

Ethereal Developer's Guide

Richard Sharpe
NS Computer Software and Services P/L

Ethereal Developer's Guide:

by Richard Sharpe

First edition Edition

Published 2000

Copyright © 2000 by NS Computer Software and Services P/L

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST. A copy of the license is included in the section entitled "GNU Free Documentation License"

Table of Contents

1. Introduction	7
What is <code>Ethereal</code> ?	7
A rose by any other name	7
A brief history of <code>Ethereal</code>	7
Platforms <code>Ethereal</code> runs on	7
Where to get <code>Ethereal</code>	7
Where to get the latest copy of this document	7
2. What is packet sniffing	9
Introduction	9
tcpdump, libpcap and other tools	9
The structure of packets	9
How a packet's payload is handled	9
An introduction to wiretap	9
3. How <code>Ethereal</code> works	11
Introduction	11
Capturing packets	11
Passes across the data	11
Calling the dissection routines	11
Parameters passed	11
4. Writing a new dissector by example	13
Introduction	13
Producing the code	13
The files you have to create and modify	13
Running <code>autoconf.sh</code>	13
Contributing your new dissector	13
5. Functions available to dissector writers	15
Groups 1	15

Chapter 1. Introduction

What is `Ethereal`?

`Ethereal` is perhaps one of blah blah...

A rose by any other name

One more

A brief history of `Ethereal`

One para

Platforms `Ethereal` runs on

One para

Where to get `Ethereal`

Another para

Where to get the latest copy of this document

Another para

Chapter 2. What is packet sniffing

Introduction

Ethereal is perhaps one of blah blah...

tcpdump, libpcap and other tools

A para here

The structure of packets

Another para

How a packet's payload is handled

Another para

An introduction to wiretap

Another para

Chapter 3. How Ethereal works

Introduction

Ethereal is perhaps one of blah blah...

Capturing packets

Another para

Passes across the data

Another para

Calling the dissection routines

Another para

Parameters passed

Another para

Chapter 4. Writing a new dissector by example

Introduction

Ethereal is perhaps one of blah blah...

Producing the code

Another para

The files you have to create and modify

A para

Running autoconf.sh

A para

Contributing your new dissector

A para

Chapter 5. Functions available to dissector writers

Groups 1

`Ethereal` is perhaps one of blah blah...

