

Table of Contents

Foreword by Gerald Combs, Creator of Wireshark	xxvii
Preface	xxix
About This Book	xxx
Who is This Book For?	xxx
How is This Book Organized?	xxx
How Can I Find Something Fast in This Book?	xxxiii
What Do Those Icons Mean?	xxxiii
Trace Files Used in This Book (.pcapng Format)	xxxiii
What’s Online at <i>www.wiresharkbook.com</i> ?	xxxiv
Which Version of Wireshark Did You Use to Write This Book?	xxxiv
Which WCNA Exam Version Does This Book Cover?	xxxiv
How Can I Submit Comments/Change Requests for This Book?	xxxv
Wireshark Certified Network Analyst™ Program Overview	xxxv
Why Should I Pursue the Wireshark CNA Certification?	xxxv
How Do I Earn the Wireshark CNA Certified Status?	xxxv
Wireshark CNA Exam Objectives	xxxvi
Wireshark University™ and Wireshark University™ Training Partners	xxxvi
Schedule Customized Onsite/Web-Based Training	xxxvi
Chapter 1: The World of Network Analysis	1
Define Network Analysis	2
Follow an Analysis Example	3
Walk-Through of a Troubleshooting Session	6
Walk-Through of a Typical Security Scenario (aka Network Forensics)	8
Troubleshooting Tasks for the Network Analyst	9
Security Tasks for the Network Analyst	10
Optimization Tasks for the Network Analyst	10
Application Analysis Tasks for the Network Analyst	10
Understand Security Issues Related to Network Analysis	11
Define Policies Regarding Network Analysis	11
Files Containing Network Traffic Should be Secured	11
Protect Your Network against Unwanted “Sniffers”	11
Be Aware of Legal Issues of Listening to Network Traffic	12
Overcome the “Needle in the Haystack Issue”	13
Review a Checklist of Analysis Tasks	14
Understand Network Traffic Flows	15
Switching Overview	15
Routing Overview	16
Proxy, Firewall and NAT/PAT Overview	17
Other Technologies that Affect Packets	18
Warnings about “Smarter” Infrastructure Devices	19
Launch an Analysis Session	19

iv Contents

Case Study: Pruning the “Puke”	21
Case Study: The “Securely Invisible” Network	22
Summary	23
Practice What You’ve Learned	23
Review Questions	26
Answers to Review Questions	27
Chapter 2: Introduction to Wireshark.....	29
Wireshark Creation and Maintenance.....	30
Obtain the Latest Version of Wireshark	30
Compare Wireshark Release and Development Versions	31
Thanks to the Wireshark Developers!	32
Calculating the Value of the Wireshark Code	32
Report a Wireshark Bug or Submit an Enhancement.....	32
Following Export Regulations.....	33
Identifying Products that Leverage Wireshark’s Capabilities	34
Capture Packets on Wired or Wireless Networks	34
Libpcap.....	34
WinPcap	34
AirPcap.....	35
Open Various Trace File Types	35
Understand How Wireshark Processes Packets	36
Core Engine.....	36
Dissectors and Plugins and Display Filters	36
GIMP Toolkit (GTK+).....	36
Use the Start Page	37
The Capture Area	38
The Files Area	38
The Online Area	38
The Capture Help Area.....	38
Identify the Nine GUI Elements	39
Add the Wireshark Version to the Title Bar	39
Displaying the Wireless Toolbar (Windows Only)	40
Opening and Closing Panes.....	40
Interpreting the Status Bar.....	41
Navigate Wireshark’s Main Menu	43
File Menu Items	43
Edit Menu Items	47
View Menu Items	51
Go Menu Items	56
Capture Menu Items	58
Analyze Menu Items	59
Statistics Menu Items	64
Telephony Menu Items.....	70
Tools Menu Items.....	72
Internals Menu Items.....	73
Help Menu Items	74

Use the Main Toolbar for Efficiency.....	77
Toolbar Icon Definitions.....	77
Focus Faster with the Filter Toolbar.....	80
Make the Wireless Toolbar Visible.....	82
Work Faster Using Right-Click Functionality.....	83
Right Click Edit or Add Packet Comment.....	84
Right Click Copy.....	85
Right Click Apply As Column.....	86
Right Click Wiki Protocol Page (Packet Details Pane).....	88
Right Click Filter Field Reference (Packet Details Pane).....	88
Right Click Resolve Name (Packet Details Pane).....	88
Right Click Protocol Preferences.....	89
Sign Up for the Wireshark Mailing Lists.....	90
Join ask.wireshark.org!.....	90
Know Your Key Resources.....	91
Get Some Trace Files.....	92
Case Study: Detecting Database Death.....	93
Summary.....	95
Practice What You've Learned.....	95
Review Questions.....	100
Answers to Review Questions.....	101
Chapter 3: Capture Traffic.....	103
Know Where to Tap Into the Network.....	104
Run Wireshark Locally.....	105
Portable Wireshark.....	105
Wireshark U3.....	106
Capture Traffic on Switched Networks.....	107
Use a Simple Hub on Half-Duplex Networks.....	107
Use a Test Access Port (TAP) on Full-Duplex Networks.....	108
Using Analyzer Agents for Remote Capture.....	112
Set up Port Spanning/Port Mirroring on a Switch.....	113
Example of Span Commands.....	114
Spanning VLANs.....	115
Analyze Routed Networks.....	116
Analyze Wireless Networks.....	117
Monitor Mode.....	117
Native Adapter Capture Issues.....	118
Capture at Two Locations (Dual Captures).....	119
Select the Right Capture Interface.....	119
Capture on Multiple Adapters Simultaneously.....	120
Interface Details (Windows Only).....	120
Capture Traffic Remotely.....	121
Configuration Parameters for Remote Capture with rpcapd.exe.....	122
Remote Capture: Active and Passive Mode Configurations.....	123
Save and Use Remote Capture Configurations.....	123

