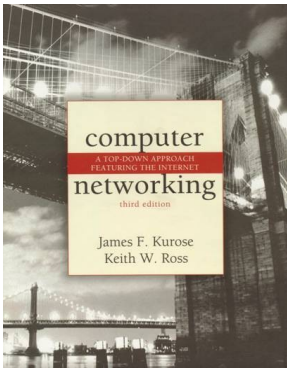
Ethereal: Getting Started



Computer Networking: A Top-down Approach Featuring the Internet, 3rd edition.

"Tell me and I forget. Show me and I remember. Involve me and I understand."
Chinese proverb

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences.

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a *copy* of packets that are sent/received from/by application and protocols executing on your machine.

Figure 1 shows the structure of a packet sniffer. At the right of Figure 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client)

that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 1 is an addition to the usual software in your computer, and consists of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. Recall from the discussion from section 1.7.2 in the text (Figure 1.18[1]) that messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

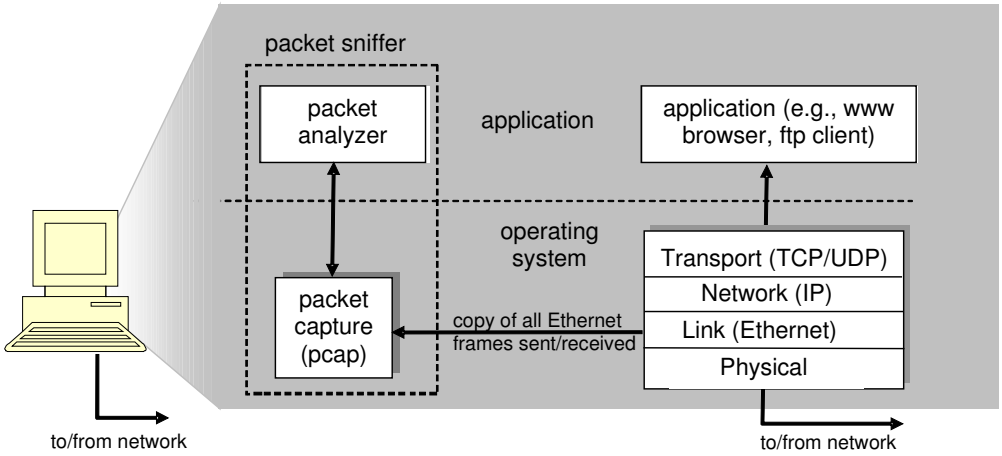


Figure 1: Packet sniffer structure

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 1. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string "GET," "POST," or "HEAD," as shown in Figure 2.8 in the text.

[1] Figure numbers refer to figures in the 3rd edition of our text.

We will be using the Ethereal packet sniffer [http://www.ethereal.com], allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Ethereal is a packet analyzer that uses a packet capture library in your computer). Ethereal is a free network protocol analyzer that runs on Windows, Linux/Unix, and Mac computers. It's an ideal packet analyzer – it is stable, has a large user base and well-documented support that includes a user-guide (http://www.ethereal.com/docs/user-guide/), man pages (http://www.ethereal.com/ethereal.1.html), and a detailed FAQ (http://www.ethereal.com/faq.html), rich functionality that includes the capability to analyze more than 500 protocols, and a well-designed user interface. It operates in computers using Ethernet to connect to the Internet, as well as so-called point-to-point protocols such as PPP. Incidentally, some people pronounce the name Ethereal as "ether-real," while others pronounce it "e-thir-E-al," as in the English word ethereal, which means ghostly or insubstantial. The name's origin comes from the Ethernet protocol, a link-level protocol that we will study extensively in Chapter 5 of the text.

