The bottom window in Figure 4.15 shows the exact bytes that were captured. The section highlighted in grey shows the HTTP packet. The numbers on the left show the data in hexadecimal format while the data on the right show the text version. The data before the highlighted section is the TCP packet.

From Chapter 2, you know that the client sends an HTTP request packet to request a Web page, and the Web server sends back an HTTP response packet. Packet number 25 in the top window in Figure 4.15 is the HTTP response sent back to my computer by the Yahoo server. You can see that the destination IP address in my HTTP request is the source IP address of this HTTP packet.

5. Figure 4.15 also shows what happens when you click the plus sign (+) in front of the Ethernet II packet to expand it. You can see that this Ethernet packet has a destination address and source address (e.g., 00:02:2d:85:cb:e0).

Deliverables

1. List the layer 2, 3, 4, and 5 PDUs that are used in your network to send a request to get a Web page.
2. List the source and destination Ethernet addresses on the message.
3. What value is in the Ethernet type field in this message? Why?

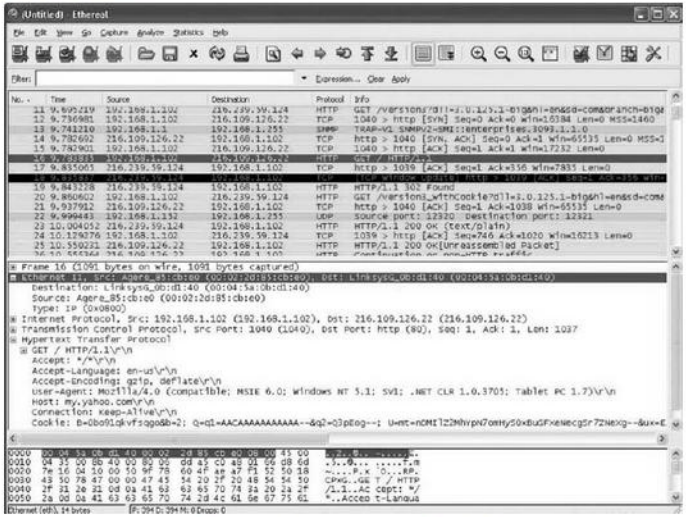

FIGURE 4.15 Analyzing packets with Wireshark