

# Contents

<b>Foreword</b>	<b>xix</b>
<b>Chapter 1 Introducing Network Analysis</b>	<b>1</b>
Introduction	2
What is Network Analysis and Sniffing?	2
Who Uses Network Analysis?	5
How are Intruders Using Sniffers?	6
What does Sniffed Data Look Like?	8
Common Network Analyzers	9
How Does It Work?	14
Explaining Ethernet	14
Understanding the OSI model	16
CSMA/CD	20
Hardware: Taps, Hubs, and Switches, Oh My!	21
Port Mirroring	24
Defeating Switches	25
Detecting Sniffers	27
Protecting Against Sniffers	31
Network Analysis and Policy	33
Summary	34
Solutions Fast Track	35
Frequently Asked Questions	37
<b>Chapter 2 Introducing Ethereal: Network Protocol Analyzer</b>	<b>39</b>
Introduction	40
What is Ethereal?	40
History of Ethereal	41
Compatibility	43
Supported Protocols	44

Ethereal's User Interface	46
Filters	48
Great Resources!	52
Supporting Programs	54
Tethereal	54
Editcap	57
Mergecap	57
Text2pcap	58
Using Ethereal in Your Network Architecture	59
Using Ethereal for Network Troubleshooting	64
Summary	69
Solutions Fast Track	69
Frequently Asked Questions	71
<b>Chapter 3 Getting and Installing Ethereal</b>	<b>73</b>
Introduction	74
Getting Ethereal	75
Platforms and System Requirements	76
Packet Capture Drivers	78
Installing libpcap	80
Installing libpcap Using the RPMs	80
Installing libpcap from the Sun packages	83
Installing libpcap from the source files	85
Installing WinPcap	87
Installing Ethereal on Windows	91
Installing Ethereal on UNIX	99
Installing Ethereal from the RPMs	99
Installing the Solaris Ethereal Package	104
Building Ethereal from Source	108
Installing Ethereal from Source on Red Hat Linux	108
Installing the Dependencies	109
Building Ethereal	115
Enabling and Disabling features via <i>configure</i>	118
Summary	121
Solutions Fast Track	121
Frequently Asked Questions	123

<b>Chapter 4 Using Ethereal</b>	<b>125</b>
Introduction	126
Getting Started with Ethereal	126
Exploring the Main Window	127
Summary Window	128
Protocol Tree Window	130
Data View Window	132
Other Window Components	134
Filter Bar	134
Information Field	136
Exploring the Menus	136
File	136
Open	138
Save As	140
Print	141
Edit	147
Find Packet	149
Go To Packet	151
Time Reference Submenu	151
Preferences	153
View	154
Display Options	155
Apply Color Filters	156
Show Packet in New Window	160
Capture	161
Capture Options	162
Edit Capture Filter List	169
Analyze	171
Edit Display Filter List	172
Match and Prepare Submenus	175
Enabled Protocols	176
Decode As	177
Decode As: Show	179
Contents of TCP Stream	179
TCP Stream Analysis Submenu	181
Summary	192

Protocol Hierarchy Statistics	192
Statistics Submenu	194
Help	194
Contents	195
Supported Protocols	196
About Plugins	196
About Ethereal	197
Pop-up Menus	197
Summary Window Pop-up Menu	197
Protocol Tree Window Pop-up Menu	198
Data View Window Pop-up Menu	200
Using Command Line Options	200
Capture and File Options	201
Filter Options	202
Other Options	202
Summary	203
Solutions Fast Track	203
Frequently Asked Questions	205
<b>Chapter 5 Filters</b>	<b>207</b>
Introduction	208
Writing Capture Filters	209
Tcpdump Syntax Explained	209
Host Names and Addresses	210
Hardware Addresses (MAC Addresses)	211
Ports	212
Logical Operations	212
Protocols	213
Protocol Fields	215
Bitwise Operators	221
Packet Size	223
Examples	224
Using Capture Filters	225
Writing Display Filters	227
Writing Expressions	229
Integers	231
Booleans	234

