Wireshark Project 2

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.

To show me that you have successfully completed Wireshark Project 2, you will need to submit a word file with the answer two questions: 3, 5, 8, 9

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;

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	13168	100.0	4919919	70 k	0	0	0
▼ Ethernet	100.0	13168	3.7	184352	2657	0	0	0
Address Resolution Protocol	5.3	703	0.4	19684	283	703	19684	283
Data	0.0	4	0.0	184	2	4	184	2
▼ Internet Protocol Version 4	91.3	12027	4.9	240540	3467	0	0	0
Internet Control Message Protocol	1.4	186	1.4	71326	1028	186	71326	1028
▼ Transmission Control Protocol	29.8	3918	39.2	1926874	27 k	2830	1490666	21 k
Malformed Packet	0.1	16	0.0	0	0	16	0	0
Transport Layer Security	8.4	1104	37.1	1827368	26 k	1072	1772935	25 k
▼ User Datagram Protocol	60.2	7923	1.3	63384	913	0	0	0
Data	11.3	1494	13.4	657652	9481	1494	657652	9481
Domain Name System	0.5	70	0.1	5168	74	70	5168	74
Dynamic Host Configuration Protocol	5.9	779	4.8	233974	3373	779	233974	3373
Link-local Multicast Name Resolution	1.5	202	0.1	4963	71	202	4963	71
▼ Multicast Domain Name System	40.7	5359	28.7	1411882	20 k	5330	1403084	20 k
Malformed Packet	0.2	29	0.0	0	0	29	0	0
Simple Service Discovery Protocol	0.1	19	0.1	3364	48	19	3364	48
▼ Internet Protocol Version 6	1.3	166	0.1	6640	95	0	0	0
▼ User Datagram Protocol	1.3	166	0.0	1328	19	0	0	0
Multicast Domain Name System	1.3	166	1.3	62967	907	166	62967	907
▼ Logical-Link Control	2.0	268	0.3	13400	193	0	0	0
Spanning Tree Protocol	2.0	268	0.2	11256	162	268	11256	162

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

Ethernet · 338

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:08:22:4a:13:51	2	656	2	656	0	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: —