Ethereal User's Guide

Richard Sharpe
NS Computer Software and Services P/L

Ethereal User's Guide:
by Richard Sharpe

First edition Edition
Published 2000

Table of Contents

List of Tables

List of Figures

List of Examples

Chapter 1. Introduction

1.1. What is Ethereal?

Every network manager at some time or other needs a tool that can capture packets off the network and analyze them. In the past, such tools were either very expensive, propietary, or both. However, with the advent of Ethereal, all that has changed

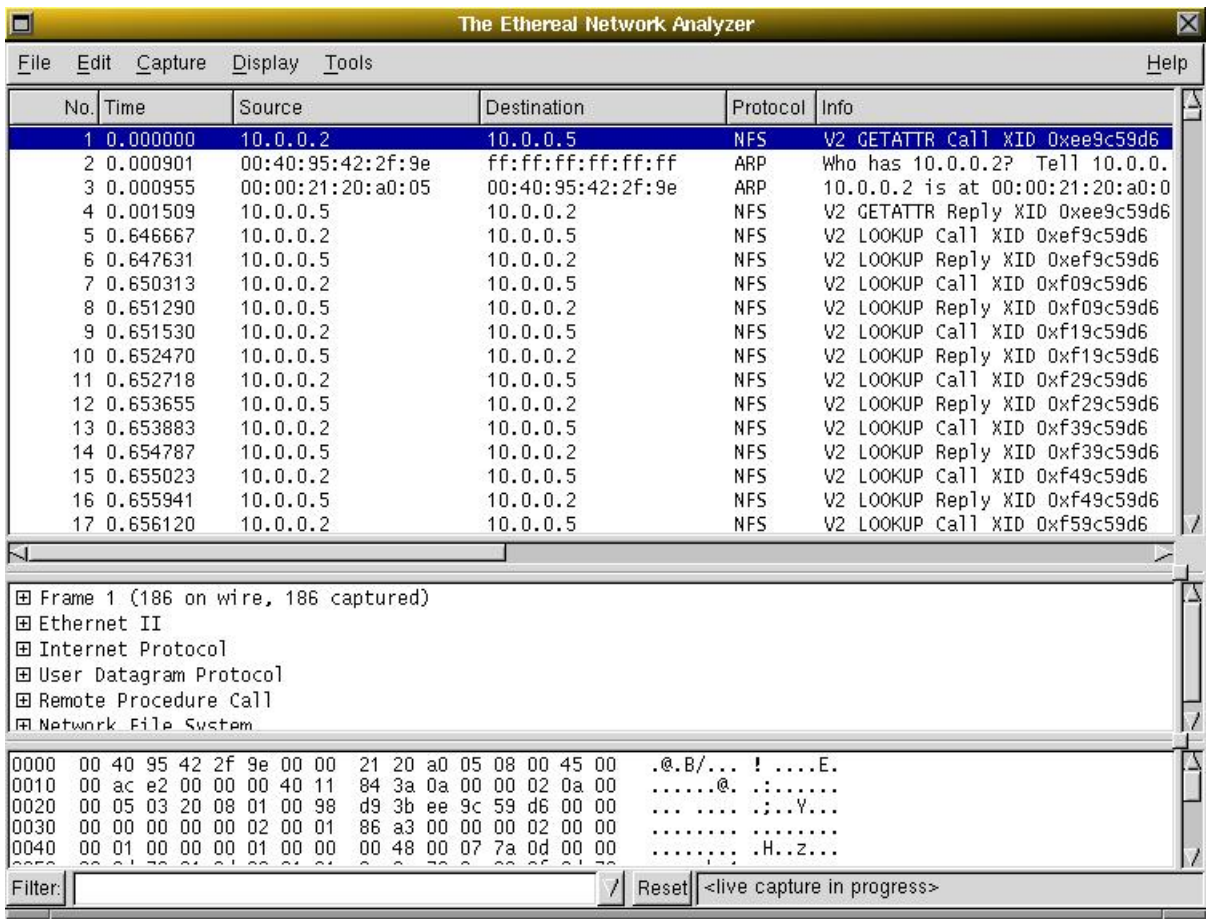
Ethereal is perhaps one the best open source packet sniffers available today. It provides the following broad functions:

- Capture and display packets from any interface on a UNIX system
- Display packets captured under a number of other capture programs:
  - tcpdump
  - Network Associates Sniffer and Sniffer Pro
  - NetXray
  - LANalyzer
  - Shomiti
  - AIX's iptrace
  - RADCOM's WAN/LAN Analyzer
  - Lucent/Ascend access products
  - HP-UX's nettl
  - Toshiba's ISDN routers
  - ISDN4BSD *i4btrace* utility
  - Microsoft Network Monitor
  - Sun snoop

- Filter packets on many criteria

Figure 1-1 shows Ethereal having captured some packets and waiting for you to examine the packets.

Figure 1-1. Ethereal captures packets and allows you to examine their content.



In addition, because all the source code for Ethereal is freely available, it is very easy

for people to add new protocols to Ethereal, either as modules, or built into the source.

There are currently protocol decoders (or dissectors, as they are known in Ethereal), for a great many protocols, including:

1.2. The status of Ethereal

Ethereal is an open source software project, and is released under the GPL. All source cose is freely available under the GPL. You are welcome to modify Ethereal to suit your own needs, and it would be appreciated if you contribute your improvements back to the Ethereal team.

The Ethereal source code and binary kits for some platforms are all available on the Ethereal website: http://www.zing.org.

1.3. Development and maintenance of Ethereal

Ethereal was initially developed by Gerald Combs. Ongoing development and maintenance of Ethereal is handled by the Ethereal team, a loose group of individuals who fix bugs and provide new functionality.

There have also been a large number of people who have contributed protocol dissectors to Ethereal, and it is expected that this will continue.

1.4. A rose by any other name

William Shakespeare wrote: *"A rose by any other name would smell as sweet."* And so it is with Ethereal, as there appears to be two different ways that people pronounce the name.

Some people pronounce it ether-real, while others pronounce it e-the-real, as in ghostly, insubstantial, etc.

You are welcome to call it what you like, as long as you find it useful.

1.5. A brief history of Ethereal

In late 1997, Gerald Combs needed a tool for tracking down networking problems and wanted to learn more about networking, so he started writing Ethereal as a way to solve both problems.

Ethereal was initially released, after several pauses in development, in July 1998 as version 0.2.0. Within days, patches, bug reports, and words of encouragement started arriving, so Ethereal was on its way to success.

Not long after that Gilbert Ramirez saw its potential and contributed a low-level dissector to it.

In October, 1998, Guy Harris, of NetApp was looking for something better than TCPview, so he started applying patches and contributing dissectors to Ethereal.

