Getting Started with Ethereal

If you have any questions concerning network and system management, visit the OPENXTRA website, www.openxtra.com. Join in with our discussion groups, exchange ideas and views, add your comments about all aspects of network and system management.

Table of Contents

About this Guide

This short guide is intended to get you started so that you have something working in a short space of time. It does not attempt to try and tell you everything about the software. Once you have learned a few basics you will be able to pick up the rest as you go along.

Typographical Conventions

Product names inside the text are in *italics*.

Tips and important points to note are shown in boxes.

> *This is how a tip or point worth noting will appear.*

Step by step instructions are numbered and shown in bold type.

Introduction to Ethereal

Ethereal is a very powerful well featured packet analyzer. It captures packets and decodes them into their component parts for analysis. The range of decodes is very large, if you've heard of a protocol there's a good chance that *Ethereal* has a decoder for it, and if you haven't there's still likely to be a decoder for it.

Ethereal is available for use on UNIX systems and for Microsoft Windows.

> *This guide is concerned with using Ethereal on machines running Microsoft Windows.*

> *Ethereal uses the same capture and filtering mechanism as tcpdump and can read files captured by tcpdump.*

This guide is not intended to cover all the features, functions, and options available in *Ethereal*. Instead it shows you how to perform some of the basic tasks, such as packet capturing, decoding, and filtering a trace file.

It also introduces you to a few of the commonly used options to help you start to become familiar with the software.

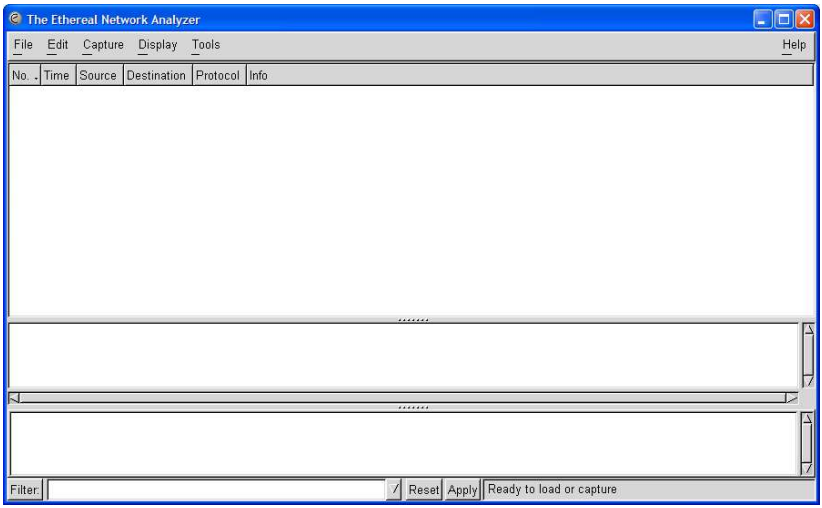
Installing Ethereal

Ethereal, and its associated utilities are installed as part of the OPENXTRA BASICS package. For installation details refer to the 'Getting Started with OPENXTRA BASICS' guide.

Using Ethereal

Step 1 In Windows click Start, All Programs, OPENXTRA BASICS.

Step 2 Select Ethereal.

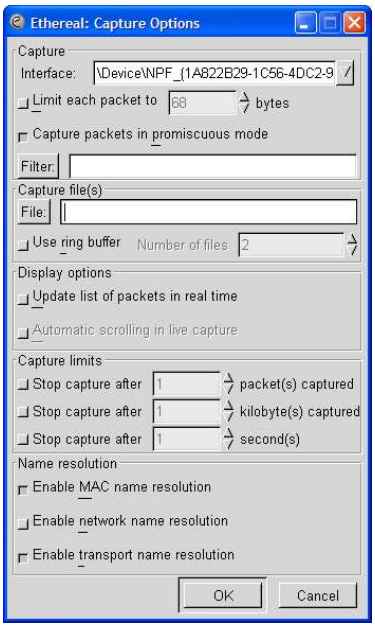


Ethereal displays a large windows consisting of three panes. To begin with the panes are blank.

Capturing packets

Click on Capture, Start.

The Capture Options box appears.



If the square button is raised the option is Off, if the square button is pressed the option is On. Options are grouped into different functions.

