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-ØA-A9-FA-DE-ØD
DHCP Enabled									Yes
Autoconfiguration	En	aJ	blε	ed				-	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 Topip).							=	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.

Wireshark: Cap	ture Interfaces			6	- • •
	Description	P	Packets	Packets/s	
	Intel(F) PRO/1000 MT Network Connection		19	0	Details
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details
Help		<u></u> tart	Stop	Options	<u>C</u> lose

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.

<u>File</u>	lit <u>V</u> iew	<u>Go</u> <u>C</u> apture	Analyze	Statistics	Telephony	Tools	Inter	nals <u>H</u> elp									
			* 2	819	¢ \$ 1	ə F	2		€ (20	2		¥ 🐔	36 D	1		
Filter:							-	Expression.	. Clear	Арр	ly Sav	e					
Time		Source		Destina	ation	j.	rotoc	ol Length	Info								
1 0.00	00000000	192.168.1	.130	157.	55.130.1	.57	TCP	5	4 4916	6 >	40013	[ACK] Seq-	=1 Ack=	1 Win=2	255 Len	=0
2 0.0	3696000	157.55.13	0.157	192.	168.1.13	0	TCP	14	4 4001	3 >	49166	[PSH	, ACK]	Seq=1	Ack=1	Win=83	Len=9(
3 0.0	34064000	192.168.1	.130	157.	55.130.1	.57	TCP	5	8 4916	i6 >	40013	[PSH	, ACK]	Seq=1	Ack=91	Win=2	55 Len=
4 0.06	59409000	157.55.13	0.157	192.	168.1.13	0	TCP	6	0 4001	3 >	49166	[ACK] Seq=	91 Ack	=5 Win=	=83 Len	=0
5 0.00	59469000	192.168.1	.130	157.	55.130.1	.57	TCP	6	6 4916	6 >	40013	[PSH	, ACK]	Seq=5	Ack=91	L Win=2	55 Len=
6 0.12	20203000	157.55.13	0.157	192.	168.1.1	0	TCP	6	0 4001	3 >	49166	[ACK	Seq=	91 Ack	-17 Wir	1=83 Lei	n=0
7 0.12	20559000	157.55.13	0.157	192.	168.1.13	0	TCP	6	0 4001	3 >	49166	LPSH	, ACK	Seq=9	1 ACK=1	17 W1n=	83 Len=
8 0. 32	27738000	192.168.1	.130	157.	55.130.1	57	TCP	22	4 4916	6 >	40013	LACK] Seq=	=1/ ACK	=95 W1r	1=255 L	en=0
9 0.30	50199000	15/.55.13	0.15/	192.	108.1.1:	0	TCP	32	6 4001	3 >	49100	LEAR	, ACK	Seq=9	D ACK=1	L/ Win=	83 Len=
10 0.50	51615000	192.168.1	.130	117.	55.130.1	.5/	TCP	2	4 4916	< 0	40013	LACK	J Seq=	=1/ ACK	=36/ W1	in=254	Len=0
12 1 19	5247000	102.168.1	1 1	162	168.1.1	0	DNS	15	+ Stan	idan d	quer	y oxa	edz #	Oxdod2	a 74	125 22	5 200 /
12 1.12	22568000	192.108.1	120	172	100.1.12 17 0 254	0	CNND	11	+ Stan	nan u	quei	y res	Donse	25 2 2	1 5 1	1 2 6	1 2 1
14 1 57	76595000	192.108.1	130	74 1	25 225 2	000	TCP		6 4052	2	httn	[SVN]	Sen=(win=8	107 107	1. 5. 0.	-1460
15 1 57	6754000	102 168 1	130	74.1	25 225 2	00	TCP	6	6 4052	2	http	[SVN]	Seg-C	Win-8	10) 10	-0 MSS	-1460
16 1 61	1218000	74 125 22	5 209	1.02	168 1 13	0	TCP	6	6 http	1	9523	[SVN	ACKI	Sec=0	Ack-1 V	/in=143	00 1 en-
17 1.6	1293000	192 168 1	130	74.1	25.225.2	09	TCP	5	4 4952	RS	http	[ACK]	Sed-1	Ack=1	win=6	5780 Le	
18 1.61	1553000	74,125,22	5,209	192.	168.1.1	0	TCP	6	6 http	> 4	9522	[SYN.	ACK]	Seg=0	Ack=1 V	vin=143	00 Len=
•				m								-					F
E Fran	e 4: 60	bytes on w	ire (4	80 bits)	. 60 byt	es ca	oture	d (480	bits)	on	inter	Face 0	V.				
H Ethe	rnet II.	. Src: cisc	o-Li f	6:84:6e	(58:6d:8	f:f6:	84:66). Dst:	Quant	taco	fa:de	e:0d (c8:0a	:a9:fa:	de:0d)		
Inte	rnet Pro	otocol vers	ion 4.	Src: 15	7.55.130	.157	(157.	55.130.	157).	DSt	192	168.1	.130	(192.16	8.1.13	0)	
. Tran	smission	Control P	rotoco	1. SEC P	ort: 400	13 (4	0013)	, DSt P	ort: 4	49166	5 (49)	166),	Seq:	91, Ack	: 5, L	en: 0	
- miximum																	