In late 1998, Richard Sharpe, who was giving TCP/IP courses, saw its potential on such courses, started looking at it to see if it supported the protocols he needed. While it didn’t at that point, new protocols could be easily added. So he started contributing dissectors and contributing patches.

The list of people who have contributed to Ethereal is long, and almost all of them started with a protocol that they needed that Ethereal did not already handle, so they copied an existing dissector and contributed the code bact to the team. You can get a list of the people who have contributed by clicking on the About Ethereal... menu item in the Help menu on the main menu bar.

1.6. Platforms Ethereal runs on

Ethereal currently runs on most UNIX platforms and the various Windows platforms. It requires GTK+, GLIB and libpcap in order to run.

Binary packages are available for the following platforms:

- AIX
- Tru64 UNIX (formerly Digital UNIX)
- Debian GNU/Linux
- Slackware Linux
- Red Hat Linux
- FreeBSD
- NetBSD
- OpenBSD
- HP/UX
- Sparc/Solaris 8
- Windows NT and 98

If a binary package is not available for your platform, you should download the source and try to build it.

1.7. Where to get Ethereal

You can get the latest copy of the Ethereal from the Ethereal Website: http://www.zing.org. The website allows you to choose from among several mirrors for downloading.

1.8. Reporting problems and getting help

If you have problems, or need help with Ethereal, there are several mailing lists that may be of interest to you:

Ethereal Users

This list is for users of Ethereal. People post with questions about building and using Ethereal. Others provide answers.

Ethereal Announce

This list is for people wanting to receive announcements about Ethereal.

Ethereal Dev

This list is for Ethereal developers. If you want to start developing a protocol dissector, join this list.

You can subscribe to each of these from the Ethereal web site: http://www.zing.org. Simply select the **mailing lists** link on the left hand side of the site. The lists are archived at the Ethereal web site as well.

When reporting crashes with Ethereal, it is helpful if you supply the following information:

1. The version number of Ethereal you found the problem with, eg Ethereal 0.8.10.
2. The version number of the other software linked with Ethereal, eg GTK+, etc. You can obtain this with the command **ethereal -v**.
3. A traceback if Ethereal crashed. You can obtain this with the following commands:

   ```
   gdb ‘whereis ethereal | cut -f2 -d: | cut -f’ ’ -d2‘ core
   traceback
   ```

   Note!: Type the characters in the first line verbatim! Those are back-tics there!

1.9. Where to get the latest copy of this document

The latest copy of this documentation can always be found on the Ethereal web site: http://www.zing.org. It can also be found at: TBD.

1.10. Providing feedback

Should you have any feedback about this document, please send them to the author at rsharpe@ns.aus.com.

Chapter 2. Building and Installing Ethereal

2.1. Introduction

As with all things, there must be a beginning, and so it is with Ethereal. To use Ethereal, you must:

- Obtain a binary package for your operating system, or
- Obtain the source and build Ethereal for your operating system

Currently, only two or three Linux Distributions ship ethereal, and they are commonly shipping an out-of-date version. No other versions of UNIX ship Ethereal so far, and Microsoft does not ship it with any version of Windows. For that reason, you will need to know where to get the latest version of Ethereal and how to install it. The current version of Ethereal is 0.8.10.

This chapter shows you how to obtain source and binary packages, and how to build Ethereal from source, should you choose to do so.

The following are the general steps you would use:

1. Download the relevant package for your needs, eg, source or binary distribution.
2. Build the source into a binary, if you have downloaded the source

   This may involve building and/or installing any other necessary packages

3. Install the binaries in their final destinations

2.2. Obtaining the source and binary distributions

You can obtain both source and binary distributions from the Ethereal web site: http://www.zing.org. Simply select the download link, and then select either the source package or binary package of your choice from the mirror site closest to you.

> **Download all the needed files:** In general, unless you have already downloaded Ethereal before, you will most likely need to down load several source packages if you are building Ethereal from source. This is covered in more detail below.

Once you have downloaded the relevant files, you can go on to the next step.

> **Note:** While you will find a number of binary packages available on the Ethereal web site, you might not find one for your platform, and they often tend to be several versions behind the current released version, as they are contributed by people who have the platforms they are built for.
>
> For this reason, you might want to pull down the source distribution and build it, as the process is relatively simple.

2.3. Before you build Ethereal

Before you build Ethereal from sources, or install a binary package, you must ensure that you have the following other packages installed:

- GTK+, The GIMP Tool Kit.

  You will also need Glib. Both can be obtained from www.gtk.org

- libpcap, the packet capture software that Ethereal uses.

You can obtain libpcap from www.tcpdump.org

Depending on your system, you may be able to install these from binaries, eg RPMs, or you may need to obtain them in source code form and build them.

If you have downloaded the source for GTK+, the instructions shown in Example 2-1 may provide some help in building it:

Example 2-1. Building GTK+ from source

```
gzip -dc gtk+-1.2.8.tar.gz | tar xv
<much output removed>
cd gtk+-1.2.8
./configure
<much output removed>
make
<much output removed>
make install
<much output removed>
```

Note!: You may need to change the version number of gtk+ in Example 2-1 to match the version of GTK+ you have downloaded.

Note!: If you use Linux, or have GNU **tar** installed, you can use **tar zxvf gtk+-1.2.8.tar.gz**. It is also possible to use **gunzip** rather than **gzip -dc** on many UNIX systems.

Note!: If you downloaded gtk+ or any other tar file using Windows, you may find your file called gtk+-1_2_8_tar.gz.

You should consult the GTK+ web site if any errors occur in carrying out the instructions in Example 2-1.

If you have downloaded the source to libpcap, the general instructions shown in Example 2-2 will assist in building it.

Example 2-2. Building and installing libpcap

```
gzip -dc libpcap-0.5.tar.Z | tar xv
<much output removed>
cd libpcap_0_5rel2
./configure
<much output removed>
make
<much output removed>
make install
<much output removed>
make install-incl
<much output removed>
```

Example 2-3. Errors while installing the libpcap include files

```
   /usr/local/include/pcap.h
/usr/bin/install -c -m 444 -o bin -g bin ./pcap-namedb.h \
   /usr/local/include/pcap-namedb.h
/usr/bin/install -c -m 444 -o bin -g bin ./net/bpf.h \
   /usr/local/include/net/bpf.h
/usr/bin/install: cannot create regular file \
‘/usr/local/include/net/bpf.h’: No such file or directory
make: *** [install-incl] Error 1
```

If you get the error shown in Example 2-3 when you submit the command **make install-incl**, simply create the missing directory with the following command:

```
mkdir /usr/local/include/net
```

and rerun the command **make install-incl**

Under RedHat 6.x you can simply install each of the packages you need from RPMs. Most Linux systems will install GTK+ and Glib in anycase, however, you will probably need to install the devel versions of each of these packages. The commands shown in Example 2-4 will install all the needed RPMs if they are not already installed.