Capture
Limit each packet to allows you to restrict allows you to specify, in bytes, how much of each packet to collect. This is useful if you are interested in the header information only, and if you want to keep the file sizes small.

Capture packets in promiscuous mode. If you want to capture everything

that your machine can see click this option. If you only want to see packets in and out of your machine leave this option unselected.

Filter allows you to enter an existing capture filter.

Capture file(s)
File allows you to save the captured packets in a named file.

Use ring buffer allows you to specify a number of files to use for the capture. In a Ring Buffer when one file is full a new one starts. When the specified number of files are all full capture begins to overwrite the files in sequence. This function is useful if you want to capture continuously but do not want to fill your hard disk.

> *Note that when Use Ring Buffer is pressed the Capture limits option, Stop capture after xx kilobyte(s) changes to Rotate capture every xx kilobytes.*

Display options

Update list of packets in real time. Use this option if you want to see the list of packets as they are captured.

Automatic scrolling in live capture. Select this if you want the packet list to scroll.

Capture limits
These options limit the number of packets you can capture. There are three options, limit by number of packets, by an amount of disk space, or by time. All can be enabled at once, the first option to be matched will cause the capture to stop.

If Use ring buffer is pressed Rotate capture every allows you to specify the file size in kilobytes.

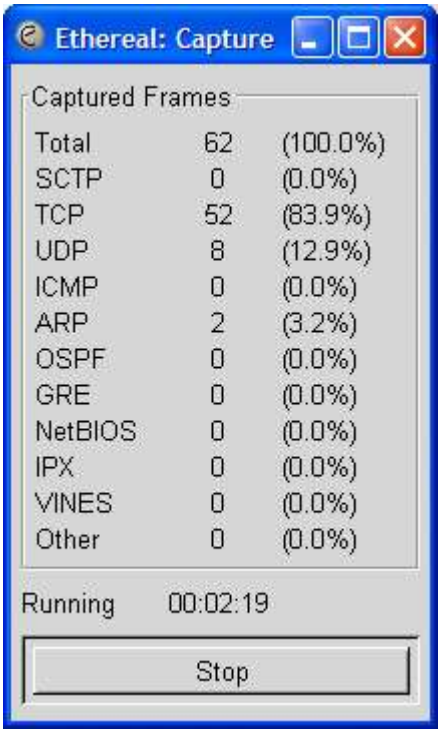
To capture continuously switch all the options Off.

Name resolution
Enable name resolution. If you want the addresses to be resolved into names select this option.

> *Enabling name resolution can slow Ethereal down increasing the risk of dropping packets.*

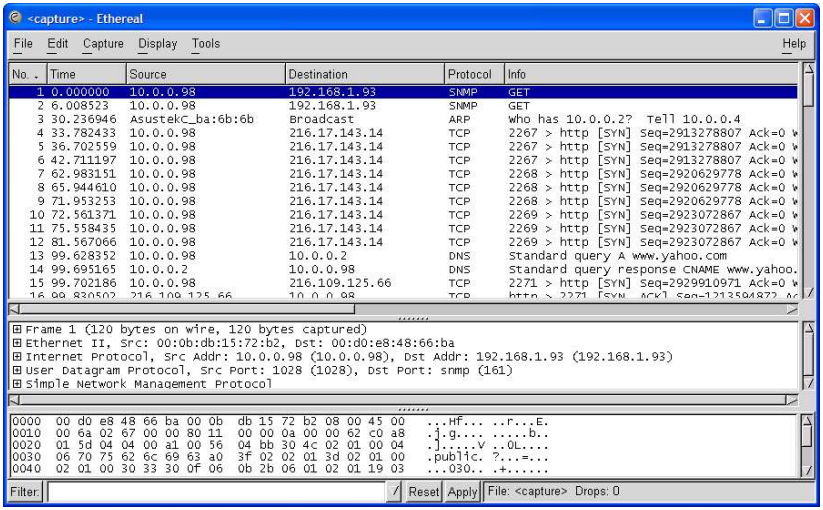
Click OK when you have set the options you require.

As packet capture proceeds a breakdown of the running totals are displayed in the capture window.



