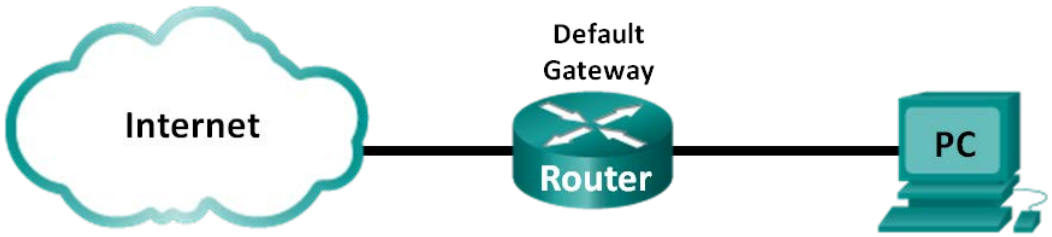
Lab - Using Wireshark to Observe the TCP 3-Way Handshake

Topology



Objectives

Part 1: Prepare Wireshark to Capture Packets

Part 2: Capture, Locate, and Examine Packets

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 FTP (File Transfer Protocol) 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 websites.

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

Required Resources

1 PC (Windows 7, 8, or 10 with a command prompt access, internet access, and Wireshark installed)

Part 1: Prepare Wireshark to Capture Packets

In Part 1, you will 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 the IP address of your PC and its network interface card (NIC) physical address, also called the MAC address.