Getting Ethereal

In order to run Ethereal, you will need to have access to a computer that supports both Ethereal and the *libpcap* packet capture library. If the *libpcap* software is not installed within your operating system, you will need to install *libpcap* or have it installed for you in order to use Ethereal. See http://www.ethereal.com/download.html for a list of supported operating systems and download sites

Download and install the Ethereal and (if needed) *libpcap* software:

- If needed, download and install the *libpcap* software. Pointers to the *libpcap* software are provided from the Ethereal download pages. For Windows machines, the *libpcap* software is known as *WinPCap*, and can be found at http://winpcap.polito.it/ See FAQ question #2 at http://winpcap.polito.it/ To determine whether or not *WinPCap* is already installed on your machine.
- Go to http://www.ethereal.com and download and install the Ethereal binary for your computer.
- Download the Ethereal user guide. You will most likely only need Chapters 1 and 3.

The Ethereal FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Ethereal.

Running Ethereal

When you run the Ethereal program, the Ethereal graphical user interface shown in Figure 2 will be displayed. Initially, no data will be displayed in the various windows.

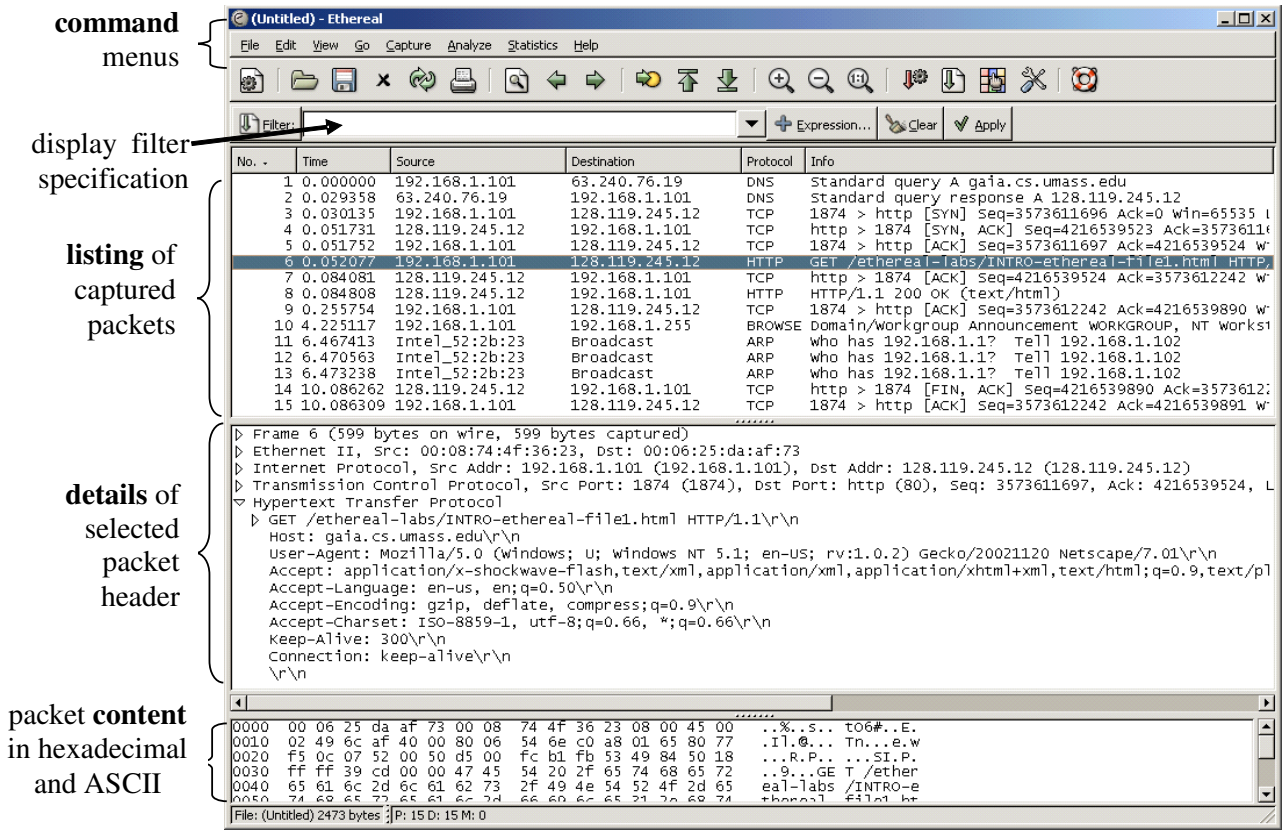


Figure 2: Ethereal Graphical User Interface

The Ethereal interface has five major components:

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Ethereal application. The Capture menu allows you to begin packet capture.
- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Ethereal; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and

protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.