Example 2-4. Installing required RPMs under RedHat Linux 6.2

```
cd /mnt/cdrom/RedHat/RPMS
rpm -ivh glib-1.2.6-3.i386.rpm
rpm -ivh glib-devel-1.2.6-3.i386.rpm
rpm -ivh gtk+-1.2.6-7.i386.rpm
rpm -ivh gtk+-devel-1.2.6-7.i386.rpm
rpm -ivh libpcap-0.4-19.i386.rpm
```

2.4. Building from Source under UNIX

Use the following general steps if you are building Ethereal from source under a UNIX operating system:

1. Unpack the source from its **gzip**'d **tar** file. If you are using Linux, or your version of UNIX uses GNU **tar**, you can use the following command:

   ```
   tar zxvf ethereal-0_8_10-tar.gz
   ```

   For other versions of UNIX, You will want to use the following commands:

   ```
   gzip -d ethereal-0_8_10-tar.gz
   tar xvf ethereal-0_8_10-tar
   ```

2. Change directory to the ethereal source directory.
3. Configure your source so it will build correctly for your version of UNIX. You can do this with the following command:

```
./configure
```

If this step fails, you will have to rectify the problems and rerun **configure**. Troubleshooting hints are provided in Section 2.9.

4. Build the sources into a binary, with the **make** command. For example:

   ```
   make
   ```

5. Install the software in its final destination, using the command:

   ```
   make install
   ```

Once you have installed Ethereal with **make install** above, you should be able to run it by entering **ethereal**.

2.5. Installing the binaries under UNIX

In general, installing the binary under your version of UNIX will be specific to the installation methods used with your version of UNIX. For example, under AIX, you would use **smit** to install the Ethereal binary package, while under

2.6. Installing from RPMs under Linux

Use the following command to install the Ethereal RPM that you have downloaded from the Ethereal web site:

```
rpm -ivh ethereal-0.8.10-1.i386.rpm
```

If the above step fails because of missing dependencies, install the dependencies first, and then retry the step above. See Example 2-4 for information on what RPMs you will need to have installed.

2.7. Building and Installing under Windows

In this section we explore how to build and install Ethereal under Windows. For many people, simply installing from the binary packages available will be sufficient, however, for some people, rebuilding will be required.

Before installing Ethereal under any version of Windows, you must download two other packages:

1. The WinPcap packet capture binary for Windows. This can be downloaded from http://netgroup-serv.polito.it/winpcap/. You should download the version specific to your version of Windows. You can find these under the link that mentions the version number (that is, you don't want the developers pack or the source code).
2. GTK libs for Win32. These are available from the Ethereal web site in the download area as well as from www.gimp.org/~tml/gimp/win32/. However, you will find it easier to download gtk-libs-$version.zip from the Ethereal web site, rather than downloading all the approriate files from the gimp location.

2.7.1. Building from source under Windows

Add a description here.

2.8. Installing Ethereal under Windows

Once you have downloaded the files you need as discussed above and/or built Ethereal from source, you can install each of them:

1. Install WinPcap. There are instructions at the WinPcap web site for installing it under Windows 9X, Windows NT and Windows 2000. These are located at: http://netgroup-serv.polito.it/winpcap/install/Default.htm

2. Install GTK+.

3. Install Ethereal

2.9. Troubleshooting during the install

A para

Chapter 3. Using Ethereal

3.1. Introduction

By now you have installed Ethereal and are most likely keen to get started capturing your first packets. In this chapter we exlore:

- How to start Ethereal
- How to capture packets in Ethereal
- How to view packets Ethereal
- How to filter packets in Ethereal

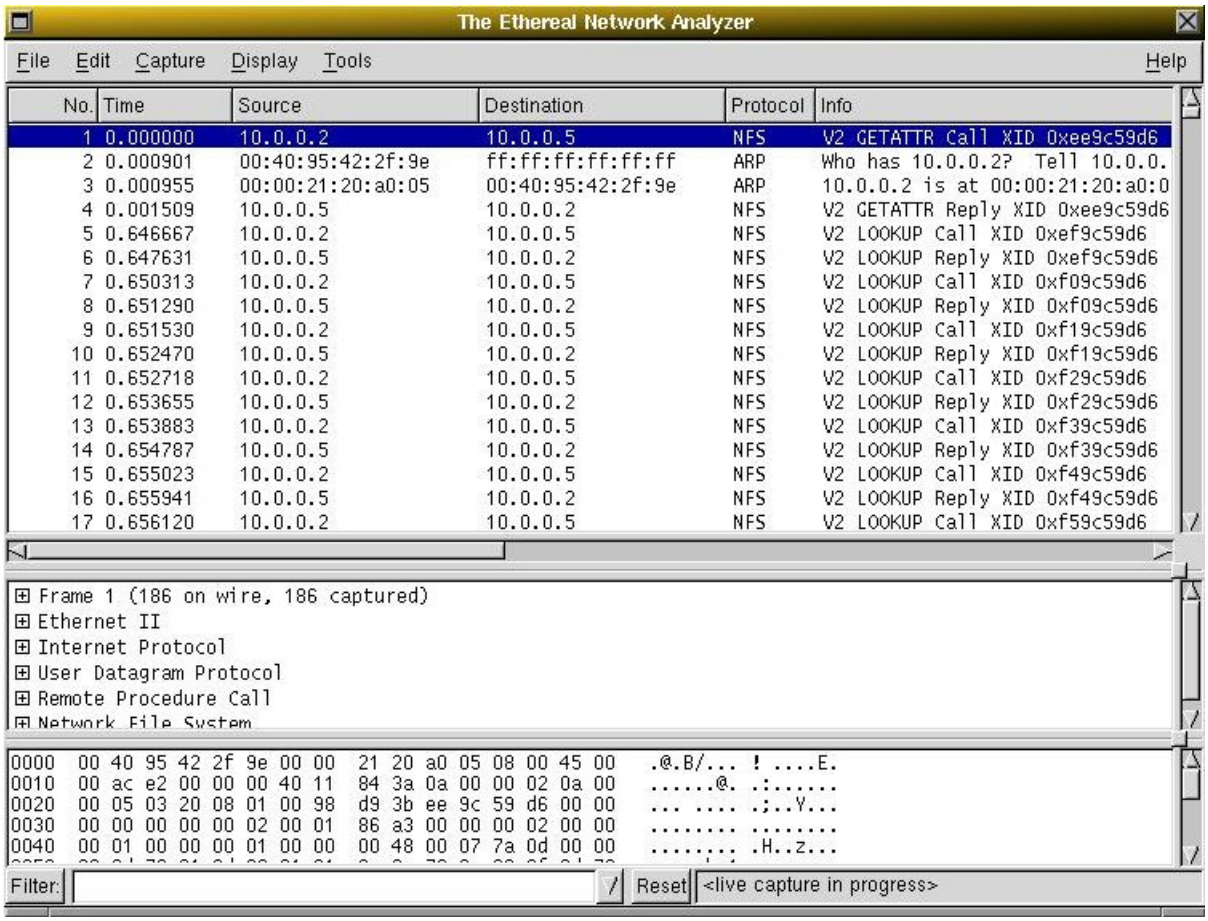
In fact, most of the functionality of Ethereal is explored in this chapter.