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.

Eile	Edit View	v <u>G</u> o	Capture Ana	alyze	Statistics	Telephony	Tools	Internals	Help							
				2	819	\$	a) 🖗	1		Q Q			- *	Ħ		
File	er: tcp							Express	ion Cle	ear Apply	Save					
No.	THINK		Source		Destination	1	Protoco	ol Length	Info							
	1 0.0000	00000	192.168.1.	130	157.55.	130.157	TCP	5	4 49166	> 4001	.3 [ACK]	Seq=	1 Ack=1	Win=25	55 Len=0	
	2 0.0336	96000	157.55.130	0.157	192.168	.1.130	TCP	144	4 40013	> 4916	6 [PSH,	ACK]	Seq=1	Ack=1 V	vin=83 L	en=90
	3 0.0340	64000	192.168.1.	130	157.55.	130.157	TCP	5	8 49166	> 4001	3 [PSH,	ACK]	Seq=1	Ack=91	Win=255	Len=4
	4 0.0694	09000	157.55.130	0.157	192.168	.1.130	TCP	6	0 40013	> 4916	6 [ACK]	Seq=	91 Ack=	5 Win=8	33 Len=0	
	5 0.0694	69000	192.168.1.	130	157.55.	130.157	TCP	6	5 49166	> 4001	3 [PSH,	ACK]	Seq=5	Ack=91	Win=255	Len=12
	6 0.1202	03000	157.55.130	0.157	192.168	.1.130	TCP	6	0 40013	> 4916	6 [ACK]	Seq=	91 Ack=	17 Win=	-83 Len=	0
	7 0.1205	59000	157.55.130	0.157	192.168	.1.130	TCP	6	0 40013	> 4916	6 [PSH,	ACK]	Seq=91	Ack=17	Win=83	Len=4
	8 0. 3277	38000	192.168.1.	130	157.55.	130.157	TCP	54	4 49166	> 4001	3 [ACK]	Seq=	17 Ack=	95 Win=	255 Len	=0
	9 0.3601	99000	157.55.130	0.157	192.168	.1.130	TCP	32	5 40013	> 4916	6 [PSH,	ACK]	Seq-95	Ack=17	/ Win=83	Len=272
1	0 0.5616	15000	192.168.1.	130	157.55.	130.157	TCP	54	4 49166	> 4001	3 [ACK]	Seq=	17 Ack=	367 Wir	1=254 Lei	n=0
1	4 1. 5765	95000	192.168.1.	130	74.125.	225.209	TCP	6	5 49522	> http	[SYN]	Seq=0	Win=81	92 Len=	-0 MSS=14	460 WS=4 SA
1	5 1. 5767	54000	192.168.1.	130	74.125.	225.209	TCP	6	6 49523	> http	[SYN]	Seq=0	Win=81	92 Len=	-0 MSS=1	460 WS=4 SA
1	6 1.6112	18000	74.125.225	5.209	192.168	.1.130	TCP	6	5 http:	> 49523	[SYN,	ACK]	Seq=0 A	ck=1 Wi	in=14300	Len=0 MSS=
1	7 1.6112	93000	192.168.1.	1,30	74.125.	225.209	TCP	5	4 49523	> http	[ACK]	Seq=1	Ack=1	Win=657	80 Len=	0
1	8 1.6115	53000	74.125.225	5.209	192.168	.1.130	TCP	6	5 http	> 49522	[SYN,	ACK]	Seq=0 A	ck=1 Wi	in=14300	Len=0 MSS=
1	9 1.6116	14000	192.168.1.	130	74.125.	225.209	TCP	54	4 49522	> http	[ACK]	Seq=1	Ack=1	Win=657	780 Len=	0
2	20 1.6136	46000	192.168.1.	130	74.125.	225.209	HTTP	61	9 GET /	HTTP/1	.1					
2	1 1.6516	62000	74.125.225	5.209	192.168	.1.130	TCP	6	0 http:	> 49523	[ACK]	Seq=1	Ack=56	6 Win=1	5488 Lei	n=0
4		19-19-19-19-19-19-19-19-19-19-19-19-19-1														
🕀 F	rame 4:	60 by	tes on wire	e (48	0 bits)	, 60 byt	tes cap	otured (4	80 bits) on i	nterfac	e O				
🕀 E	thernet	II, S	irc: Cisco-I	Li_f6	:84:6e	(58:6d:8	Sf:f6:8	84:6e), D	st: Qua	antaCo_t	a:de:0	d (cB:	0a:a9:1	a:de:0	d)	
• I	nternet	Proto	col Version	n 4,	Src: 15	7.55.130	0.157	(157.55.1	30.157)	, Dst:	192.16	8.1.13	0 (192.	168.1.	130)	