- The **packet-header details window** provides details about the packet selected (highlighted) in the packet listing window. (To select a packet in the packet listing window, place the cursor over the packet's one-line summary in the packet listing window and click with the left mouse button.). These details include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the right-pointing or down-pointing arrowhead to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest level protocol that sent or received this packet are also provided.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Ethereal graphical user interface, is the **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Ethereal hide (not display) packets except those that correspond to HTTP messages.

Taking Ethereal for a Test Run

The best way to learn about any new piece of software is to try it out! Do the following

1. Start up your favorite web browser, which will display your selected homepage.

2. Start up the Ethereal software. You will initially see a window similar to that shown in Figure 2, except that no packet data will be displayed in the packet-listing, packet-header, or packet-contents window, since Ethereal has not yet begun capturing packets.

3. To begin packet capture, select the Capture pull down menu and select *Start*. This will cause the "Ethereal: Capture Options" window to be displayed, as shown in Figure 3.

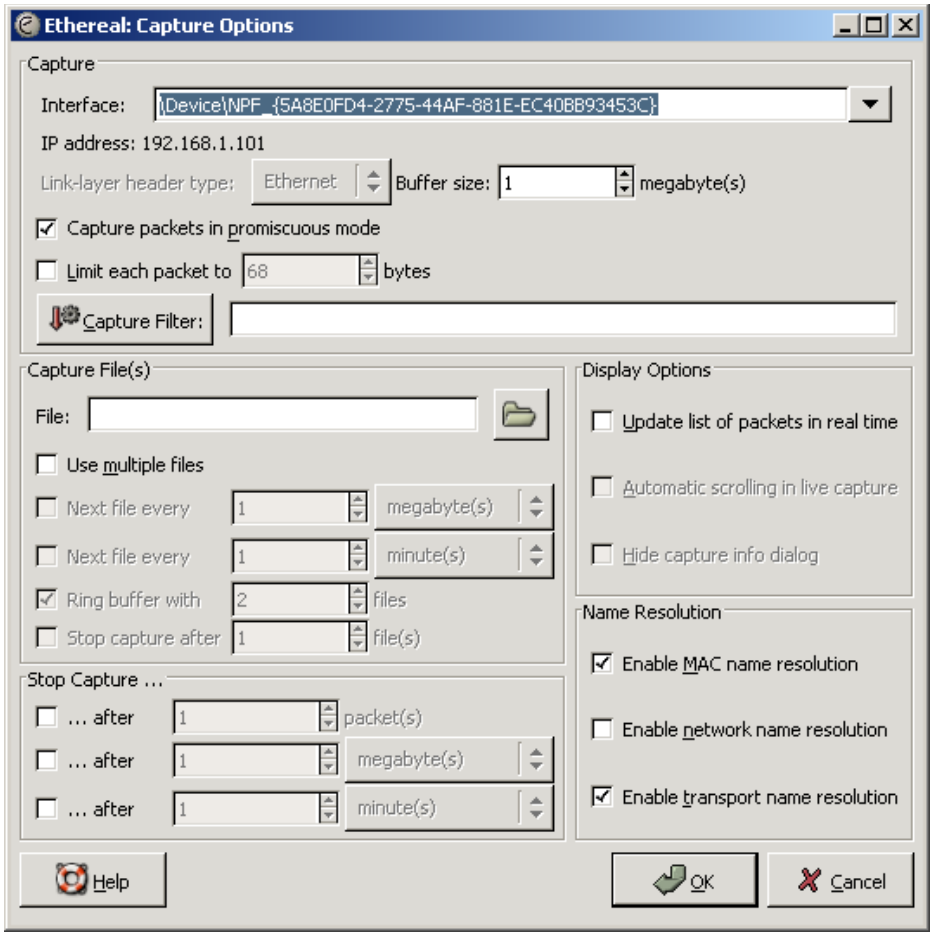


Figure 3: Ethereal Capture Options Window

4. You can use all of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window. In case your computer has more than one active network interface (e.g., if you have both a wireless and a wired Ethernet connection), you will need to select an interface that is being used to send and receive packets (mostly likely the wired interface). After selecting the network interface (or using the default interface chosen by Ethereal), click OK. Packet capture will now begin - all packets being sent/received from/by your computer are now being captured by Ethereal!