3.2. Starting Ethereal

You can start Ethereal from the command line under UNIX, but it can also be started from most Window managers as well. In this section we will look at starting it from the command line.

Before looking at the command line parameters Ethereal understands, lets look at Ethereal itself. Figure 3-1 shows Ethereal as you would usually see it.

Figure 3-1. Ethereal is comprised of three main windows



Ethereal is comprised of three main windows, or panes.

1. The top pane is the packet list pane. It displays a summary of each packet captured. By clicking on packets in this pane your control what is displayed in the other two panes.
2. The middle pane is the tree view pane. It displays the packet selected in the top

pane in more detail.

3. The bottom pane is the data view pane. It displays the data from the packet selected in the top pane, and highlights the field selected in the tree view pane

Ethereal supports a large number of command line parameters. To see what they are, simply enter the command **ethereal -h** and the help information shown in Example 3-1 should be printed.

Example 3-1. Help information available from Ethereal

```
This is GNU ethereal 0.8.10, compiled with GTK+ 1.2.6, with libp-
cap 0.4, with libz 1.1.3, without SNMP
ethereal [ -vh ] [ -kQS ] [ -b <bold font> ] [ -B <byte view height> ]
[ -c count ] [ -D ] [ -f <capture filter> ] [ -i interface ]
[ -m <medium font> ] [ -n ] [ -P <packet list height> ] [ -r infile ]
[ -R <read filter> ] [ -s snaplen ] [ -t <time stamp format> ]
[ -T <tree view height> ] [ -w savefile ]
```

We will examine each of these possible command line options in turn.

The first thing to notice is that issuing the command **ethereal** by itself will bring up Ethereal. However, you can include as many of the command line parameters as you like. Their meanings are as follows:

Ethereal flags

-h

The **-h** option requests Ethereal to print its version and usage instructions and exit.

-v

The **-v** option requests Ethereal to print out its version information and exit.

-i <interface>

The **-i** option allows you to specify, from the command line, which interface packet capture should occur on if capturing packets.

An example would be:**ethereal -i eth0**.

To get a listing of all the interfaces you can capture on, use the command **ifconfig -a** or **netstat -i**.

-k

The **-k** option specifies that Ethereal should start capturing packets immediately. This option requires the use of the **-i** parameter to specify the interface that packet capture will occur from.

-Q

This option forces Ethereal to exit when capturing is complete. It can be used with the **-c** option. It must be used in conjunction with the **-i** and **-w** options.

-S

This option specifies that Ethereal will display packets as it captures them. This is done by capturing in one process and displaying them in a separate process.

-b <bold font>

This option sets the name of the bold font that Ethereal uses for data in the byte view pane when it is highlighted (ie, selected in the protocol pane

-B <byte view height>

This option sets the initial height of the byte view pane. This pane is the bottom pane in the Ethereal display

-c <count>

This option specifies the number of packets to capture when capturing live data. It would be used in conjunction with the **-k** option.

-D

This option changes the way Ethereal deals with the original IPv4 TOS fiels, so that rather than treating it as the Differentiated Services Field, it is treated as a Type of Service field.

-f <capture filter>

This option sets the initial capture filter expression to be used when capturing packets

-m <medium font>

This option sets the name of the font used for most text displayed by Ethereal.

-n

This option specifies that Ethereal not perform address to name translation nor to translate TCP and UDP ports into names.

-P <packet list height>

This option sets the initial height of the packet list pane, ie, the top pane.

-r <infile>

This option provides the name of a capture file for Ethereal to read and display. This capture file can be in one of the formates Ethereal understands, including:

- libpcap
- Net Mon
- Snoop
- NetXray

For a complete list, see the Ethereal man pages (**man ethereal**).

-R <read filter>

This option specifies a capture filter to be applied when reading packets from a capture file. The syntax of this filter is that of the display filters discussed in . Packets not matching the filter are discarded.

-s <snaplen>

This option specifies the snapshot length to use when capturing packets. Ethereal will only capture **<snaplen>** bytes of data for each packet.

-t <time stamp format>

This option sets the format of packet timestamps that are displayed in the packet list window. The format can be one of:

- **r**, which specifies timestamps are displayed relative to the first packet captured.
- **a**, which specifies that actual dates and times be displayed for all packets.
- **d**, which specifies that timestamps are relative to the previous packet.

-T <tree view height>

This option sets the initial height of the tree view pane.

-w <savefile>

This option sets the name of the **savefile** to be used when saving a capture file.

3.3. The Ethereal menus

The Ethereal menu, which sits across the top of the Ethereal window, contains the

following items:

File

This menu contains menu-items to open and reread capture files, save capture files, print capture files, print packets, and to quit from Ethereal.

Edit

This menu contains menu-items to find a frame and goto a frame, as well as to set your preferences and create filters (cut, copy, and paste are not presently implemented).

Capture

This menu contains the one item, capture, which allows you to capture packets from any interface.

Display

This menu contains menu-items to modify options, match selected frames, colorize frames, expand all frames, collapse all frames, and show a packet in a separate window.

Tools

This menu contains menu-items to manage plugins, follow a TCP stream, and obtain a summary of the packets that have been captured.

Help

This menu contains the About Ethereal... menu item.

Each of these are described in more detail in the sections that follow.

3.3.1. The Ethereal file menu

The Ethereal file menu contains the fields shown in Table 3-1.