If you have set a value in the Capture limits options capturing will continue until that value is reached. If not you can press the Stop button at any time.

When you stop capturing the opening screen now shows the captured packets.



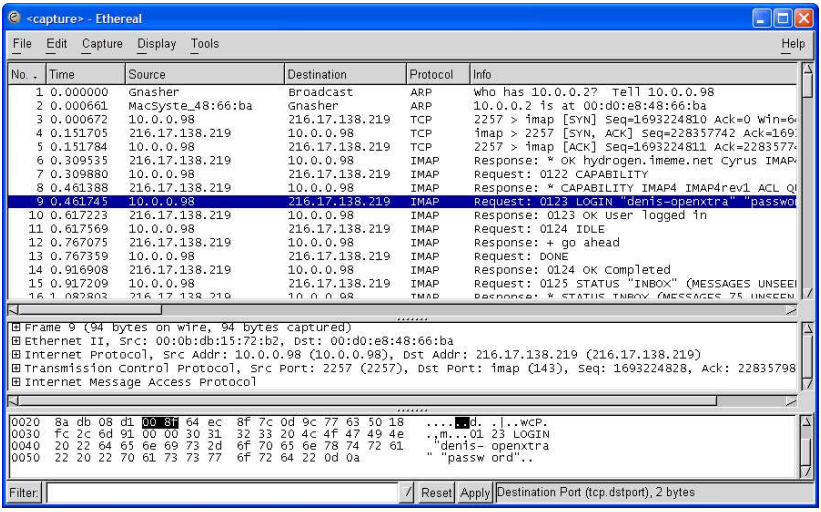
Scroll through the list to find the packet you are interested in and click on it to see the details.

> *You can also resize the windows if required by pointing your cursor at the bars between panes. Click and hold the left mouse button, and drag the bar to the required position.*

Opening an existing file

Click on File, Open. Select a file and press Enter.

> *Ethereal can read packet capture files from tcpdump using the -w option, and uses the same filtering system and syntax.*



When a file is open the top pane shows a list of the packets, with times, addresses, protocols and summary information, the central pane shows a detailed breakdown of the highlighted packet protocols, and the bottom pane shows the raw hex and ASCII data in the packet.

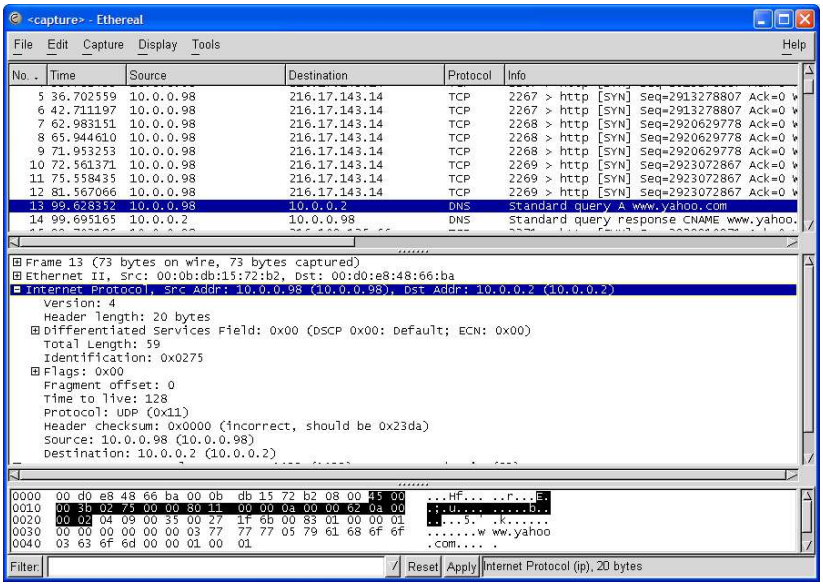
Displaying multiple packets

Click Display, Show Packet in New Window, to view a packet in a separate window. Using this allows you to view details of several packets at once.

Viewing protocol details

The central pane shows the protocols in the highlighted packet. Click the plus or minus sign to expand or collapse the protocols.

> *Display has an option to expand and collapse all protocols with a single key press.*



Display options

The display options in *Ethereal* are very powerful.

Options... allows you to specify the format of the Time field and the type of Name resolution required.

