

## 81 CHAPTER 1 • COMPUTER NETWORKS AND THE INTERNET

The screenshot shows the Wireshark interface with the following components:

- Command menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Help.
- Filter:** http
- Listing of captured packets:**

No.	Time	Source	Destination	Protocol	Info
121	4.954082	128.119.245.136	165.193.123.224	HTTP	GET /kurose-ross HTTP/1.1
124	4.969038	165.193.123.224	128.119.245.136	HTTP	HTTP/1.1 302 Moved Temporarily
129	5.018429	128.119.245.136	165.193.123.218	HTTP	GET /kurose-ross HTTP/1.1
131	5.036939	165.193.123.218	128.119.245.136	HTTP	HTTP/1.1 302 Moved Temporarily
139	5.056789	128.119.245.136	165.193.123.218	HTTP	GET /kurose-ross/ HTTP/1.1
146	5.079867	165.193.123.218	128.119.245.136	HTTP	[TCP out-of-order] HTTP/1.1 200 OK
158	5.154773	128.119.245.136	165.193.123.218	HTTP	GET /kurose-ross/banner.gif HTTP/1.1
159	5.154860	128.119.245.136	165.193.123.218	HTTP	GET /kurose-ross/net3e.jpg HTTP/1.1
212	5.219770	165.193.123.218	128.119.245.136	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
214	5.220261	128.119.245.136	165.193.123.218	HTTP	GET /kurose-ross/net2e.jpg HTTP/1.1
222	5.234456	128.119.245.136	165.193.123.218	HTTP	GET /kurose-ross/pearson.gif HTTP/1.1
259	5.310633	128.119.245.136	165.193.123.218	HTTP	GET /favicon.ico HTTP/1.1
265	5.327525	165.193.123.218	128.119.245.136	HTTP	HTTP/1.1 200 OK (image/x-icon)
- Details of selected packet header:**
  - Frame 121 (470 bytes on wire, 470 bytes captured)
  - Ethernet II, Src: wistron\_23:68:8a (00:16:d3:23:68:8a), Dst: DigitalE\_00:e8:0b (aa:00:04:00:e8:0b)
  - Internet Protocol, Src: 128.119.245.136 (128.119.245.136), Dst: 165.193.123.224 (165.193.123.224)
  - Transmission Control Protocol, Src Port: 2108 (2108), Dst Port: http (80), Seq: 1, Ack: 1, Len: 416
  - Hypertext Transfer Protocol
- Packet contents in hexadecimal and ASCII:**

```

0020 7b e0 08 3c 00 50 11 ad b5 36 f4 f2 3e 53 50 18  { .<.P...6.>SP.
0030 ff ff 99 5c 00 00 47 45 54 20 2f 6b 75 72 6f 73  ..\...GE T /kuros
0040 65 2d 72 6f 73 73 20 48 54 54 50 2f 31 2e 31 0d  e-ross H TTP/1.1.
0050 0a 48 6f 73 74 3a 20 77 77 77 2e 61 77 6c 2e 63  .Host: w ww.awl.c
0060 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20  om..User -Agent:
0070 4d 6f 73 6d 6c 6c 7f 25 2a 2b 2c 2d 2e 2f 30 21 11- / 5 8 7a 2a

```

Figure 1.29 ♦ A Wireshark screen shot

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer passively copies (sniffs) messages being sent from and received by your computer; it also displays the contents of the various protocol fields of these captured messages. A screenshot of the Wireshark packet sniffer is shown in Figure 1.29. Wireshark is a free packet sniffer that runs on Windows, Linux/Unix, and Mac computers. Throughout the textbook, you will find Wireshark labs that allow you to explore a number of the protocols studied in the chapter. In this first Wireshark lab, you'll obtain and install a copy of Wireshark, access a Web site, and capture and examine the protocol messages being exchanged between your Web browser and the Web server.

You can find full details about this first Wireshark lab (including instructions about how to obtain and install Wireshark) at the Web site <http://www.awl.com/kurose-ross>.