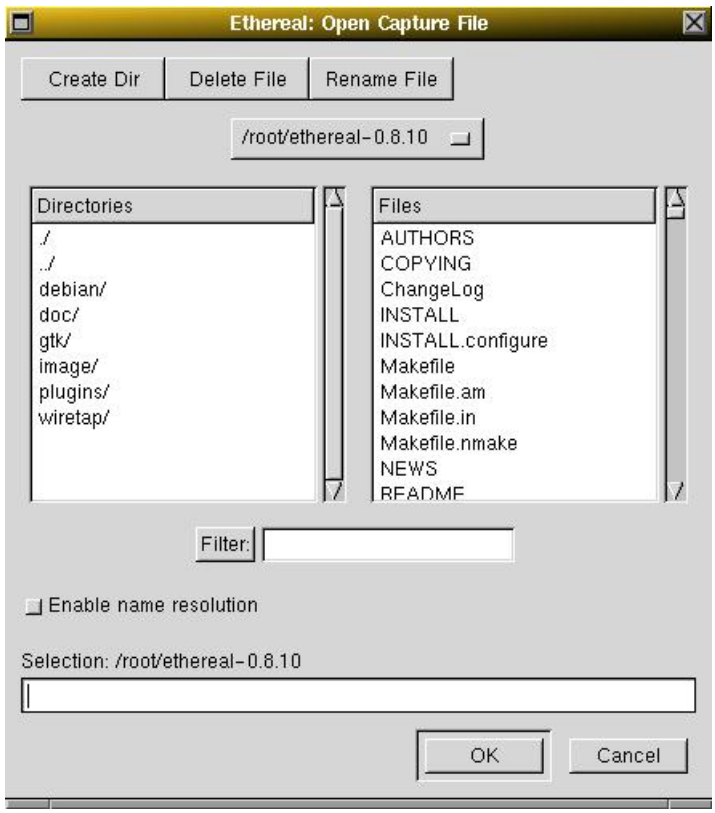
Table 3-1. File menu

Menu Item	Accelerator	Description
Open...	Ctrl-O	This menu item brings up the file open dialog box that allows you to load a capture file for viewing. It is discussed in more detail in Section 3.3.1.1.
Close	Ctrl-W	This menu item closes the current capture. If you have not saved the capture, it is lost.
Save	Ctrl-S	This menu item saves the current capture. If you have not set a default capture file name (perhaps with the **-w capfile option), Ethereal pops up the Save Capture File As dialog box (which is discussed further in Section 3.3.1.2).**
Save As...		This menu item allows you to save the current capture file to whatever file you would like. It pops up the Save Capture File As dialog box (which is discussed further in Section 3.3.1.2).
Reload	Ctrl-R	This menu item allows you to reload the current capture file. This menu item is no longer needed, and may be removed in future releases of Ethereal
Print...		This menu item allows you to print all the packets in the capture file. It pops up the Ethereal Print dialog box (which is discussed further in).
Print Packet	Ctrl-P	This menu item allows you to print the current packet.
Quit	Ctrl-Q	This menu item allows you to quit from Ethereal. In the current release of Ethereal (0.8.10), Ethereal silently exits even if you have not saved the current capture file. This may be changed in a future release of Ethereal.

3.3.1.1. The File Open dialog box

The Ethereal File Open dialog box allows you to search for a capture file containing previously captured packets for display in Ethereal. Figure 3-2 shows an example of the Ethereal Open File Dialog box.

Figure 3-2. The Ethereal Open File Dialog box



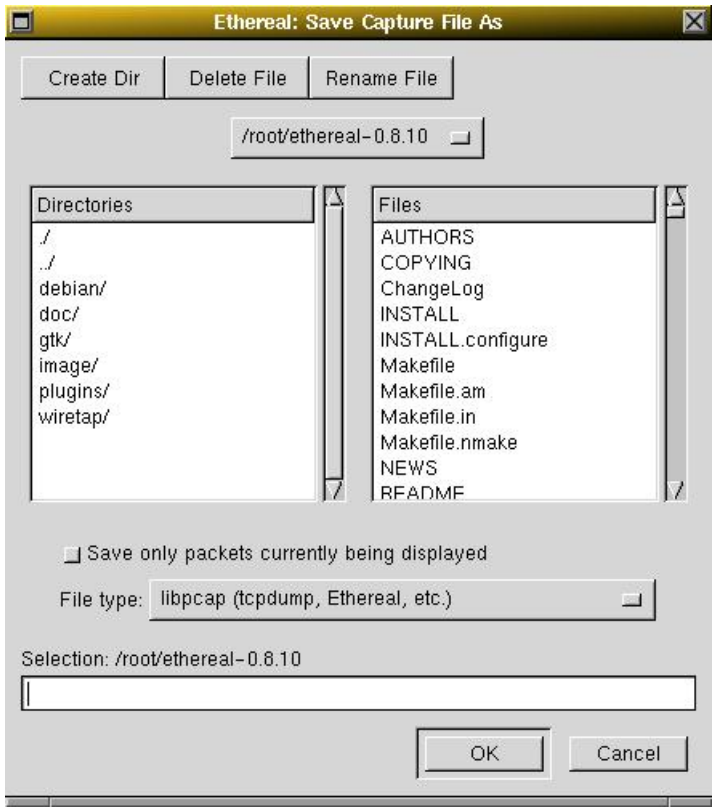
With this dialog box, you can perform the following actions:

1. Create directories with the **Create Dir** button.
2. Delete files with the **Delete File** button.
3. Rename files with the **Rename File** button.
4. Select files and directories with the directories and files list boxes and the file system heirarchy drop down box.
5. Specify a display filter with the Filter button and filter field. Clicking on the Filter button causes Ethereal to pop up the Filters dialog box (while is discussed further in).
6. Specify that name resolution is to be performed for all addresses in packets by clicking on the "Enable name resolution" radio button.
7. Type in the name of the capture file you wish to open, as a standard file name in your file system.
8. Click on OK to accept your selected file and open it. If Ethereal recognizes the capture format, it will display the packets read from the capture file in the packet list pane. If it does not recognize the capture format, it will display an error dialog box. After clicking OK, you can try another file.
9. Click on Cancel to go back to Ethereal and not load a capture file.

3.3.1.2. The Save Capture File As dialog box

The Ethereal Save Capture File As dialog box allows you to save the current capture to a file. Figure 3-3 shows an example of this dialog box.

Figure 3-3. The Ethereal Save Capture File As dialog box



With this dialog box, you can perform the following actions:

1. Create directories with the **Create Dir** button.
2. Delete files with the **Delete File** button.
3. Rename files with the **Rename File** button.
4. Select files and directories with the directories and files list boxes and the file system heirarchy drop down box.

