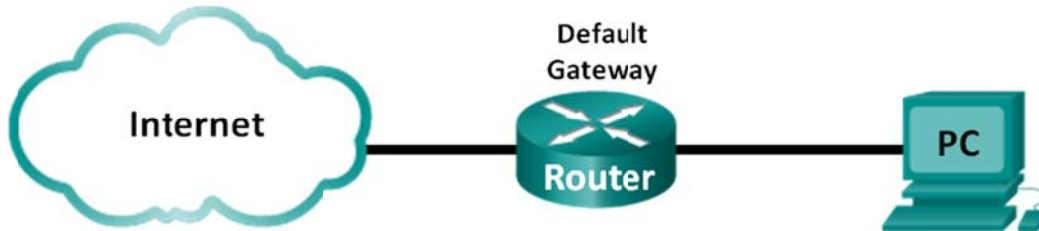


# Lab - Using Wireshark to Observe the TCP 3-Way Handshake

## 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.

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

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

```
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
```

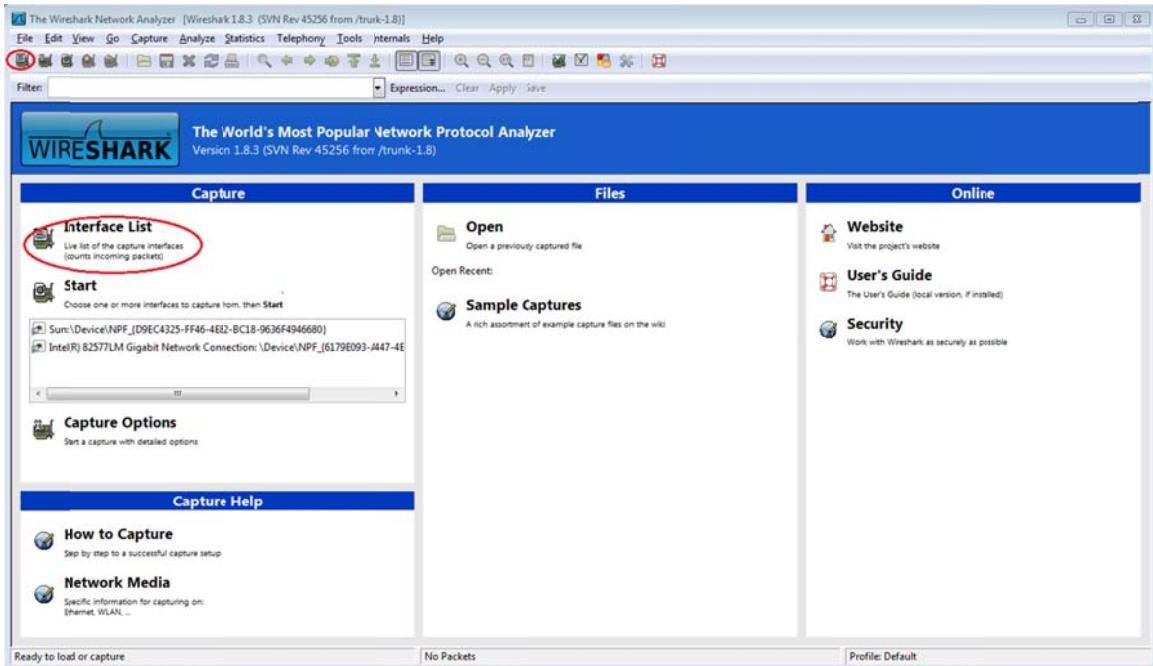
- b. Write down the IP and MAC addresses associated with the selected Ethernet adapter, because that is the source address to look for when examining captured packets.