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

```
Physical Address. . . . . . . . . : 00-24-D7-1C-50-44
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80dd:5657:ad20:f4b3%16(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.1.146(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

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

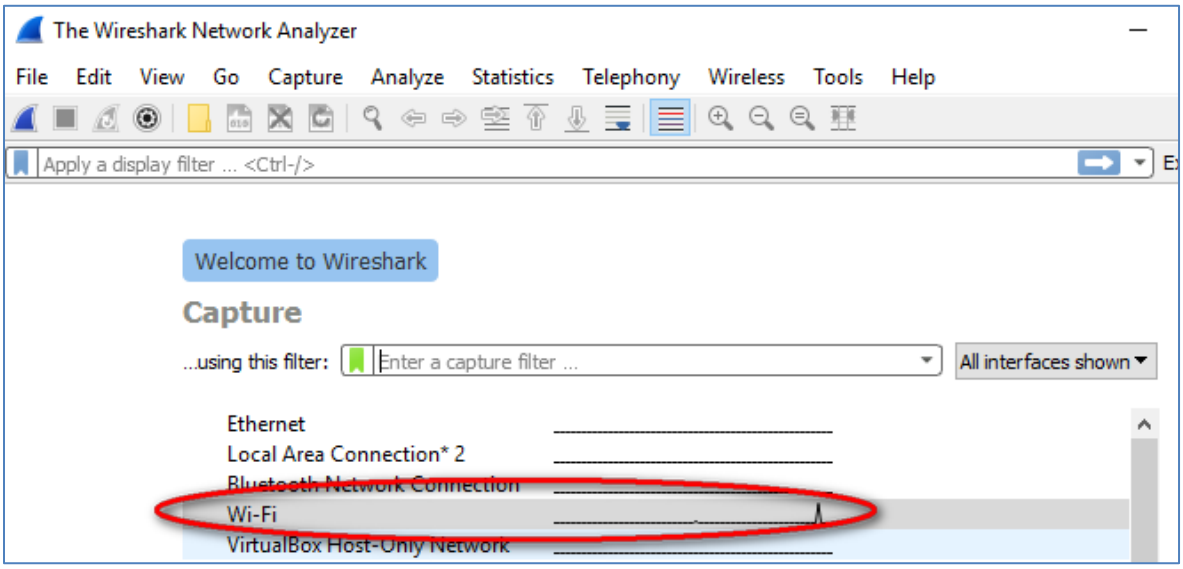
The PC host IP address:

The PC host MAC address:

Step 2: Start Wireshark and select the appropriate interface.

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

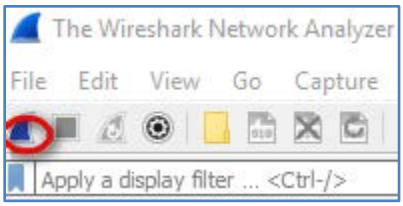