5. Save only the packets currently being displayed (as apposed to all the packets captured) by clicking on the "Save only packets currently being displayed" radio button.
6. Specify the format of the saved capture file by clicking on the File type drop down box. You can choose from among the following types:
   a. libpcap (tcpdump, Ethereal, etc.)
   b. modified libpcap (tcpdump)
   c. RedHat Linux libpcap (tcpdump)
   d. Network Associates Sniffer (DOS based)
   e. Sun Snoop
   f. Microsoft Network Monitor 1.x
   g. Network Associates Sniffer (Windows based) 1.1
7. Type in the name of the file you wish to save the captured packets in, as a standard file name in your file system.
8. Click on OK to accept your selected file and save to it. If Ethereal has a problem saving the captured packets to the file you specified, it will display an error dialog box. After clicking OK, you can try another file.
9. Click on Cancel to go back to Ethereal and not save the captured packets.

3.3.1.3. The Ethereal Edit menu

The Ethereal Edit menu contains the fields shown in Table 3-2.

Table 3-2. Edit menu

Menu Item	Accelerator	Description
Cut	Ctrl-X	This menu item is not currently implemented, so it is greyed out.

Menu Item	Accelerator	Description
Copy	Ctrl-C	This menu item is not currently implemented, so it is greyed out.
Paste	Ctrl-V	This menu item is not currently implemented, so it is greyed out.
Find Frame...	Ctrl-F	This menu item brings up a dialog box that allows you to find a frame by entering an Ethereal display filter. There is further information on finding frames in .
Go to Frame...	Ctrl-G	This menu item brings up a dialog box that allows you to specify a frame to goto by frame number.
Preferences...		This menu item brings up a dialog box that allows you to set preferences for many parameters that control Ethereal. You can also save your preferences so Ethereal will use them the next time you start it.
Filters...		This menu item brings up a dialog box that allows you to create and edit filters. You can name filters, and you can save them for future use.

3.3.1.4. The Ethereal Capture menu

The Ethereal Capture menu contains the fields shown in Table 3-3.

Table 3-3. Capture menu

Menu Item	Accelerator	Description
Start...	Ctrl-K	This menu item brings up the Capture Preferences dialog box (discussed further in Section 3.3.2) and allows you to start capturing packets.

3.3.1.5. The Ethereal Display menu

The Ethereal Display menu contains the fields shown in Table 3-4.

Table 3-4. Display menu

Menu Item	Accelerator	Description
Options...		This menu item brings up a dialog box that controls the way that Ethereal displays some information about packets. Examples include the way timestamps are handled, whether addresses and other numbers are translated, and so forth. This is further discussed in .
Match Selected		This menu item allows you to select all packets that have a matching value in the field selected in the tree view pane (middle pane).
Colorize Display		This menu item brings up a dialog box that allows you color packets in the packet list pane according to filter expressions you choose. It can be very useful for spotting certain types of packets.
Collapse All		Ethereal keeps a list of all the protocol subtrees that are expanded, and uses it to ensure that the correct subtrees are expanded when you display a packet. This menu item collapses the tree view of all packets in the capture list.
Expand All		This menu item expands all subtrees in all packets in the capture.
Display Packet in New Window		This menu item brings up the selected packet in a separate window. The separate window shows only the tree view and byte view panes.

3.3.1.6. The Ethereal Tools menu

The Ethereal Tools menu contains the fields shown in Table 3-5.

Table 3-5. Tools menu

Menu Item	Accelerator	Description
Plugins...		This menu item brings up a dialog box that allows you to manage Ethereal plugins. There are very few plugins todate.
Follow TCP Stream		This menu item brings up a separate window and displays all the TCP segments captured that are on the same TCP connection as a selected packet. The data in the TCP stream is sorted into order, with duplicate segments removed, and it is then displayed in ascii. You can change the format is you desire.
Summary		This menu item brings up a statistics window that shows information about the packets captured.

3.3.1.7. The Ethereal Help menu

The Ethereal Help menu contains the fields shown in Table 3-6.

Table 3-6. Help menu

Menu Item	Accelerator	Description
About Ethereal...		This menu item brings up an information window that provides some simple information on Ethereal, as well as providing a list of the contributors to Ethereal.

3.3.2. Capturing packets with Ethereal

There are two methods you can use to capture packets with Ethereal:

1. From the command line using the following:

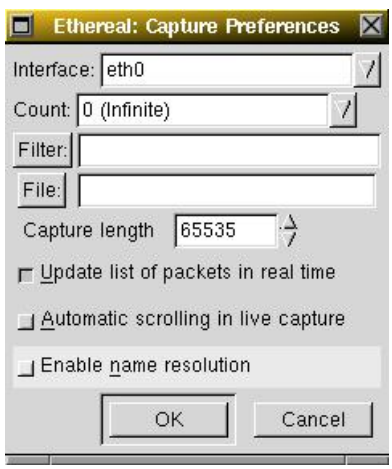
   ```
   ethereal -i eth0 -k
   ```

2. By starting Ethereal and then selecting Start... from the Capture menu. This brings up the Capture Preferences dialog box and will be dealt with in more detail in Section 3.3.2.1.

3.3.2.1. The Capture Preferences dialog box

When you select Start... from the Capture menu, Ethereal pops up the Capture Preferences dialog box as shown in Figure 3-4.

Figure 3-4. The Capture Preferences dialog box



You can set the following fields in this dialog box:

Interface

This field specifies the interface you want to capture on. You can only capture on one interface, and you can only capture on interfaces that the Ethereal has found on the system. It is a drop-down list, so simply click on the button on the right hand side and select the interface you want. It defaults to the first, non-loopback, interface.

This field performs the same function as the **-i <interface>** command line option.

Count

This field specifies the number of packets that you want to capture. It defaults to 0, which means do not stop capturing. Enter the value that you want in here, or leave it blank.

Filter

This field allows you to specify a capture filter. Capture filters are discussed in more details in Section 3.3.3. It defaults to empty, or no filter.

File

This field allows you to specify the file name that will be used for the capture when you later choose Save... or Save As... from the Ethereal File menu. There is no default for this value.

Capture length

This field allows you to specify the maximum amount of data that will be captured for each packet, and is sometimes referred to as the **snaplen**. The default is 65535, which will be sufficient for most protocols. It should be at least the MTU for the interface you are capturing on.

Update list of packets in real time

> This radio button allows you to specify that Ethereal should update the packet list pane in real time. If you do not specify this, Ethereal does not display any packets until you cancel the capture. When you click on this radio button, Ethereal captures in a separate process and feeds the captures to the display process. [Is this true for Windows?]

Automatic scrolling in live capture

> This radio button allows you to specify that Ethereal should scroll the packet list pane as new packets come in, so you are always looking at the last packet. If you do not specify this, Ethereal simply adds new packets onto the end of the list, but does not scroll the packet list pane.

Enable name resolution

> This radio button allows you to control whether or not Ethereal translates IP addresses into names and port numbers into protocols. By clicking on this radio button, the packet list pane will have more useful information, but you will also cause name lookup requests to occur, which might disturb the capture. Also, if you cannot reach the name server, you may find that Ethereal takes a long time in updating the packet list pane as it waits for name transation to time out.