The box at the bottom of the opening screen allows you to specify display

filters. Display filters can be very complex, but the good news is that you do not have to know a great deal about the syntax to make useful filters. By far the easiest way to build display filters is from inside the protocol details view.

Display Match, Selected

This very useful for viewing filtered selections from the full packet trace. There are a number of powerful options.

Step 1 Click on a field inside the central protocol pane.

Not all selections make sensible filters but with a bit of trial and error you will quickly learn what makes works and what does not.

Step 2 Click Display, Match, Selection.

A filtered list of packets appears.

> *Other options allow you to reverse the filter, and perform other boolean operations.*

The Filter details appear at the bottom of the screen.

To clear the Filter press the Reset button.

You can save and name your Filters using the options under Filter.

> *An alternative way to filter a file is to simply type the name of the protocol in the Filter box and click on Apply.*

Making Display filters by hand

Step 1 Click Edit, Display Filters...

Step 2 Type a name for the filter in the Filter name box.

Step 3 Add a Filter string.

> *You can use the Add Expression button to make this easier. Click it, go to the protocol you are interested in, click that*

and select a field. Type a value.

Step 4 Click New.

Editing Display Filters

Step 1 Click Edit, Display Filters...

Step 2 Click the filter you want to edit.

Step 3 Edit the Filter string.

You can use the Add Expression button to make this easier. Click it, go to the protocol you are interested in, click that and select a field. Type a value.

Step 4 Click Change.

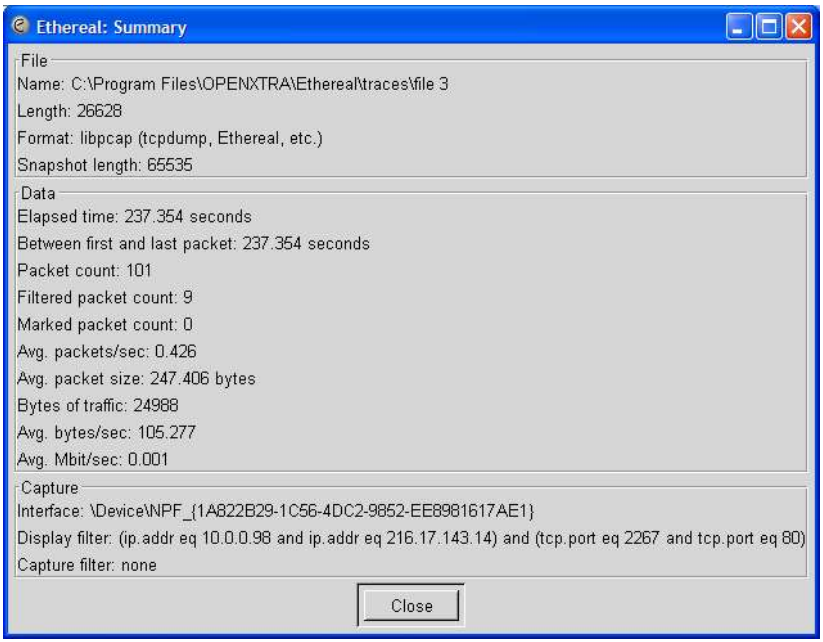
Step 5 Click Close.

Tools options

The Tools options allow you to perform advanced analysis on the packets in the file. This section describes some of the simpler options.