⊕ Transmission Contro] Protocol, Src Port: 40013 (40013), Dst Port: 49166 (49166), Seq: 91, Ack: 5, Len: 0

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.

	Telephony Toos Internais Telep					
	. 🗢 🔶 ኛ 👱 🔲 🖬 🕚	Q Q Q 🗹 📓 🛙	0 🧏 🐝 🔛			
ten tcp	Expression	Clear Apply Save				
Time Source	Destination Protocol	Length Info				
10 0.561615000 192.168.1.130	157.55.130.157 TCP	54 49166 > 4001	3 [ACK] Seq=17 Act	=367 W1n=214 Len=		
15 1 576754000 192 168 1 130	74.125.225.209 TCP	66 49522 > http	[SYN] Seg=0 win=1	192 Len=0 MSS=146	0 WS-4 SACK PEOM-1	
16 1, 611218000 74, 125, 225, 209	192,168,1,130 TCP	66 http > 4952	[SYN, ACK] Seg=0	Ack=1 win=14300 L	en=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=	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 L	en=0 MSS=1430 SACK_PERM=	1 W5=64
				the Baseline and		
Source port: 49523 (49523) Destination port: http (80) [stream index: 2] sequence number: 0 (relative s Header length: 32 bytes Flags: 0x002 (SYN) 006 = Reserved: Not 0	equence number) set dow Reduced (IWR): Not set set it :: Not set					
the first office - reput the per						
0 = Reset: Not set						
<pre></pre>	bled]					
	bled] 5e 0d 08 00 41 00 Xm. n. co a8 01 82 41 7d .4 78. 00 00 00 00 88 02 10 03 03 02 0 01		a . 1. Insat			

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.