The PC host IP address:

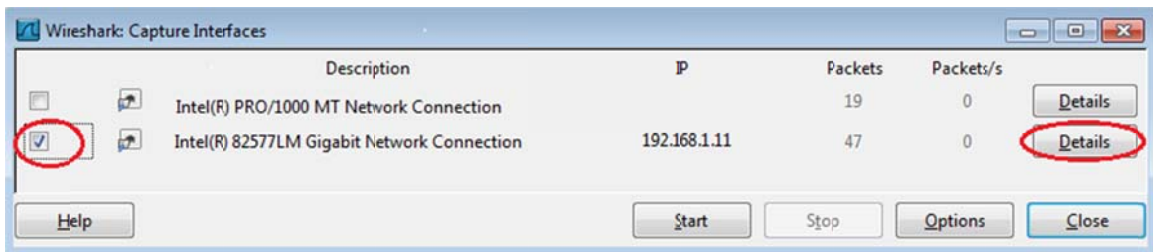
The PC host MAC address:

### 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.

- Go to [www.google.com](http://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:

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

Time	Source	Destination	Protocol	Length	Info
0.000000000	192.168.1.130	157.55.130.157	TCP	54	49166 > 40013 [ACK] Seq=1 Ack=1 win=255 Len=0
0.033696000	157.55.130.157	192.168.1.130	TCP	144	40013 > 49166 [PSH, ACK] Seq=1 Ack=1 win=83 Len=90
0.034064000	192.168.1.130	157.55.130.157	TCP	58	49166 > 40013 [PSH, ACK] Seq=1 Ack=91 win=255 Len=0
0.069409000	157.55.130.157	192.168.1.130	TCP	60	40013 > 49166 [ACK] Seq=91 Ack=5 win=83 Len=0
0.069469000	192.168.1.130	157.55.130.157	TCP	66	49166 > 40013 [PSH, ACK] Seq=5 Ack=91 win=255 Len=0
0.120203000	157.55.130.157	192.168.1.130	TCP	60	40013 > 49166 [ACK] Seq=91 Ack=17 win=83 Len=0
0.120559000	157.55.130.157	192.168.1.130	TCP	60	40013 > 49166 [PSH, ACK] Seq=91 Ack=17 win=83 Len=0
0.327738000	192.168.1.130	157.55.130.157	TCP	54	49166 > 40013 [ACK] Seq=17 Ack=95 win=255 Len=0
0.360199000	157.55.130.157	192.168.1.130	TCP	326	40013 > 49166 [PSH, ACK] Seq=95 Ack=17 win=83 Len=0
0.561615000	192.168.1.130	157.55.130.157	TCP	54	49166 > 40013 [ACK] Seq=17 Ack=367 win=254 Len=0
1.140459000	192.168.1.130	192.168.1.1	DNS	74	Standard query 0xded2 A www.google.com
1.155247000	192.168.1.1	192.168.1.130	DNS	154	Standard query response 0xded2 A 74.125.225.209
1.232568000	192.168.1.130	172.17.0.254	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.4
1.576595000	192.168.1.130	74.125.225.209	TCP	66	49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460
1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460
1.611218000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0
1.611293000	192.168.1.130	74.125.225.209	TCP	54	49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
1.611553000	74.125.225.209	192.168.1.130	TCP	66	http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0

Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: cisco-Li\_f6:84:6e (58:6d:8f:f6:84:6e), Dst: quantaco\_fa:de:0d (c8:0a:a9:fa:de:0d)  
Internet Protocol Version 4, Src: 157.55.130.157 (157.55.130.157), Dst: 192.168.1.130 (192.168.1.130)  
Transmission Control Protocol, Src Port: 40013 (40013), Dst Port: 49166 (49166), Seq: 91, Ack: 5, Len: 0

#### 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](http://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](http://www.google.com).

- Frame 11 shows the DNS query from the PC to the DNS server, attempting to resolve the domain name, [www.google.com](http://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.