Automatically Save Packets to One or More Files	124
Create File Sets for Faster Access	124
Use a Ring Buffer to Limit the Number of Files Saved	125
Define an Automatic Stop Criteria	125
Optimize Wireshark to Avoid Dropping Packets.....	125
Consider a Dedicated Analyzer Laptop.....	125
Capture Options for Optimization	126
Display Options for Optimization	126
Conserve Memory with Command-Line Capture.....	126
Case Study: Dual Capture Points the Finger.....	128
Case Study: Capturing Traffic at Home.....	130
Summary.....	131
Practice What You’ve Learned	131
Review Questions	133
Answers to Review Questions	134
Chapter 4: Create and Apply Capture Filters	135
The Purpose of Capture Filters	136
Apply a Capture Filter to an Interface	137
Build Your Own Set of Capture Filters.....	139
Identifiers	139
Qualifiers.....	139
Filter by a Protocol	141
Filter Incoming Connection Attempts.....	141
Create MAC/IP Address or Host Name Capture Filters	141
Use a “My MAC” Capture Filter for Application Analysis	143
Filter Your Traffic <i>Out</i> of a Trace File (Exclusion Filter).....	144
Capture One Application’s Traffic Only.....	145
Use Operators to Combine Capture Filters	145
Create Capture Filters to Look for Byte Values.....	146
Manually Edit the Capture Filters File.....	147
Sample <i>cfilters</i> File.....	148
Share Capture Filters with Others	148
Case Study: Kerberos UDP to TCP Issue	149
Summary.....	151
Practice What You’ve Learned	151
Review Questions	152
Answers to Review Questions	153
Chapter 5: Define Global and Personal Preferences	155
Find Your Configuration Folders.....	156
Set Global and Personal Configurations	156
Customize Your User Interface Settings.....	159
“File Open” Dialog Behavior	159
Maximum List Entries.....	159
Pane Configurations	160
Columns	161

Define Your Capture Preferences.....	162
Select a Default Interface for Faster Capture Launch	163
Enable Promiscuous Mode to Analyze Other Hosts' Traffic.....	163
The Future Trace File Format is Here: pcap-ng.....	163
See the Traffic in Real Time.....	164
Automatically Scroll During Capture	164
Automatically Resolve IP and MAC Names	165
Resolve Hardware Addresses (MAC Name Resolution).....	165
Resolve IP Addresses (Network Name Resolution)	167
Plot IP Addresses on a World Map with GeoIP	168
Resolve Port Numbers (Transport Name Resolution).....	168
Resolve SNMP Information	169
Configure Filter Expressions.....	170
Configure Statistics Settings.....	171
Define ARP, TCP, HTTP/HTTPS and Other Protocol Settings.....	172
Detect Duplicate IP Addresses and ARP Storms	172
Define How Wireshark Handles TCP Traffic.....	173
Set Additional Ports for HTTP and HTTPS Dissection.....	174
Enhance VoIP Analysis with RTP Settings	174
Configure Wireshark to Decrypt SSL Traffic.....	174
Configure Protocol Settings with Right-Click.....	175
Case Study: Non-Standard Web Server Setup.....	176
Summary	177
Practice What You've Learned.....	177
Review Questions.....	179
Answers to Review Questions.....	180
Chapter 6: Colorize Traffic.....	181
Use Colors to Differentiate Traffic Types	182
Disable One or More Coloring Rules	183
Share and Manage Coloring Rules	184
Identify Why a Packet is a Certain Color	184
Create a "Butt Ugly" Coloring Rule for HTTP Errors	185
Color Conversations to Distinguish Them	187
Temporarily Mark Packets of Interest.....	188
Alter Stream Reassembly Coloring.....	189
Case Study: Coloring SharePoint Connections During Login.....	191
Summary	192
Practice What You've Learned.....	192
Review Questions.....	197
Answers to Review Questions.....	198
Chapter 7: Define Time Values and Interpret Summaries.....	199
Use Time to Identify Network Problems.....	200
Understand How Wireshark Measures Packet Time.....	200
Choose the Ideal Time Display Format	201
Deal with Timestamp Accuracy and Resolution Issues	203