Once you have set the values you desire and have selected the radio buttons you need, simply click on OK to commence the capture, or Cancel to cancel the capture.

If you start a capture, Ethereal pops up a dialog box that shows you the progress of the capture and allows you to stop capturing when you have enough packets captured.

3.3.3. Filtering while capturing

Ethereal uses the libpcap filter language for capture filters. This is explained in the tcpdump man page. If you can understand it, you are a better man that I am, Gunga Din!

You enter the capture filter into the Filter field of the Ethereal Capture Preferences dialog box, as shown in Figure 3-4. The following is an outline of the syntax of the **tcpdump** capture filter language.

A capture filter takes the form of a series of primitive expressions connected by conjuctions (**and/or**) and optionally preceeded by **not**:

```
[not] primitive [and|or [not] primitive ...]
```

An example is shown in Example 3-2.

Example 3-2. A capture filter for telnet than captures traffic to and from a particular host

```
tcp port 23 and host 10.0.0.5
```

This example captures telnet traffic to and from the host 10.0.0.5, and shows how to use two primitives and the **and** conjunction. Another example is shown in Example 3-3, and shows how to capture all telnet traffic except that from 10.0.0.5.

Example 3-3. Capturing all telnet traffic not from 10.0.0.5

```
tcp port 23 and not host 10.0.0.5
```

A primitive is simply one of the following:

[src|dst] host <host>

This primitive allows you to filter on a host IP address or name. You can optionally preceed the primitive with the keyword **src|dst** to specify that you are only interested in source or destination addresses. If these are not present, packets where the specified address appears as either the source or the destination address will be selected.

ether [src|dst] host <ehost>

This primitive allows you to filter on Ethernet host addresses. You can optionally includethe keyword **src|dst** between the keywords **ether** and **host** to specify that you are only interested in source or destination addresses. If these are not present, packets where the specified address appears in either the source or destination address will be selected.

gateway host <host>

This primitive allows you to filter on packets that used **host** as a gateway. That is, where the etherent source or destination was **host** but neither the source nor destination IP address was **host**.

[src|dst] net <net> [{mask <mask>}|{len <len>}]

This primitive allows you to filter on network numbers. You can optionally preceed this primitive with the keyword **src|dst** to specify that you are only interested in a source or destination network. If neither of these are present, packets will be selected that have the specified network in either the source or destination address. In addition, you can specify either the netmask or the CIDR prefix for the network if they are different from your own.

[tcp|udp] [src|dst] port <port>

This primitive allows you to filter on TCP and UDP port numbers. You can optionally preceed this primitive with the keywords **src|dst** and **tcp|udp** which allow you to specify that you are only interested in source or destination ports and TCP or UDP packets respectively. The keywords **tcp|udp** must appear before **src|dst**.

If these are not specified, packets will be selected for both the TCP and UDP protocols and when the specified address appears in either the source or destination port field.

less|greater <length>

This primitive allows you to filter on packets whose length was less than or equal

to the specified length, or greater than or equal to the specified length, respectively.

ip|ether proto <protocol>

This primitive allows you to filter on the specified protocol at either the Ethernet layer or the IP layer.

ether|ip broadcast|multicast

This primitive allows you to filter on either Ethernet or IP broadcasts or multicasts.

<expr> relop <expr>

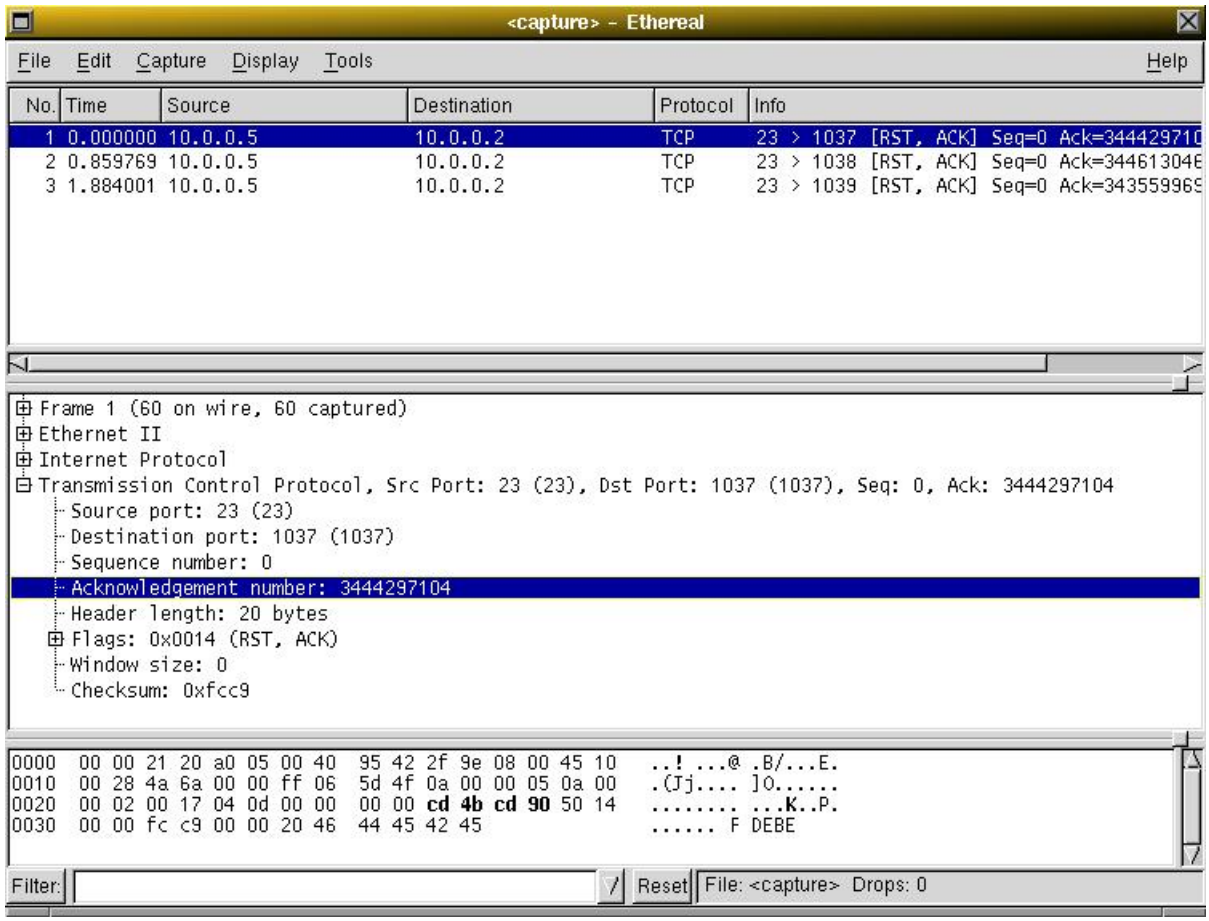
This primitive allows you to create complex filter expressions that select bytes or ranges of bytes in packets. Please see the tcpdump man pages for more details.