5. Once you begin packet capture, a packet capture summary window will appear, as shown in Figure 4. This window summarizes the number of packets of various types that are being captured, and (importantly!) contains the *Stop* button that will allow you to stop packet capture. Don't stop packet capture yet.

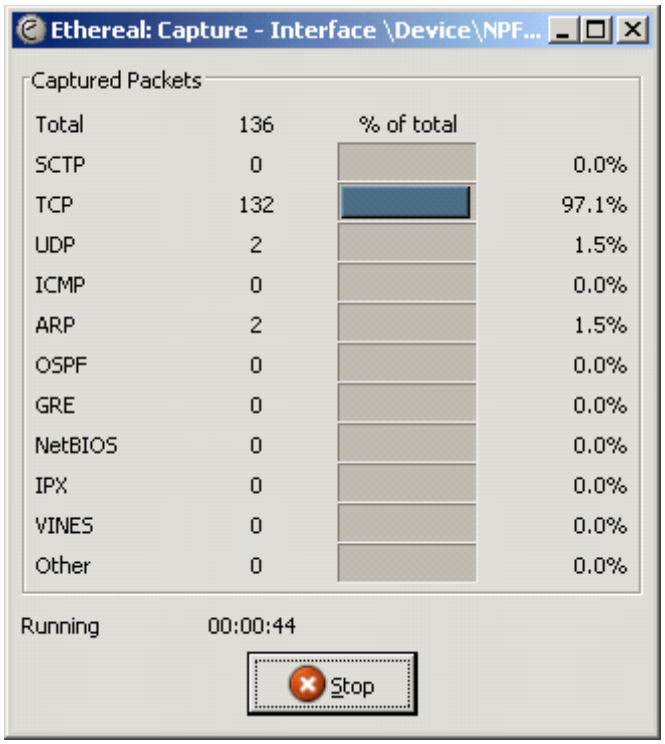


Figure 4: Ethereal Packet Capture Window

6. While Ethereal is running, enter the URL:

   http://katahdin.cs.dartmouth.edu/~sensorlab/metrosense/index.html

   and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at katahdin.cs.dartmouth.edu and exchange HTTP messages with the server in order to download this page, as discussed in section 2.2 of the text. The Ethernet frames containing these HTTP messages will be captured by Ethereal.

7. After your browser has displayed the index.html page, stop Ethereal packet capture by selecting stop in the Ethereal capture window. This will cause the Ethereal capture window to disappear and the main Ethereal window to display all packets captured since you began packet capture. The main Ethereal window should now look similar to Figure 2. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the katahdin.cs.dartmouth.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the *Protocol* column in Figure 2). Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user. For now, you

should just be aware that there is often much more going on than "meet's the eye"!

8. Type in "http" (without the quotes, and in lower case – all protocol names are in lower case in Ethereal) into the display filter specification window at the top of the main Ethereal window. Then select *Apply* (to the right of where you entered "http"). This will cause only HTTP message to be displayed in the packet-listing window.

9. Select the first http message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the katahdin.cs.dartmouth.edu HTTP server. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window[2]. By clicking on right-pointing and down-pointing arrowsheads to the left side of the packet details window, *minimize* the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. *Maximize* the amount information displayed about the HTTP protocol. Your Ethereal display should now look roughly as shown in Figure 5 (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).

