

# CONTENTS IN DETAIL

<b>ACKNOWLEDGMENTS</b>	<b>xv</b>
------------------------	-----------

<b>INTRODUCTION</b>	<b>xvii</b>
---------------------	-------------

Why This Book? .....	xvii
Concepts and Approach .....	xviii
How to Use This Book .....	xix
About the Sample Capture Files .....	xx
The Rural Technology Fund .....	xx
Contacting Me .....	xx

<b>1</b>	
<b>PACKET ANALYSIS AND NETWORK BASICS</b>	<b>1</b>

Packet Analysis and Packet Sniffers .....	2
Evaluating a Packet Sniffer .....	2
How Packet Sniffers Work .....	3
How Computers Communicate .....	4
Protocols .....	4
The Seven-Layer OSI Model .....	5
Data Encapsulation .....	8
Network Hardware .....	10
Traffic Classifications .....	14
Broadcast Traffic .....	14
Multicast Traffic .....	15
Unicast Traffic .....	15
Final Thoughts .....	16

<b>2</b>	
<b>TAPPING INTO THE WIRE</b>	<b>17</b>

Living Promiscuously .....	18
Sniffing Around Hubs .....	19
Sniffing in a Switched Environment .....	20
Port Mirroring .....	21
Hubbing Out .....	22
Using a Tap .....	24
ARP Cache Poisoning .....	26
Sniffing in a Routed Environment .....	30
Sniffer Placement in Practice .....	31

<b>3</b>	
<b>INTRODUCTION TO WIRESHARK</b>	<b>35</b>

A Brief History of Wireshark .....	35
The Benefits of Wireshark .....	36

Installing Wireshark.....	37
Installing on Microsoft Windows Systems.....	37
Installing on Linux Systems.....	39
Installing on Mac OS X Systems.....	40
Wireshark Fundamentals.....	41
Your First Packet Capture.....	41
Wireshark's Main Window.....	42
Wireshark Preferences.....	43
Packet Color Coding.....	45

## **4 WORKING WITH CAPTURED PACKETS 47**

Working with Capture Files.....	47
Saving and Exporting Capture Files.....	48
Merging Capture Files.....	49
Working with Packets.....	49
Finding Packets.....	50
Marking Packets.....	51
Printing Packets.....	51
Setting Time Display Formats and References.....	52
Time Display Formats.....	52
Packet Time Referencing.....	52
Setting Capture Options.....	53
Capture Settings.....	53
Capture File(s) Settings.....	54
Stop Capture Settings.....	55
Display Options.....	56
Name Resolution Settings.....	56
Using Filters.....	56
Capture Filters.....	56
Display Filters.....	62
Saving Filters.....	65

## **5 ADVANCED WIRESHARK FEATURES 67**

Network Endpoints and Conversations.....	67
Viewing Endpoints.....	68
Viewing Network Conversations.....	69
Troubleshooting with the Endpoints and Conversations Windows.....	70
Protocol Hierarchy Statistics.....	71
Name Resolution.....	72
Enabling Name Resolution.....	73
Potential Drawbacks to Name Resolution.....	73
Protocol Dissection.....	74
Changing the Dissector.....	74
Viewing Dissector Source Code.....	76
Following TCP Streams.....	76
Packet Lengths.....	78

Graphing .....	79
Viewing IO Graphs .....	79
Round-Trip Time Graphing.....	81
Flow Graphing .....	82
Expert Information .....	82

## **6 COMMON LOWER-LAYER PROTOCOLS 85**

Address Resolution Protocol .....	86
The ARP Header.....	87
Packet 1: ARP Request .....	88
Packet 2: ARP Response.....	89
Gratuitous ARP .....	89
Internet Protocol .....	91
IP Addresses .....	91
The IPv4 Header .....	92
Time to Live .....	93
IP Fragmentation .....	95
Transmission Control Protocol .....	98
The TCP Header.....	98
TCP Ports.....	99
The TCP Three-Way Handshake .....	101
TCP Teardown .....	103
TCP Resets.....	105
User Datagram Protocol.....	105
The UDP Header .....	106
Internet Control Message Protocol .....	107
The ICMP Header.....	107
ICMP Types and Messages.....	107
Echo Requests and Responses .....	108
Traceroute .....	110