ile Edit View Go Capture Analyze Statis	ics Telephony Ioot Internals	Help		
x w & e e e e a x 2 2 1	9. * * * 7 2 🔳		2 🥵 🐝 🙀	
iten tcp	• Expr	ession Clear Apply Save		
. Time Source	Destination	Protocol Length Info		
10 0.561615000 192.168.1.130	157 555 130 157	TCP 54 49166 > 400.	13 [ACK] Seq=17 Ack=367 Win=254 Len=0	
14 1,576595000 192.168.1.130	74.125.225.209	TCP 66 49522 > htt	p [SYN] Seq=0 win=8192 Len=0 M55=1460 w	S=4 SACK_PERM=1
15 1.576754000 192.168.1.130	74.125.225.209	TCP 66 49523 > http	p [SYN] Seq=0 win=8192 Len=0 MSS=1460 w	S=4 SACK_PERM=1
16 1.611218000 74.125.225.209	192.168.1.130	TCP 66 http > 4952	3 [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 > htt	p [ACK] Seq=1 Ack=1 win=65780 Len=0	
18 1.611553000 74.125.225.209	192.168.1.130	TCP 66 http > 4952	2 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=	0 MSS=1430 SACK_PERM=1 WS=64
		III.		
Destination port: 49523 (49523) [Stream index: 2] Sequence number: 0 (relative Acknowledgment number: 1 (re Header length: 32 bytes 000 Reserved: NC 000 Reserved: NC 000 Rongestion V 000 Congestion V 000 Congestion V 000 Urgent: Not 000 Push: Not si 000 Push: Not si 000 Push: Not si	sequence number) lative ack number) t set et indow Reduced ((wR): Not t set set nt: Set t et	t set		
@1. = Syn: Set				
window size value: 14300				
[calculated window size: 14300]				
Checksum: OxhaeS [validation di	sabled			
00 c8 0a a9 fa de 0d 58 6d 8f f 10 00 34 49 cc 00 00 33 06 4f 5 20 01 82 00 50 c1 73 a2 e5 5b 9 30 37 dc ba e5 00 00 02 04 05 9 40 03 06	6 84 6e 08 00 41 20 f 4a 7d e1 d1 c0 a8 1 3b 89 92 21 80 12 6 01 01 04 02 01 03 7.	XmnE I3. 0_3} .P.S [.;		

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:

Image: Second	Clear Apple Control Control Clear Apple Control Contro	WE Sk Description Iard query response 0xded2 A 74.125.225.209 A 74.125.225.210 A 74.125.225.210 Iard query response 0xded2 A 74.125.225.209 A 74.125.225.210 A 74.125.225.210 Iard query response 0xded2 A 74.125.225.209 A 74.125.225.210 A 74.125.225.210 Is for the form A 56.12.21.251.2.1.51.1.1.3.0.12.21.251.251.251.1.1.1.3.0.12.21.251.251.251.1.1.1.3.0.12.21.251.251.251.251.2.1.1.1.1.3.0.12.21.251.251.251.251.251.251.251.251.2
Filter Source Destination 12 1.55247000 192.168.1.130 192.168.1.130 13 1.2245368000 192.168.1.130 172.17,0.224 14 1.576555000 192.168.1.130 74.125.225.225.209 15 1.61236000 74.125.225.209 192.168.1.130 74.125.225.209 16 1.61238000 74.125.225.209 192.168.1.130 74.125.225.209 18 1.611553000 74.125.225.209 192.168.1.130 74.125.225.209 18 1.611553000 74.125.225.209 192.168.1.130 74.125.225.209 18 1.611553000 74.125.225.209 192.168.1.130 74.125.225.209 15 1.611553000 74.125.225.209 192.168.1.130 74.125.225.209 19 1.611553000 74.125.225.209 192.168.1.130 74.125.225.209 15 1.611553000 74.125.225.209 192.168.1.130 74.125.225.209 15 1.53000 74.125.225.209 192.168.1.130 74.125.225.209 15 1.611553000 74.125.25.25.209	Expression Clear Aophy 5 Protocol Length Info DNS 154 Stan SNAP 110 get- TCP 66 4952 TCP 66 4952 TCP 66 4952 TCP 66 http TCP 54 4952 TCP 66 http 3 SNAP 10 get- 8 SNAP 1	WF land query response 0xded2 A 74.125.225.209 A 74.125.225.210 A 74.125.225.212 / state state is 6.1.2.1.25.3.2.1.5.1 is 3.6.1.2.1.25.25.210 A 74.125.225.210 A 74.125.225.212 / is fittp [SYN] seq=0 win=8192 ten=0 k55=1460 w5=4 54CK_PERM=1 > http:[SYN] seq=0 win=8192 ten=0 k55=1460 w5=4 54CK_PERM=1 w5=64 > 49523 [SYN, ACK] seq=0 Ack=1 win=14300 ten=0 M55=1430 SACK_PERM=1 w5=64 > http:[SYN, ACK] seq=0 Ack=1 win=14300 ten=0 M55=1430 SACK_PERM=1 w5=64 > http:[Ack: 1, ten: 0
No. Time Source Destination 12 1.155247000 192,168.1.1 192,168.1.30 13 1.222568000 192,168.1.130 172,17,0224 14 1.576555000 192,168.1.130 74,125,225,225,209 15 1.576555000 192,168.1.130 74,125,225,225,209 16 1.611293000 192,168.1.130 74,125,225,209 18 1.611553000 74,125,225,209 192,168.1.130 7 1.611553000 74,125,225,209 192,168.1.130 7 1.611553000 74,125,225,209 192,168.1.30 6 Transmission Control Protocol, Src Port: 49523 (4952 Source port: 49523 (4952) 9 Destination port: http (80) [Stram index: 2] Sequence number: 1 (relative sequence number) Acknowledgment number: 1 (relative ack number) Header length: 20 bytes # Flags: 0x010 (AcK) 000, = Nonce: Not Set 0 0 = Congestion window Reduced (twR) 0	Protocol Length Info DNS 134 Starn SNAP 139 get- TCP 66 43952 TCP 66 64952 TCP 66 64952 TCP 66 61ttp TCP 54 4952 TCP 66 http ""	<pre>land query response 0xded2</pre>
12:1.155247000 192.166.1.1 192.166.1.130 13:1.25555000 192.166.1.130 74.125.225.205 14:1.576555000 192.166.1.130 74.125.225.205 15:1.576555000 192.166.1.130 74.125.225.205 16:1.611248000 74.125.225.209 192.166.1.130 17:1.611249000 74.125.225.209 192.166.1.130 ■ Transmission Control Protocol, Src Port: 49523 (4952) Source port: 49523 (4952) Destination port: http (80) [Stram index:2] Sequence number: 1 (relative sequence number) Acknowledgment number: 1 (relative sequence number) Acknowledgment number: 1 (relative sequence number) Header length: 20 bytes ■ Flag: 0x010 (AcK) 000 Reserved: Not Set 0 = Nonce: Not Set 0	DNS IS4 Stan SNMP II0 getc TCP 66 4932 TCD 66 4332 TCP 66 44932 TCP 66 http TCP 66 http = = = = = = = = = =	<pre>land query response 0xded2</pre>
<pre>13.1.232568000 192.168.1.130 172.17.0.24 13.1.575555000 192.168.1.130 74.125.225.20 15.1.157.25255200 192.168.1.130 15.1.611248000 192.168.1.130 74.125.225.20 18.1.611253000 192.168.1.130 74.125.225.20 192.168.1.130 171.61129000 192.168.1.120 74.125.25.20 192.168.1.130 10.12 10</pre>	SNAP 110 (pet- TCP 66 (3952) TCP 68 (3952) TCP 66 (1952) TCP 56 (1952) TCP 56 (1952) TCP 56 (1952) TCP 66 (1952) TCP 56 (1952) TCP	equest 1.3.6.1.2.1.25.3.2.1.5.1.1.3.6.1.2.1.25.3.5.1.2.1.25.3.5.1.1.1.1.1.3.6.1.2.1.25.3.5.1. :> http [SNU] seqn=0 win=5122 ten=0 555=1460 WS=4 SACK_PERM=1 :> http [SNU] seqn=0 win=5122 ten=0 555=1460 WS=4 SACK_PERM=1 :> http [ACK] seqn=1 Ack=1 win=14300 ten=0 MSS=1430 SACK_PERM=1 WS=64 :> http [ACK] seqn=1 Ack=1 win=14300 ten=0 MSS=1430 SACK_PERM=1 WS=64 :> 49522 [SYN, ACK] seq=0 Ack=1 win=14300 ten=0 MSS=1430 SACK_PERM=1 WS=64), Seq: 1, Ack: 1, ten: 0