10. Exit Ethereal

[2] Recall that the HTTP GET message that is sent to the katahdin.cs.dartmouth.edu web server is contained within a TCP segment, which is contained (encapsulated) in an IP datagram, which is encapsulated in an Ethernet frame. If this process of encapsulation isn't quite clear yet, review section 1.7 in the text

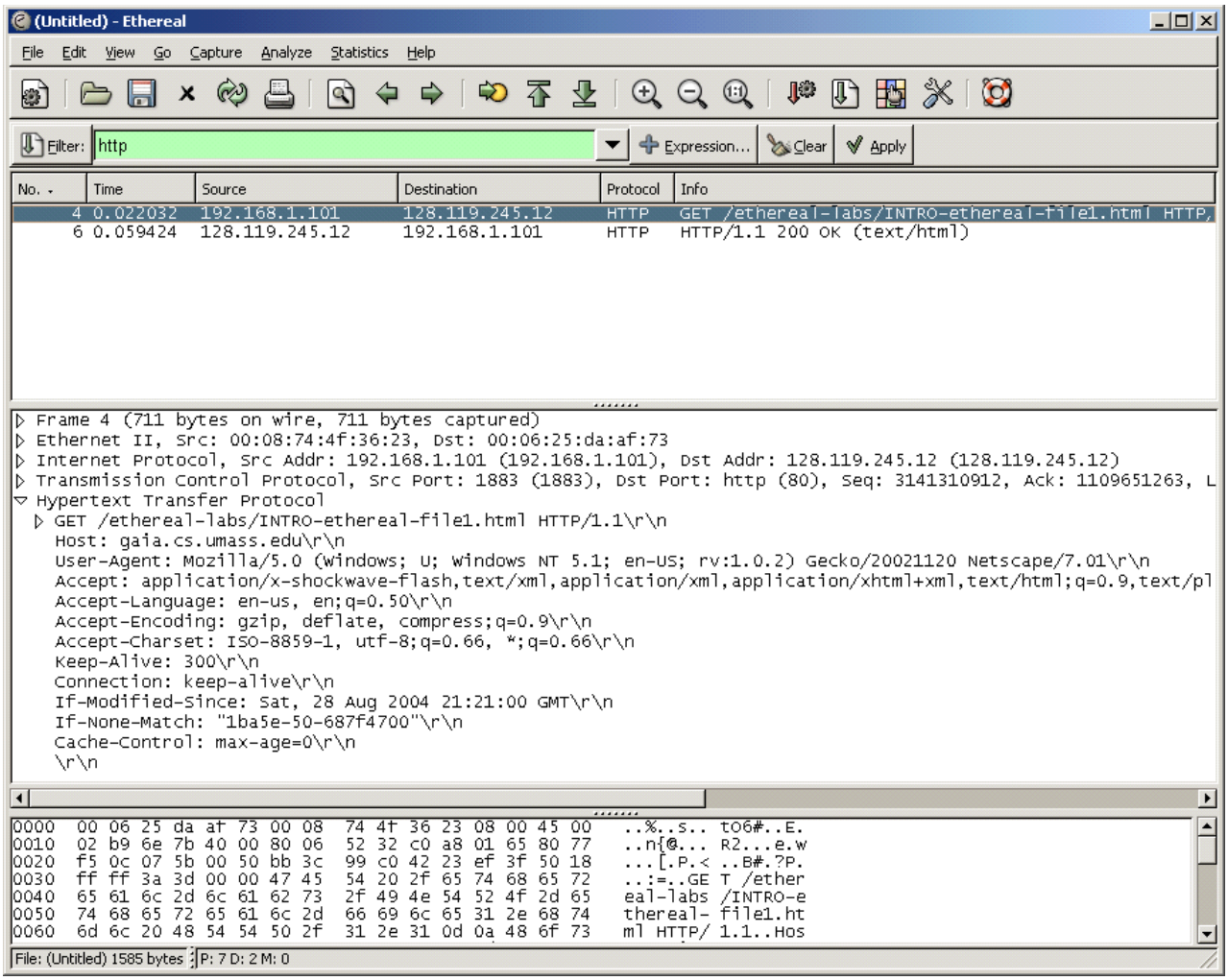


Figure 5: Ethereal display after step 9