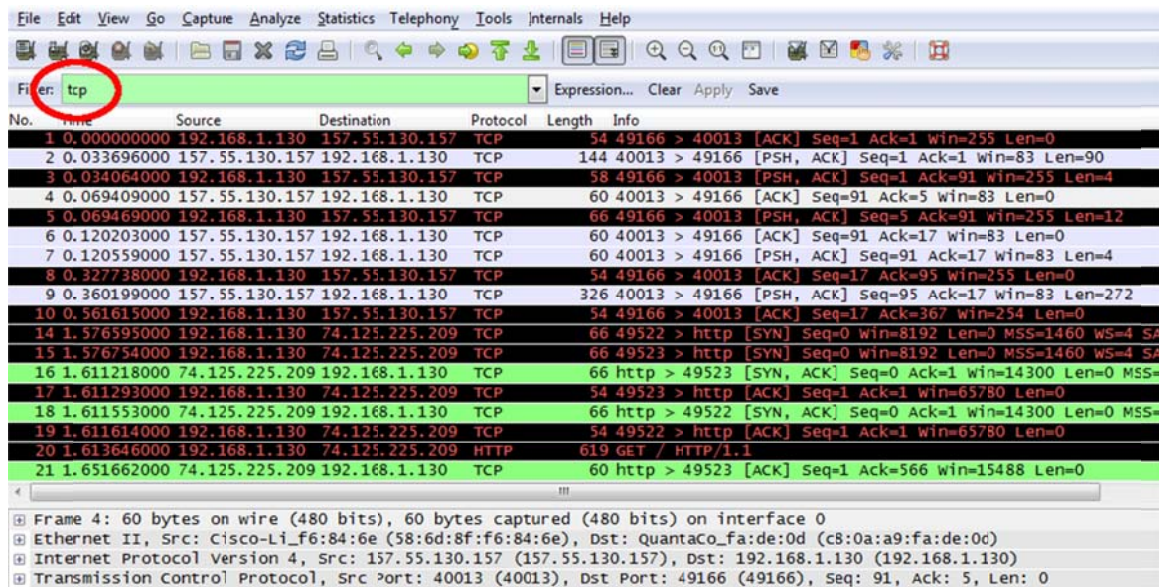
What is the IP address of the DNS server that the computer queried?

- Frame 12 is the response from the DNS server with the IP address of [www.google.com](http://www.google.com).
- 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.

## Lab - Using Wireshark to Observe the TCP 3-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.

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



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

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
10	0.361613000	192.168.1.130	192.168.1.130	TCP	34	49166 > 40013 [ACK] Seq=17 Ack=367 win=234 Len=0
11	1.576593000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	1.611218000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17	1.611293000	192.168.1.130	74.125.225.209	TCP	34	49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18	1.611553000	74.125.225.209	192.168.1.130	TCP	66	http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64

Transmission Control Protocol, Src Port: 49523 (49523), Dst Port: http (80), Seq: 0, Len: 0

Source port: 49523 (49523)  
 Destination port: http (80)  
 [Stream index: 2]  
 Sequence number: 0 (relative sequence number)  
 Header length: 32 bytes

Flags: 0x002 (SYN)

- 000. .... = Reserved: Not set
- ...0. .... = Nonce: Not set
- ...0. .... = Congestion window Reduced (cWR): Not set
- ...0. .... = ECN-Echo: Not set
- ...0. .... = Urgent: Not set
- ...0. .... = Acknowledgment: Not set
- ...0. .... = Push: Not set
- ...0. .... = Reset: Not set
- ...1. .... = Syn: Set
- ...0. .... = Fin: Not set

Window size value: 8192  
 [calculated window size: 8192]  
 Checksum: 0xee9f [validation disabled]

3000 58 6d 8f f6 84 6e c8 0a a9 fa de 0d 08 00 41 00 .....Xm...n.E  
 3010 00 34 20 37 40 00 00 06 00 00 c0 a8 01 82 41 7d .....4I...3.0J]...  
 3020 e1 d1 c1 73 00 50 3b 89 92 20 00 00 00 81 02 ...P.s...[;...  
 3030 20 00 ee 9f 00 00 02 04 05 b4 01 03 03 02 01 01 .....7.....  
 3040 04 02 ..