3.3.4. Viewing packets you have captured

Once you have captured some packets, or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on that packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.

You can then expand any part of the tree view by clicking on the **plus**sign to the left of that part of the payload, and you can select individual fields by clicking on them in the tree view pane. An example with a TCP segment selected is shown in Figure 3-5. It also has the Acknowledgment number in the TCP header selected, which shows up in the byte view as the selected bytes.

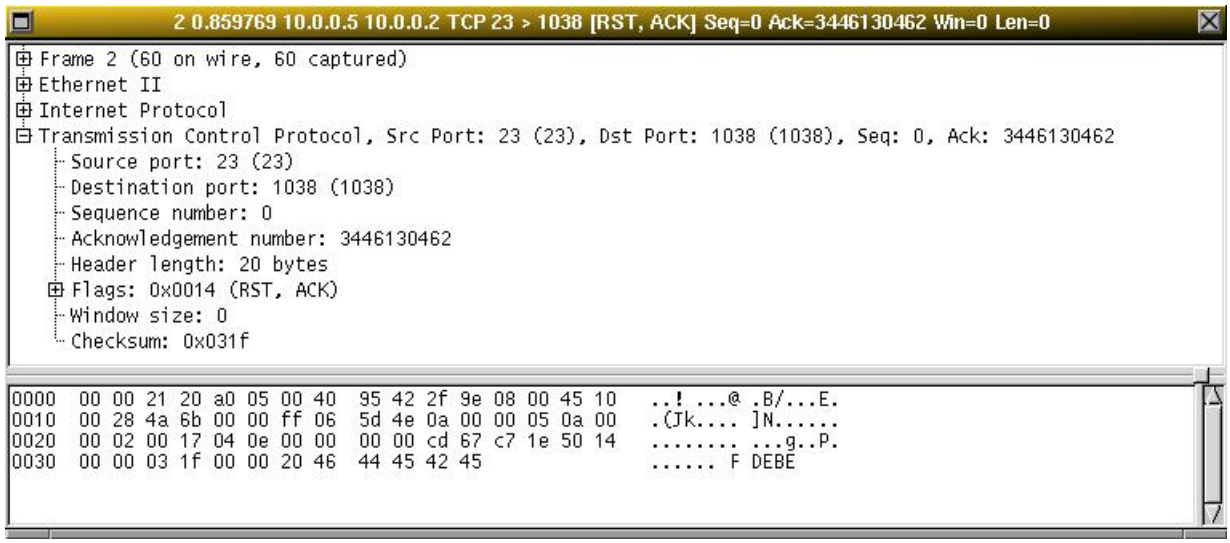
Figure 3-5. Ethereal with a TCP segment selected for viewing



You can also select and view packets when Ethereal is capturing if you selected "Update list of packets in real time" in the Ethereal Capture Preferences dialog box.

In addition, you can view individual packets in a separate window as shown in Figure 3-6. This allows you to easily compare two or more packets.

Figure 3-6. Viewing a packet in a separate window



Finally, you can bring up a pop-up menu over either the packet list pane or the tree view pane by clicking your right mouse button. The menu that is popped up contains the following items:

Match Selected

This menu item is the same as the Display menu item of the same name. It allows you to filter all packets that match the selected field.

Follow TCP Stream

This menu item is the same as the Display menu item of the same name. It allows you to view all the data on a TCP stream between a pair of nodes.

Filters...

This menu item is the same as the Edit menu item of the same name. It allows you to specify and manage filters.

Colorize Display...

This menu item is the same as the Display menu item of the same name. It allows you to colorize packets in the packet list pane.

Print...

This menu item is the same as the File menu item of the same name. It allows you to print packets.

Print Packet

This menu item is the same as the File menu item of the same name. It allows you to print the currently selected packet.

Show Packet in New Window

This menu item is the same as the Display menu item of the same name. It allows you to display the selected packed in another window.

3.3.5. Saving captured packets

Another para

3.3.6. Reading capture files

Another para

3.3.7. Filtering packets while viewing

Another para

3.3.8. More advanced aspects

Another para

Chapter 4. Troubleshooting with Ethereal

4.1. An approach to troubleshooting with Ethereal

Ethereal is perhaps one of blah blah...

4.2. Examples of troubleshooting

Another para

Chapter 5. Miscellaneous Topics

5.1. Capturing with tcpdump for viewing with Ethereal

Ethereal is perhaps one of blah blah...

5.2. Using editpcap

A para

5.3. Other tools

Another para

Appendix A. Ethereal Error Messages

A.1. Capture file format not understood

If Ethereal cannot decode the capture file format of the file you have asked it to load, you will receive a warning box similar to that shown in Figure A-1.

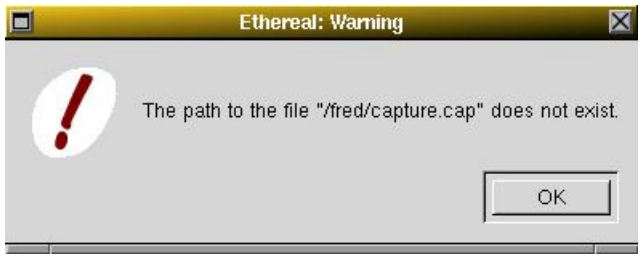
Figure A-1. Ethereal Read Format warning

A.2. Save file error

If Ethereal cannot open the file you requested it to save captured packets in, you will

receive a warning box similar to that shown in Figure A-2.

Figure A-2. Save Error warning



Appendix B. The GNU Free Document Public Licence

B.1. Copyright

Version 1.1, March 2000

B.2. Preamble

The purpose of this License is to make a manual, textbook, or other written document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

B.3. Applicability and Definitions

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

B.4. Verbatim Copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

B.5. Copying in Quantity

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers

that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

B.6. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a

copy of it. In addition, you must do these things in the Modified Version:

- Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).
- State on the Title page the name of the publisher of the Modified Version, as the publisher.
- Preserve all the copyright notices of the Document.
- Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document’s license notice.
- Include an unaltered copy of this License.
- Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the

Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

- In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.
- Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

B.7. Combining Documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

B.8. Collections of Documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

B.9. Aggregation with Independent Works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document’s Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

B.10. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

B.11. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

B.12. Future Revisions of this License

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.