Summary

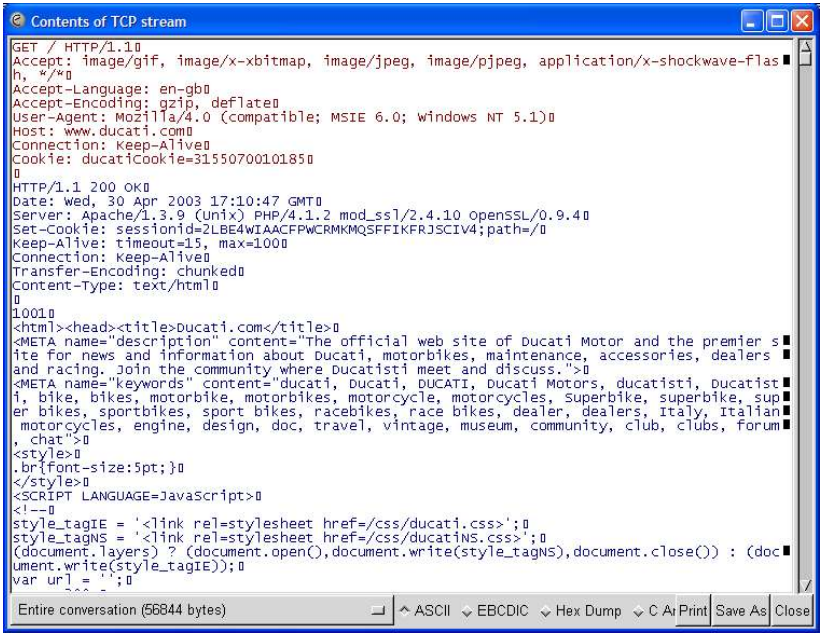
Click Tools, Summary, for a breakdown of the data that you have collected.



Follow TCP Stream

Click Tools, Follow TCP Stream. This option tracks the information in a

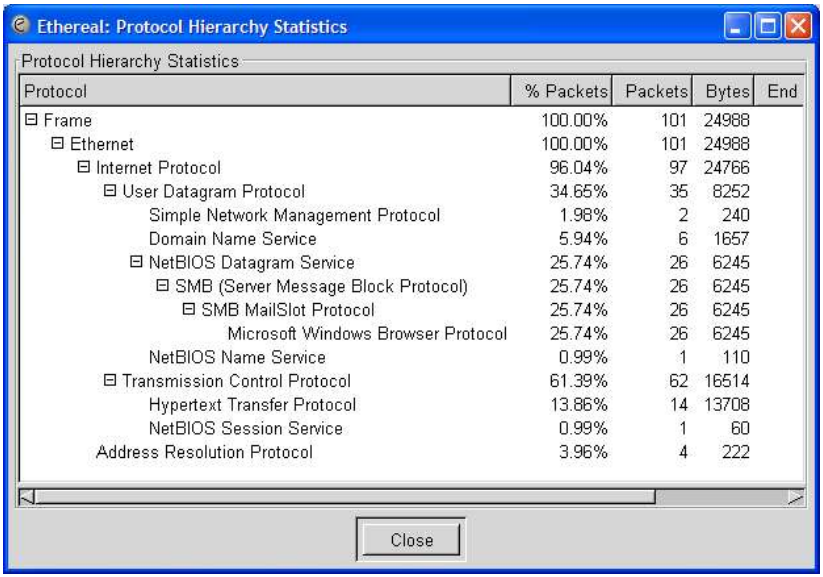
TCP conversation and makes it easy to follow the traffic between two endpoints.



This information may be displayed in ASCII, EBCDIC, Hex or C arrays and printed or saved.

Display Protocol Hierarchy Statistics

This option gives a breakdown of protocols and sub protocols in the file.



Protocol	% Packets	Packets	Bytes	End
⊟ Frame	100.00%	101	24988	
⊟ Ethernet	100.00%	101	24988	
⊟ Internet Protocol	96.04%	97	24766	
⊟ User Datagram Protocol	34.65%	35	8252	
Simple Network Management Protocol	1.98%	2	240	
Domain Name Service	5.94%	6	1657	
⊟ NetBIOS Datagram Service	25.74%	26	6245	
⊟ SMB (Server Message Block Protocol)	25.74%	26	6245	
⊟ SMB MailSlot Protocol	25.74%	26	6245	
Microsoft Windows Browser Protocol	25.74%	26	6245	
NetBIOS Name Service	0.99%	1	110	
⊟ Transmission Control Protocol	61.39%	62	16514	
Hypertext Transfer Protocol	13.86%	14	13708	
NetBIOS Session Service	0.99%	1	60	
Address Resolution Protocol	3.96%	4	222	

What next?

This short introduction has given you a start with *Ethereal*. There are many more advanced features to try.

If you have any questions concerning *Ethereal*, or any other tools, visit the OPENXTRA website, www.openxtra.com. Join in with our discussion groups, exchange ideas and views, add your comments about all aspects of network and system management.

For more information go to the Ethereal website at: www.ethereal.com.