## **7 COMMON UPPER-LAYER PROTOCOLS 113**

Dynamic Host Configuration Protocol.....	113
The DHCP Packet Structure .....	114
The DHCP Renewal Process .....	115
DHCP In-Lease Renewal .....	119
DHCP Options and Message Types .....	120
Domain Name System .....	120
The DNS Packet Structure .....	121
A Simple DNS Query .....	122
DNS Question Types .....	124
DNS Recursion .....	124
DNS Zone Transfers .....	127
Hypertext Transfer Protocol.....	129
Browsing with HTTP .....	129
Posting Data with HTTP .....	131
Final Thoughts.....	132

<b>8</b>	<b>BASIC REAL-WORLD SCENARIOS</b>	<b>133</b>
Social Networking at the Packet Level .....		134
Capturing Twitter Traffic .....		134
Capturing Facebook Traffic .....		137
Comparing Twitter vs. Facebook Methods .....		140
Capturing ESPN.com Traffic .....		140
Using the Conversations Window .....		140
Using the Protocol Hierarchy Statistics Window .....		141
Viewing DNS Traffic .....		142
Viewing HTTP Requests .....		143
Real-World Problems .....		144
No Internet Access: Configuration Problems .....		144
No Internet Access: Unwanted Redirection .....		147
No Internet Access: Upstream Problems .....		150
Inconsistent Printer .....		153
Stranded in a Branch Office .....		155
Ticked-Off Developer .....		159
Final Thoughts.....		163
<b>9</b>	<b>FIGHTING A SLOW NETWORK</b>	<b>165</b>
TCP Error-Recovery Features .....		166
TCP Retransmissions .....		166
TCP Duplicate Acknowledgments and Fast Retransmissions.....		169
TCP Flow Control .....		173
Adjusting the Window Size .....		174
Halting Data Flow with a Zero Window Notification .....		175
The TCP Sliding Window in Practice.....		175
Learning from TCP Error-Control and Flow-Control Packets.....		178
Locating the Source of High Latency .....		179
Normal Communications.....		180
Slow Communications—Wire Latency.....		180
Slow Communications—Client Latency.....		181
Slow Communications—Server Latency .....		182
Latency Locating Framework.....		182
Network Baselineing .....		183
Site Baseline.....		184
Host Baseline.....		185
Application Baseline.....		186
Additional Notes on Baselines .....		186
Final Thoughts.....		187
<b>10</b>	<b>PACKET ANALYSIS FOR SECURITY</b>	<b>189</b>
Reconnaissance .....		190
SYN Scan .....		190
Operating System Fingerprinting .....		194

Exploitation .....	197
Operation Aurora .....	197
ARP Cache Poisoning .....	202
Remote-Access Trojan .....	206
Final Thoughts.....	213

## 11

### **WIRELESS PACKET ANALYSIS 215**

Physical Considerations .....	216
Sniffing One Channel at a Time .....	216
Wireless Signal Interference .....	217
Detecting and Analyzing Signal Interference .....	217
Wireless Card Modes.....	218
Sniffing Wirelessly in Windows .....	219
Configuring AirPcap.....	219
Capturing Traffic with AirPcap .....	221
Sniffing Wirelessly in Linux.....	222
802.11 Packet Structure .....	223
Adding Wireless-Specific Columns to the Packet List Pane .....	225
Wireless-Specific Filters.....	226
Filtering Traffic for a Specific BSS ID.....	226
Filtering Specific Wireless Packet Types .....	227
Filtering a Specific Frequency .....	227
Wireless Security .....	228
Successful WEP Authentication.....	229
Failed WEP Authentication .....	230
Successful WPA Authentication .....	231
Failed WPA Authentication.....	232
Final Thoughts.....	233

## **APPENDIX**

### **FURTHER READING 235**

Packet Analysis Tools.....	235
tcpdump and Windump .....	235
Cain & Abel .....	236
Scapy .....	236
Netdude .....	236
Colasoft Packet Builder .....	237
CloudShark .....	237
pcapr .....	237
NetworkMiner .....	238
Tcpreplay.....	238
ngrep .....	238
libpcap .....	239
hping.....	239
Domain Dossier .....	239
Perl and Python.....	239

Packet Analysis Resources .....	239
Wireshark Home Page.....	239
SANS Security Intrusion Detection In-Depth Course .....	239
Chris Sanders Blog .....	240
Packetstan Blog .....	240
Wireshark University .....	240
IANA .....	240
TCP/IP Illustrated (Addison-Wesley).....	240
The TCP/IP Guide (No Starch Press) .....	240

## **INDEX**

**241**