In the Wireshark Project 1, you learned how to view traffic in Wireshark. In this project (which assumes you have already completed Wireshark Project 1), you'll analyze additional characteristics of your network's traffic.

As with Project 1, this project is written to work with a Windows 7 workstation; however, the steps are very similar for versions of Wireshark running on other operating systems. Again, your workstation should have TCP/IP properly installed and configured and be connected to the Internet. You should also be logged on as a user with administrator-equivalent privileges.

- 1. Begin with an existing capture session—that is, keep the session you generated from Project 1 or create a new group of data by generating and capturing about two minutes of traffic over the Web and via the command line interface.
- 2. Wireshark provides several methods for analyzing a group of data. To begin, click Statistics in the main menu and then click Summary. The Wireshark Summary window appears.
- 3. How many packets did you capture? What was their average size?

Packets - Captured: 5992; Average packet size - 347;

Statistics			
Measurement	Captured	Displayed	Marked
Packets	29946	29946 (100.0%)	_
Time span, s	1055.057	1055.057	_
Average pps	28.4	28.4	_
Average packet size, B	509	509	_
Bytes	15229143	15229143 (100.0%)	0
Average bytes/s	14 k	14 k	_
Average bits/s	115 k	115 k	_

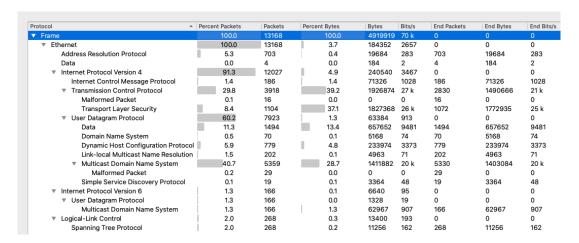
- 4. Close the Wireshark: Summary window.
- 5. Click **Statistics** in the main menu and then click **Protocol Hierarchy**. The Wireshark: Protocol Hierarchy Statistics window appears, revealing, for example, the percentage of your traffic that used Ethernet frames, the percentage that used IP and TCP, and so on.
- a. Did any of your traffic use a type of frame that was not Ethernet? No
- b. What percentage of your traffic relied on IP?

Internet Protocol Version 6 - Percent Packets - 1.3;

Internet Protocol Version 4 - Percent Packets - 91.3;

c. How many of your packets, if any, used IPv6?

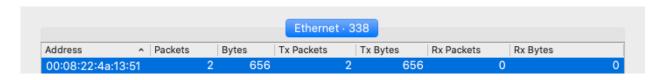
Internet Protocol Version 6 - Packets - 166;



- 6. Close the Wireshark: Protocol Hierarchy Statistics window.
- 7. Click **Statistics** on the main menu and then click **Endpoints**. The Endpoints window appears, with the Ethernet tab selected by default. Wireshark defines endpoints as a logical end of any transmission, such as a node, and identifies each endpoint with an IP address or MAC address.
- 8. In the Ethernet tab, nodes are listed in order of the highest volume of traffic generated and received, cumulatively. What node sits at the top of this list, and what kind of equipment does it represent?

Address: 00:08:22:4a:13:51

Packets: 2
Bytes: 656
TxPackets: 2
TxBytes: 656
Rx Packets: 0
Rx Bytes: 0



9. Click the **IPv4** tab. A list of endpoints appears. As with the endpoints listed in the Ethernet tab, the one responsible for the greatest number of bytes transmitted and received (cumulatively), is listed first. **Which IP address is at the top of this list? To what node** does it belong?

Address: 0.0.0.0
Packets: 1,377
Bytes: 475 k
Tx Packets: 1,400
Tx Bytes: 490 k
Rx Packets: 0
Rx Bytes: 0
Country: —
City: —
AS Number: —
AS Organization: —

