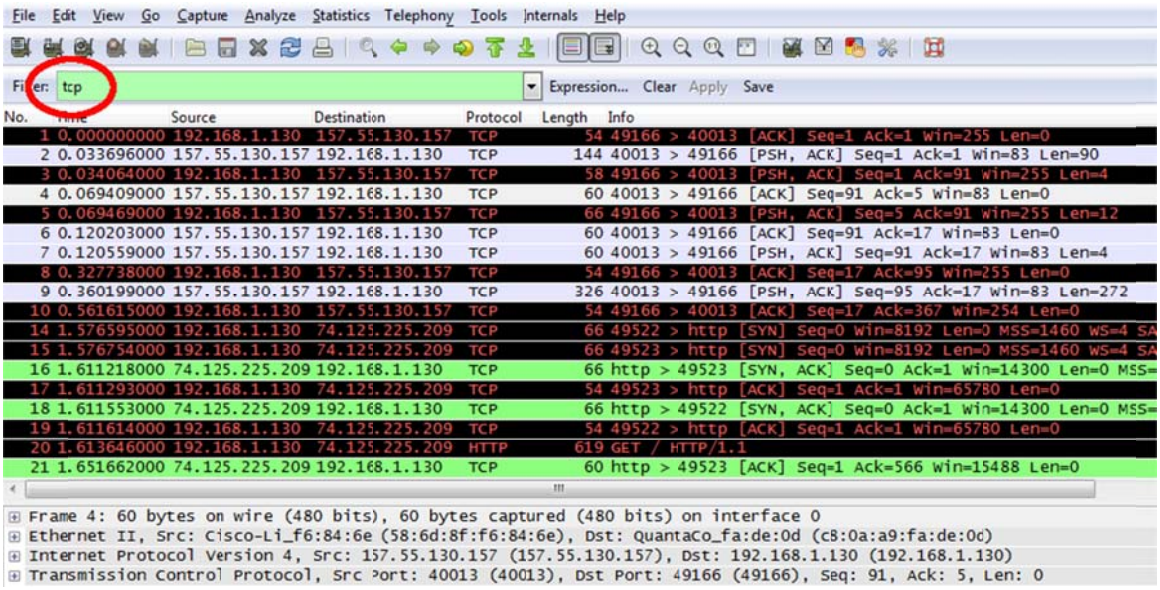
What is the IP address of the DNS server that the computer queried?

b. Frame 12 is the response from the DNS server with the IP address of www.google.com.

c. Find the appropriate packet for the start of your three-way handshake. In this example, frame 15 is the start of the TCP three-way handshake.

What is the IP address of the Google web server?

d. If you have many packets that are unrelated to the TCP connection, it may be necessary to use the Wireshark filter capability. Enter **tcp** in the filter entry area within Wireshark and press Enter.



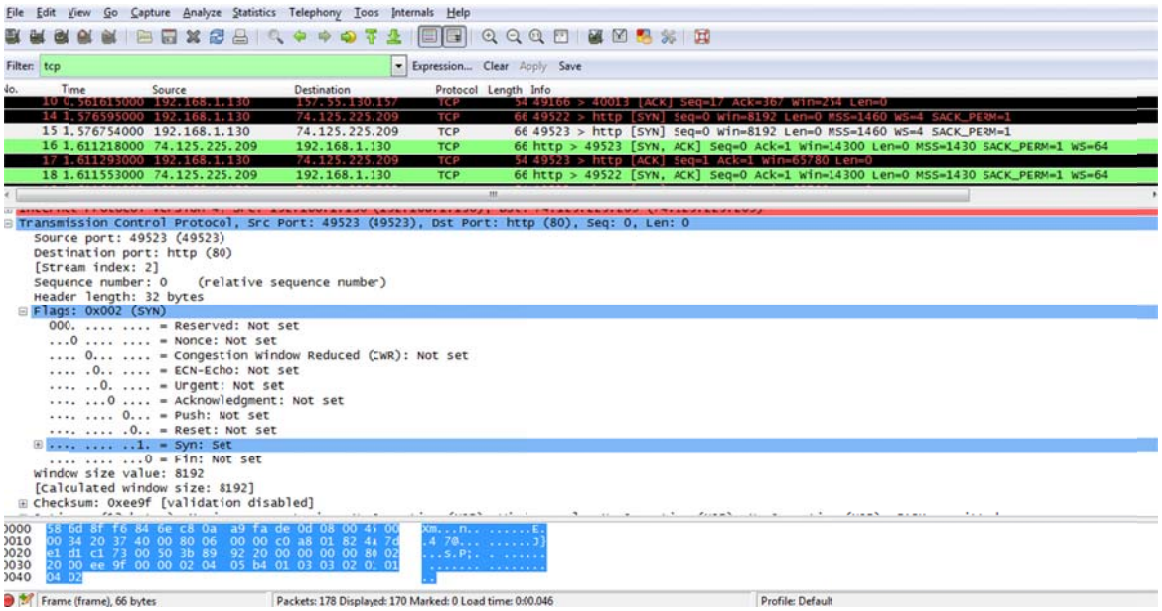
Step 3: Examine information within packets including IP addresses, TCP port numbers, and TCP control flags.

a. In our example, frame 15 is the start of the three-way handshake between the PC and the Google web server. In the packet list pane (top section of the main window), select the frame. This highlights the line and displays the decoded information from that packet in the two lower panes. Examine the TCP information in the packet details pane (middle section of the main window).

b. Click the **+** icon to the left of the Transmission Control Protocol in the packet details pane to expand the view of the TCP information.

c. Click the **+** icon to the left of the Flags. Look at the source and destination ports and the flags that are set.