b. After Wireshark starts, select the active interface for data capture. The active interface will show traffic activities.



Part 2: Capture, Locate, and Examine Packets

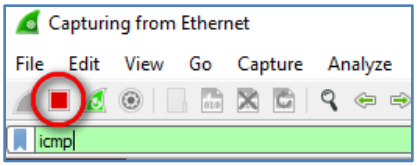
Step 1: Capture the data.

a. Click the **Start** button to start the data capture.



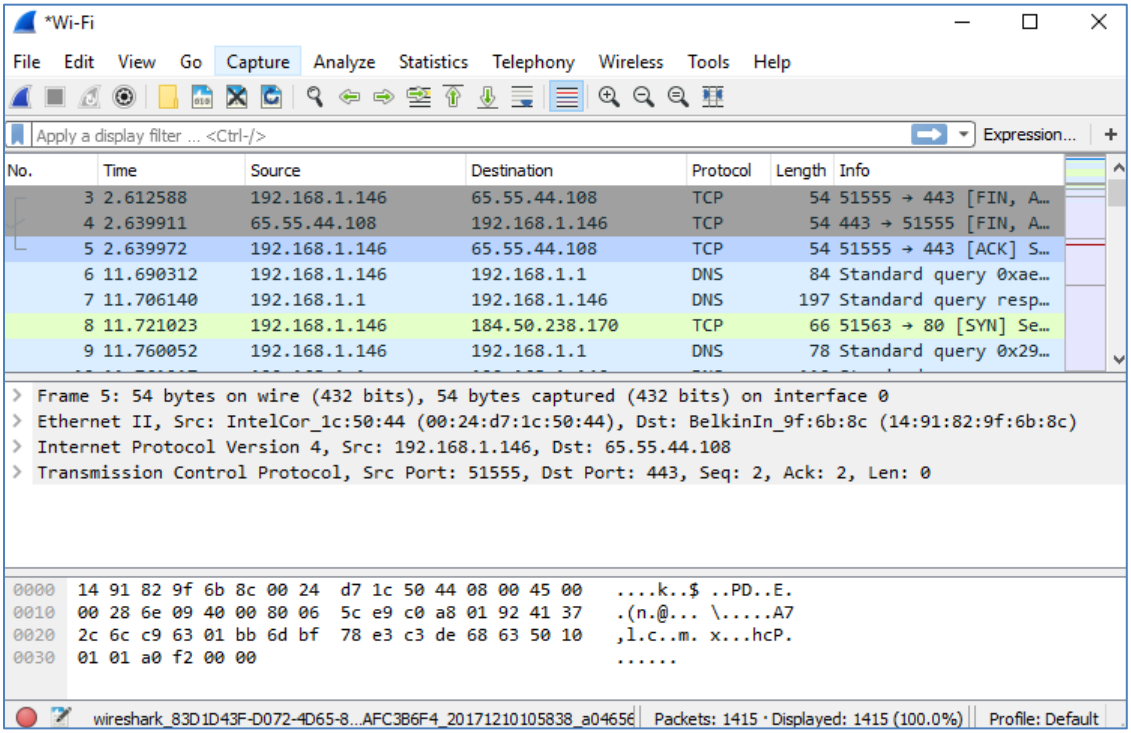
b. Open a web browser and visit www.google.com.

c. Minimize the browser and return to Wireshark. Stop the data capture.



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