14 1.576595000 192.168.1.130 74.125.225.209 15 3.576545000 192.168.1.130 74.125.225.209 16 1.611283000 74.125.225.209 192.168.1.130 17 1.611293000 192.168.1.130 74.125.225.209 18 1.611553000 74.125.225.209 192.168.1.130 4 ■ Transmission Control Protocol, Src Port: 49523 (4952 Source port: 49523 (49523) Destination port: http (80) [Stream index: 2] Sequence number: 1 (relative sequence number) Acknowledgment number: 1 (relative sequence number) Acknowledgment number: 1 (relative sequence number) Header length: 20 bytes ■ Flag: 0x010 (AcK) 000 = Reserved: Not set 0	TCP 66 4952 TCP 66 6952 TCP 66 6http TCP 54 4952 TCP 66 http # # # 3), Dst Port: http (80	<pre>> http [SYN] seq=0 win=8192 Len=0 vsG=1460 wS=4 SACK_PERM=1 > http [SYN] seq=0 win=8192 Len=0 vsG=1430 uS=4 SACK_PERM=1 > 49523 [SYN, ACK] seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 wS=64 > http [Ack] seq=1 Ack=1 win=5780 Len=0 > 49522 [SYN, ACK] seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 wS=64), seq: 1, Ack: 1, Len: 0</pre>
15 3.576754000 102.168.1100 74.125.2525.209 16 16.1611218000 74.125.252.209 102.168.1.300 17 1.611293000 192.168.1.30 74.125.252.209 18 1.611553000 74.125.225.209 192.168.1.30 □ Transmission Control Protocol, Src Port: 49523 (4952) Source port: 49523 (4952) Destination port: http (80) [Stream index: 2] Sequence number: 1 (relative sequence number) Acknowledgment number: 1 (relative ack number) Header length: 20 bytes □ Flag: 0x010 (AcK) 000 = Reserved: Not set 0	TCP 66 43952 TCP 66 http TCP 54 4952 TCP 66 http "" 33), Dst Port: http (80	<pre>i> http [SYN] seq=0 win=8192 ten=0 sSG=1460 wSu=4 SACK_PPENM=1 > 49523 [SYN, ACK] Seq=0 ACk=1 win=14300 ten=0 MSS=1430 SACK_PERM=1 wS=64 > http [ACK] Seq=1 Ack=1 win=65780 ten=0 > 49522 [SYN, ACK] Seq=0 Ack=1 win=14300 ten=0 MSS=1430 SACK_PERM=1 wS=64), Seq: 1, Ack: 1, ten: 0</pre>
16 1.611218000 74.125.225.209 192.168.1.130 17 1.611293000 192.168.1.130 74.125.225.209 18 1.611553000 74.125.225.209 192.168.1.130 Transmission Control Protocol, Src Port: 49523 (4952 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 ■ Flag: 0x010 (AcK) 000 = Reserved: Not set 0 = Kon-Echo: Not set 0	TCP 66 http TCP 54 4952 TCP 66 http " " " " "	> 49523 [SYN, ACK] Seq=0 ACK=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 wS=64 > http [ACK] Seq=1 ACK=1 win=5780 Len=0 > 49522 [SYN, ACK] Seq=0 ACK=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 wS=64), Seq: 1, ACK: 1, Len: 0
17 1.611293000 192.168.1.130 74.125.225.209 18 1.611293000 74.125.225.209 192.168.1.130	TCP 54 4952 TCP 66 http 33), Dst Port: http (80	<pre>> http [ACk] Seq=1 Ack=1 win=65780 Len=0 > 49522 [Syn, Ack] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 wS=64), Seq: 1, Ack: 1, Len: 0</pre>
18 1.611553000 74.125.225.209 192.168.1.130 ■ Transmission Control Protocol, Src Port: 49523 (4952 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 ■ Flag: 0x010 (AcK) 000 = Reserved: Not set0 = Kone: Not set0	TCP 66 http ""	> 49522 [SYN, ACK] Seq=0 ACK=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 wS=64
<pre> Transmission Control Protocol, Src Port: 49523 (4952 Source port: 49523 (49523) Destination port: http (80) [Stream index: 2] Sequence number: 1 (relative sequence number) Acknowledgment number: 1 (relative ack number) Meader length: 20 bytes Flags: 0x010 (AcK) 000 Reserved: Not set 0 = Nonce: Not set 0 = Congestion window Reduced (twR) 0 = ECN-Echo: Not set 0</pre>	"" 3), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
	: Not set	

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?