Note: You may have to adjust the top and middle windows sizes within Wireshark to display the necessary information.



What is the TCP source port number?

How would you classify the source port?

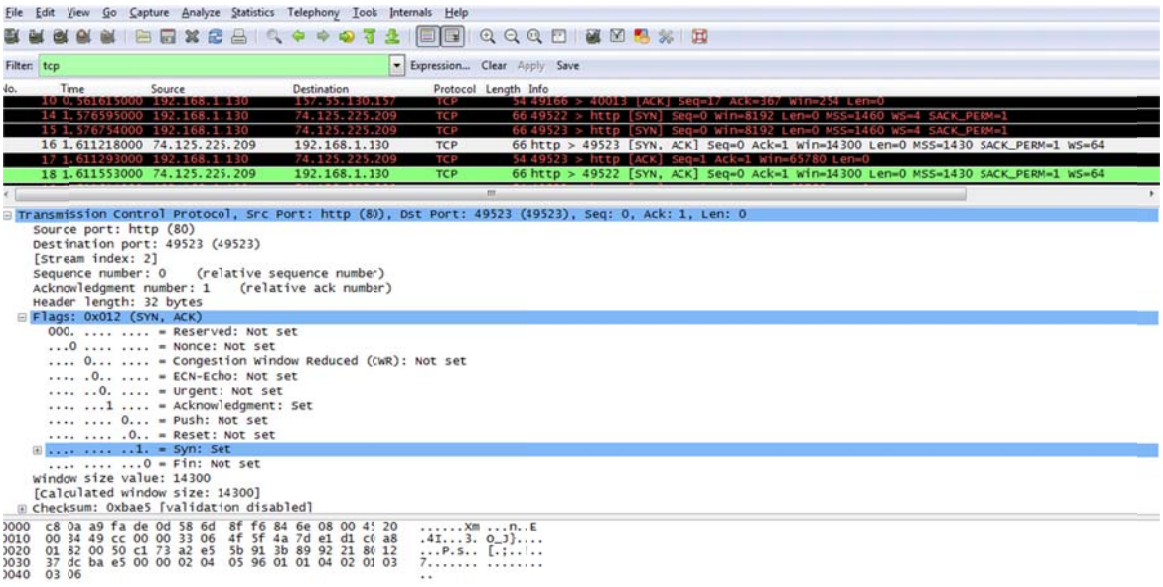
What is the TCP destination port number?

How would you classify the destination port?

Which flag (or flags) is set?

What is the relative sequence number set to?

d. To select the next frame in the three-way handshake, select **Go** on the Wireshark menu and select **Next Packet In Conversation**. In this example, this is frame 16. This is the Google web server reply to the initial request to start a session.

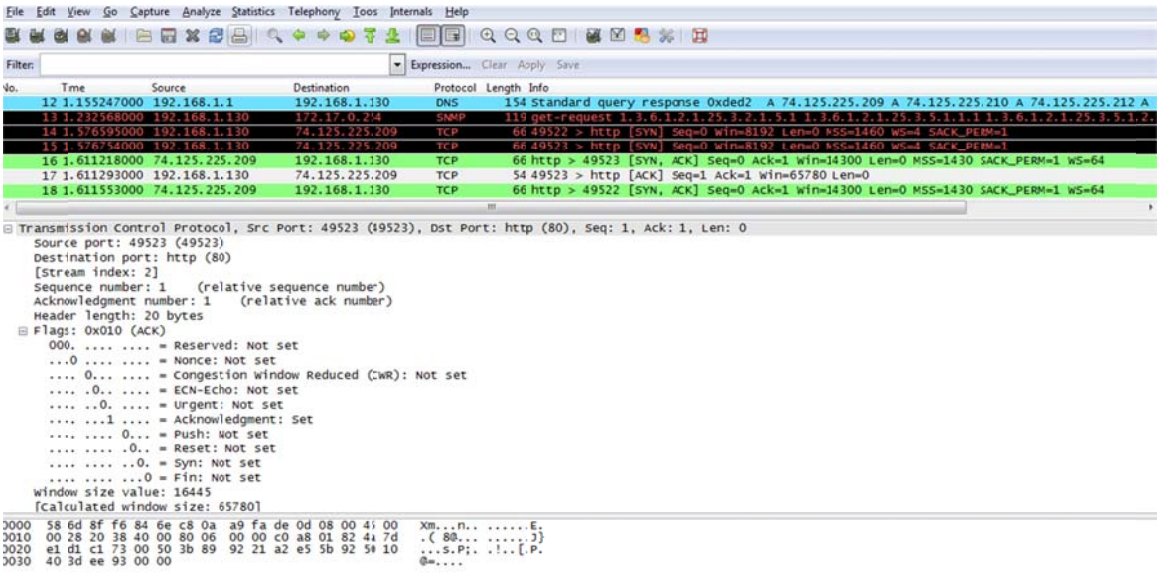


What are the values of the source and destination ports?

Which flags are set?

What are the relative sequence and acknowledgement numbers set to?

e. Finally, examine the third packet of the three-way handshake in the example. Clicking frame 17 in the top window displays the following information in this example:



Examine the third and final packet of the handshake.

Which flag (or flags) is set?

The relative sequence and acknowledgement numbers are 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 the Wireshark program.

Reflection

1. 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?

2. What other ways could Wireshark be used in a production network?