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. If the PC already had an ARP entry for the default gateway, then it means that it started with the DNS query to resolve www.google.com.

a. Frame 6 shows the DNS query from the PC to the DNS server, which is 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.

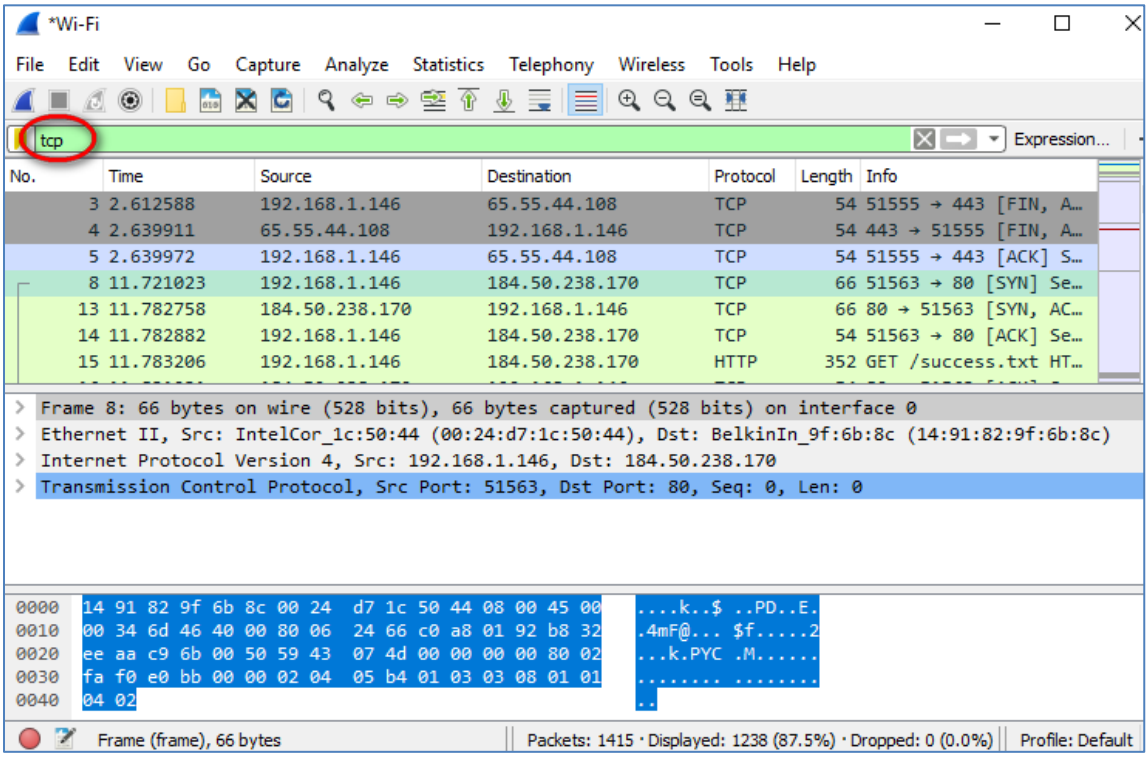
   What is the IP address of the DNS server that the computer queried?

b. Frame 7 is the response from the DNS server. It contains the IP address of www.google.com.

c. Find the appropriate packet for the start of your three-way handshake. In the example, frame 8 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 