Frame (frame), 66 bytes | Packets: 178 Displayed: 170 Marked: 0 Load time: 0:00.046 | Profile: Default

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.

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
10	0.361613000	192.168.1.130	192.168.1.130	TCP	34	49166 > 40013 [ACK] Seq=17 Ack=367 win=234 Len=0
11	1.576593000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15	1.576754000	192.168.1.130	74.125.225.209	TCP	66	49523 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	1.611218000	74.125.225.209	192.168.1.130	TCP	66	http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17	1.611293000	192.168.1.130	74.125.225.209	TCP	34	49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18	1.611553000	74.125.225.209	192.168.1.130	TCP	66	http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64

Transmission Control Protocol, Src Port: http (80), Dst Port: 49523 (49523), Seq: 0, Ack: 1, Len: 0

Source port: http (80)  
 Destination port: 49523 (49523)  
 [Stream index: 2]  
 Sequence number: 0 (relative sequence number)  
 Acknowledgment number: 1 (relative ack number)  
 Header length: 32 bytes

Flags: 0x012 (SYN, ACK)

- 000. .... = Reserved: Not set
- ...0. .... = Nonce: Not set
- ...0. .... = Congestion window Reduced (cWR): Not set
- ...0. .... = ECN-Echo: Not set
- ...0. .... = Urgent: Not set
- ...1. .... = Acknowledgment: Set
- ...0. .... = Push: Not set
- ...0. .... = Reset: Not set
- ...1. .... = Syn: Set
- ...0. .... = Fin: Not set

Window size value: 14300  
 [calculated window size: 14300]  
 Checksum: 0xbae5 [validation disabled]

3000 c8 0a a9 fa de 0d 58 6d 8f f6 84 6e 08 00 41 20 .....Xm...n.E  
 3010 00 34 49 cc 00 00 33 06 4f 5f 4a 7d e1 d1 c1 a8 .....4I...3.0J]...  
 3020 01 82 00 50 c1 73 a2 e5 5b 91 3b 89 92 21 86 12 ...P.s...[;...  
 3030 37 6c ba e5 00 00 02 04 05 96 01 01 04 02 01 03 .....7.....  
 3040 03 06 ..

What are the values of the source and destination ports?

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

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:

```
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
13 1.155247000 192.168.1.1 192.168.1.130 DNS 154 standard query response Oxdd2 A 74.125.225.209 A 74.125.225.210 A
14 1.232968000 192.168.1.130 172.17.0.214 SNMP 119 get-Request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.3.1.1.1 1.3.6.1.2.1.25.3.3.1.2
15 1.576595000 192.168.1.130 74.125.225.209 TCP 66 49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16 1.611218000 74.125.225.209 192.168.1.130 TCP 66 http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17 1.611293000 192.168.1.130 74.125.225.209 TCP 54 49523 > http [ACK] Seq=1 Ack=1 win=65780 Len=0
18 1.611553000 74.125.225.209 192.168.1.130 TCP 66 http > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
Transmission Control Protocol, Src Port: 49523 (49523), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
Source port: 49523 (49523)
Destination port: http (80)
[Stream index: 2]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0. .... = Nonce: Not set
...0. .... = Congestion Window Reduced (cWR): Not set
...0. .... = ECN-Echo: Not set
...0. .... = Urgent: Not set
...1. .... = Acknowledgment: Set
...0. .... = Push: Not set
...0. .... = Reset: Not set
...0. .... = Syn: Not set
...0. .... = Fin: Not set
Window size value: 16445
[calculated window size: 65780]
3000 58 6d 8f f6 84 6e c8 0a a9 fa de 0d 08 00 41 00 Xm...n... ..E.
3010 00 28 20 38 40 00 80 06 00 00 c0 a8 01 82 41 7d (. (88... ..3]
3020 e1 d1 c1 73 00 50 3b 89 92 21 a2 e5 5b 92 5f 10 ...S.P; .!..[.P.
3030 40 3d ee 93 00 00 @=....
```

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?