Floating Point Numbers	234
Strings	234
Byte Sequences	236
Addresses	237
Time Fields	239
Other Field Types	240
Ranges	241
Logical Operations	244
Multiple Occurrences of Fields	244
Hidden Fields	247
Filter List Dialog Boxes	249
Filter Expression Dialog Box	254
Summary	257
Solutions Fast Track	257
Frequently Asked Questions	259
<b>Chapter 6 Other Programs Packaged with Ethereal</b>	<b>261</b>
Introduction	262
Tethereal	262
Tethereal Statistics	271
Editcap	281
Mergecap	287
Text2pcap	293
Summary	299
Solutions Fast Track	299
Frequently Asked Questions	301
<b>Chapter 7 Integrating Ethereal with Other Sniffers</b>	<b>303</b>
Introduction	304
Reading Capture Files with Ethereal	304
Saving Capture Files with Ethereal	306
Ethereal Integration	308
Tethereal	308
Capturing and Saving Data With Tethereal	310
Reading Ethereal Files With Tethereal	312
TCPDump	313
Capturing and Saving Data With TCPDump	314

## xvi Contents

Reading Ethereal Files With TCPDump	316
WinDump	317
Capturing and Saving Data With WinDump	318
Reading Ethereal Files With WinDump	319
Snort	320
Capturing and Saving Data With Snort	322
Reading Ethereal Files With Snort	325
Snoop	326
Capturing and Saving Data With Snoop	329
Reading Ethereal Files With Snoop	330
Microsoft Network Monitor	333
Capturing and Saving Data With Network Monitor	334
Reading Ethereal Files With Network Monitor	336
WildPackets EtherPeek	336
Capturing and Saving Data With EtherPeek	336
Reading Ethereal Files With EtherPeek	338
Network Associates' Sniffer Technologies Netasyst	339
Capturing and Saving Data With Netasyst	340
Reading Ethereal Files With Netasyst	341
HP-UX's nettl	342
Capturing and Saving Data with nettl	345
Reading Ethereal Files with nettl	347
Summary	350
Solutions Fast Track	350
Frequently Asked Questions	352
<b>Chapter 8 Real World Packet Captures</b>	<b>353</b>
Introduction	354
Scanning	354
TCP Connect Scan	355
SYN Scan	356
Xmas Scan	357
Null Scan	358
Remote Access Trojans	359
SubSeven Legend	360
NetBus	361
RST.b	363

Dissecting Worms	365
SQL Slammer Worm	365
Code Red Worm	367
Ramen Worm	371
Summary	376
Solutions Fast Track	376
Frequently Asked Questions	378
<b>Chapter 9 Developing Ethereal</b>	<b>379</b>
Introduction	380
Prerequisites for Developing Ethereal	381
Skills	382
Tools/Libraries	383
Ethereal Design	387
aclocal-fallback and aclocal-missing	388
debian	388
doc	388
epan	389
gtk	389
help	390
image	390
packaging	390
plugins	391
tools	392
wiretap	392
Developing a Dissector	392
Step 1 Copy the Template	393
Step 2 Define the <i>Includes</i>	395
Step 3 Create the Function to Register	397
Step 4 Instruct Ethereal	400
Step 5 Create the Dissector	401
Step 6 Pass Payloads	408
Running a Dissector	409
The Dissection Process	410
Advanced Topics	412
Dissector Considerations	413
Creating Sub-trees	413

**xviii** Contents

Bitfields	415
Unicode Strings	417
Conversations	418
Packet Retransmissions	419
Passing Data Between Dissectors	420
Saving Preference Settings	421
Packet Fragmentation	422
Value Strings	422
The Ethereal GUI	424
The Item Factory	424
Using GTK	425
TAPS	429
Plug-ins	429
Summary	430
Solutions Fast Track	431
Frequently Asked Questions	434
<b>Appendix Supported Protocols</b>	<b>437</b>
<b>About the CD</b>	<b>449</b>
<b>Index</b>	<b>451</b>