tool. Type **tcp** in the filter entry area within Wireshark and press **Enter**.



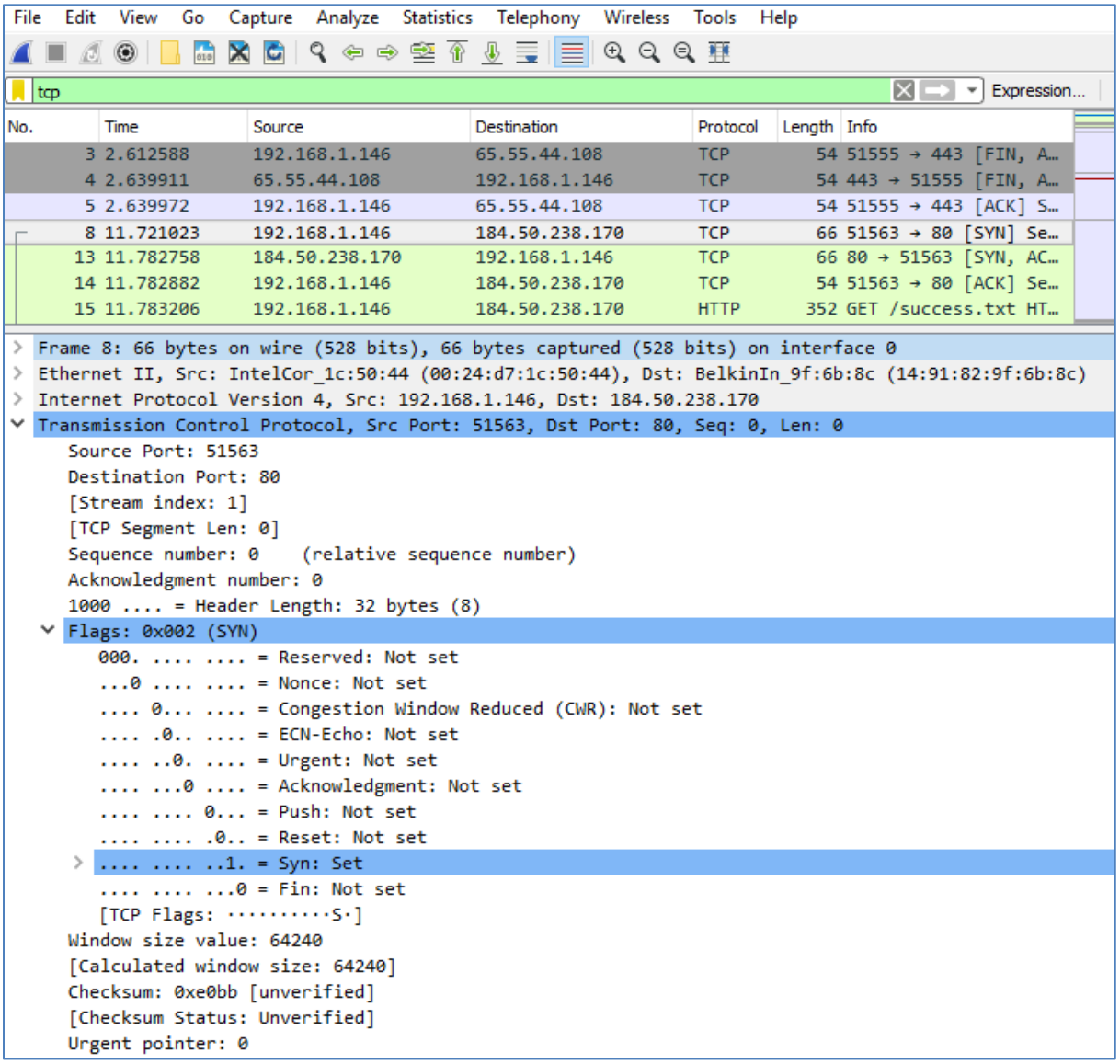
Step 3: Examine the information within packets including IP addresses, TCP port numbers, and TCP control flags.

a. In our example, frame 8 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?

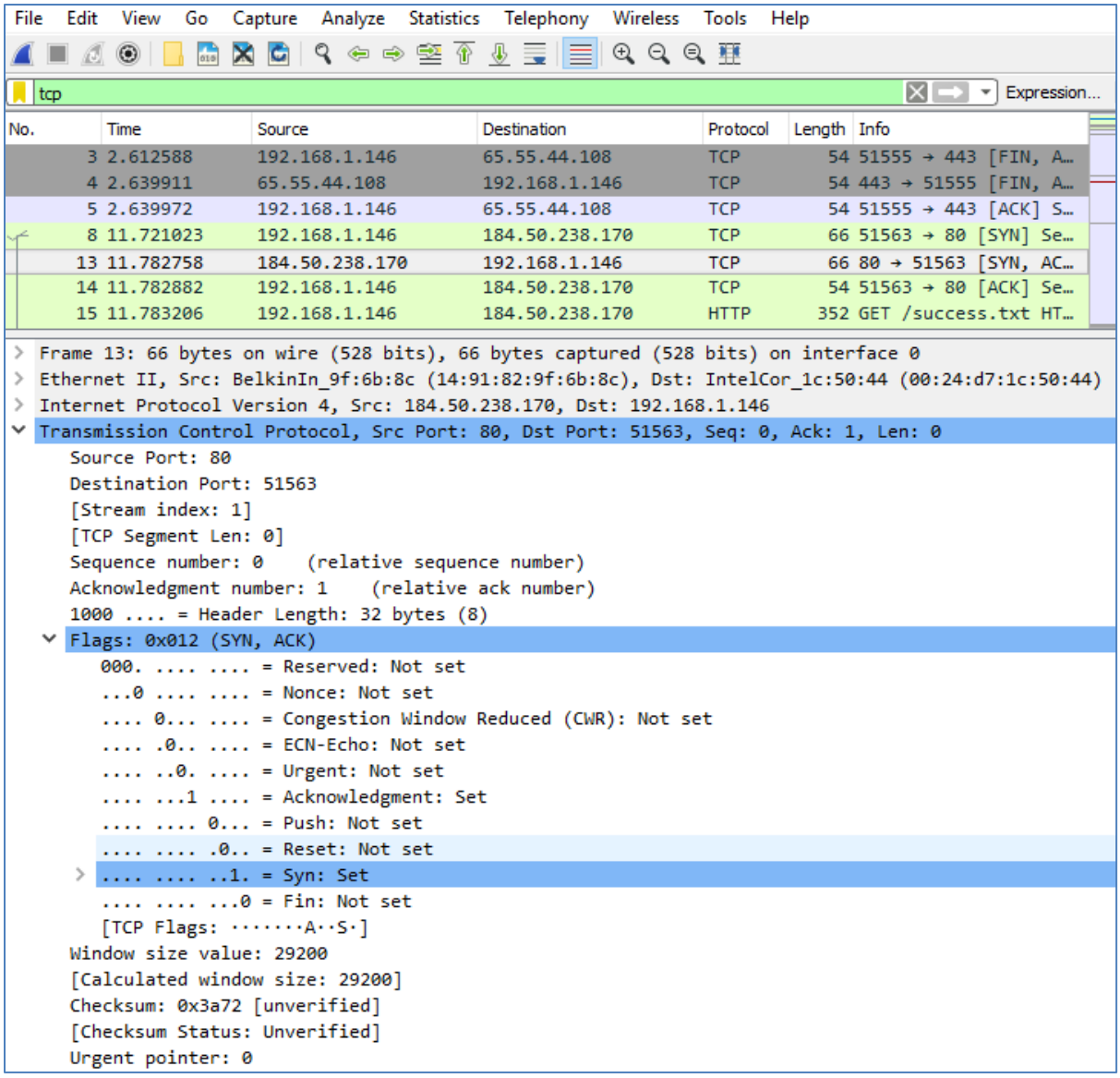
What is the TCP destination port number?

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 13. This is the Google web server reply to the initial request to start a session.

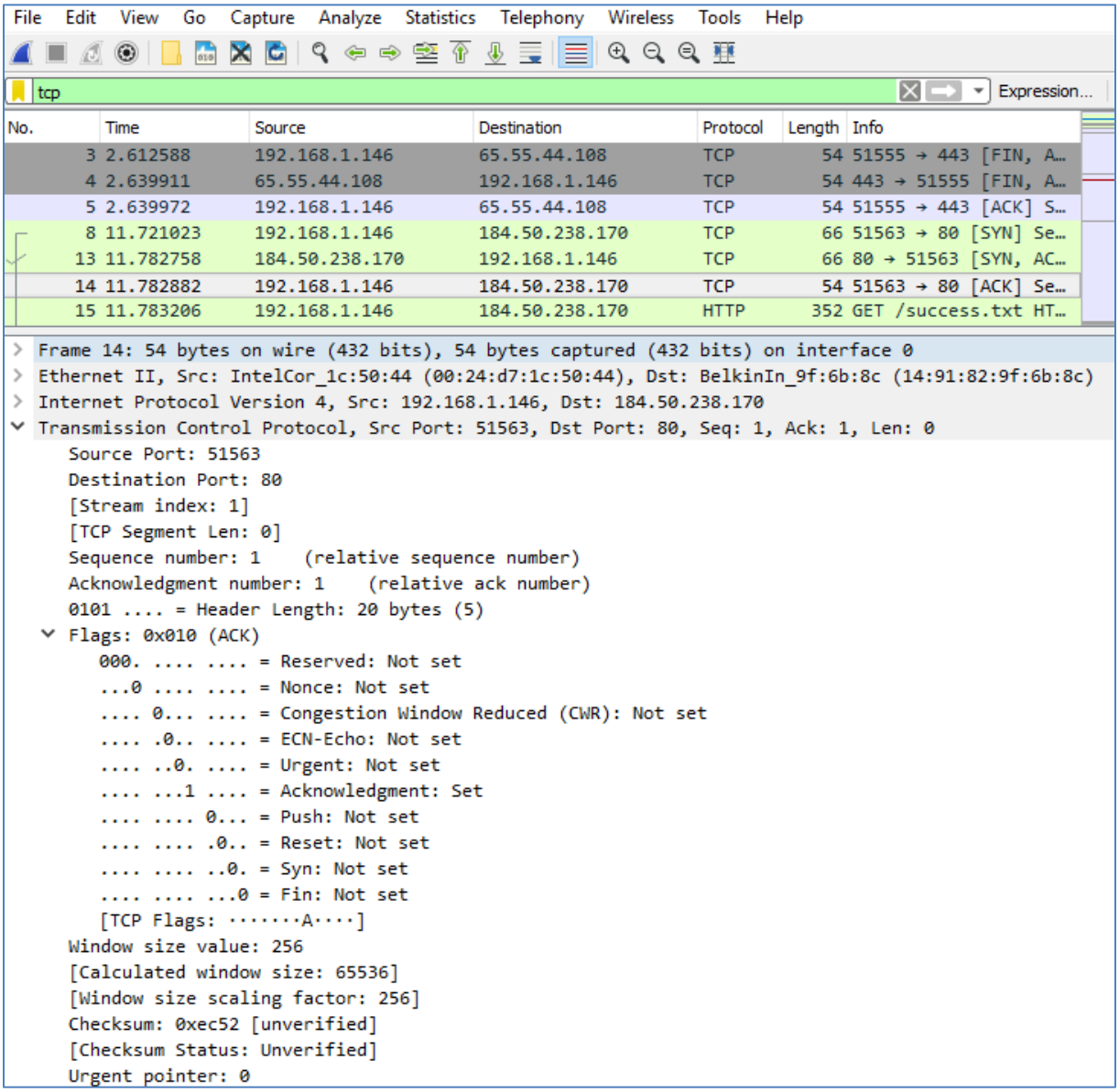


What are the values of the source and destination ports?

Which flags are set?

What are the relative sequence and acknowledgment numbers set to?

e. Finally, examine the third packet of the three-way handshake in the example. Click frame 14 in the top window to display 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 acknowledgment numbers are set to 1 as a starting point. The TCP connection is 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. List three filters that might be useful to a network administrator?

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