Send Trace Files Across Time Zones	204
Identify Delays with Time Values	205
Create Additional Time Columns.....	206
Measure Packet Arrival Times with a Time Reference.....	206
Identify Client, Server and Path Delays.....	208
Calculate End-to-End Path Delays	209
Locate Slow Server Responses.....	209
Spot Overloaded Clients.....	209
View a Summary of Traffic Rates, Packet Sizes and Overall Bytes Transferred	210
Compare Up to Three Traffic Types in a Single Summary Window	211
Compare Summary Information for Two or More Trace Files	212
Case Study: Time Column Spots Delayed ACKs	214
Summary.....	216
Practice What You've Learned	216
Review Questions	218
Answers to Review Questions	219
Chapter 8: Interpret Basic Trace File Statistics.....	221
Launch Wireshark Statistics	222
Identify Network Protocols and Applications.....	222
Protocol Settings Can Affect Your Results.....	224
Identify the Most Active Conversations	226
List Endpoints and Map Them on the Earth	227
Spot Suspicious Targets with GeoIP.....	228
List Conversations or Endpoints for Specific Traffic Types.....	228
Evaluate Packet Lengths	229
List All IPv4/IPv6 Addresses in the Traffic.....	231
List All Destinations in the Traffic	231
List UDP and TCP Usage	232
Analyze UDP Multicast Streams	232
Graph the Flow of Traffic	234
Gather Your HTTP Statistics	236
Examine All WLAN Statistics.....	237
Case Study: Application Analysis: Aptimize Website Accelerator™	238
Case Study: Finding VoIP Quality Issues.....	243
Summary.....	245
Practice What You've Learned	245
Review Questions	247
Answers to Review Questions	248
Chapter 9: Create and Apply Display Filters	249
Understand the Purpose of Display Filters.....	250
Create Display Filters Using Auto-Complete	253
Apply Saved Display Filters	254
Use Expressions for Filter Assistance.....	255

Make Display Filters Quickly Using Right-Click Filtering.....	256
Apply as Filter	257
Prepare a Filter.....	257
Copy As Filter	257
Filter on Conversations and Endpoints.....	258
Filter on the Protocol Hierarchy Window	258
Understand Display Filter Syntax.....	259
Combine Display Filters with Comparison Operators.....	260
Alter Display Filter Meaning with Parentheses.....	261
Filter on the Existence of a Field.....	261
Filter on Specific Bytes in a Packet.....	262
Find Key Words in Upper or Lower Case.....	263
More Interesting Regex Filters.....	263
Let Wireshark Catch Display Filter Mistakes	264
Use Display Filter Macros for Complex Filtering.....	264
Avoid Common Display Filter Mistakes.....	266
Manually Edit the <i>dfilters</i> File.....	267
Case Study: Using Filters and Graphs to Solve Database Issues.....	269
Case Study: The Chatty Browser.....	270
Case Study: Catching Viruses and Worms.....	271
Summary	272
Practice What You've Learned.....	272
Review Questions.....	274
Answers to Review Questions.....	275
Chapter 10: Follow Streams and Reassemble Data.....	277
The Basics of Traffic Reassembly.....	278
Follow and Reassemble UDP Conversations	278
Follow and Reassemble TCP Conversations.....	280
Identify Common File Types.....	283
Reassemble an FTP File Transfer	283
Follow and Reassemble SSL Conversations	285
Reassemble an SMB Transfer.....	287
Case Study: Unknown Hosts Identified.....	288
Summary	289
Practice What You've Learned.....	289
Review Questions.....	291
Answers to Review Questions.....	292
Chapter 11: Customize Wireshark Profiles.....	293
Customize Wireshark with Profiles.....	294
Create a New Profile.....	295
Share Profiles.....	296
Create a Troubleshooting Profile	297
Create a Corporate Profile	298
Create a WLAN Profile	298
Create a VoIP Profile.....	299
Create a Security Profile.....	300

Case Study: Customizing Wireshark for the Customer	301
Summary	302
Practice What You've Learned	302
Review Questions	303
Answers to Review Questions	304
Chapter 12: Annotate, Save, Export and Print Packets	305
Annotate a Packet or an Entire Trace File	306
Save Filtered, Marked and Ranges of Packets	309
Export Packet Content for Use in Other Programs	311
Export SSL Keys	313
Save Conversations, Endpoints, IO Graphs and Flow Graph Information	314
Export Packet Bytes	314
Case Study: Saving Subsets of Traffic to Isolate Problems	315
Summary	317
Practice What You've Learned	317
Review Questions	319
Answers to Review Questions	320
Chapter 13: Use Wireshark's Expert System.....	321
Let Wireshark's Expert Information Guide You.....	322
Launch Expert Info Quickly	322
Colorize Expert Info Elements	325
Filter on TCP Expert Information.....	326
Understand TCP Expert Information	327
What Triggers TCP Retransmissions?.....	327
What Triggers Previous Segment Not Captured?.....	328
What Triggers ACKed Lost Packet?	328
What Triggers Keep Alive?.....	328
What Triggers Duplicate ACK?	328
What Triggers Zero Window?.....	329
What Triggers Zero Window Probe?	329
What Triggers Zero Window Probe ACK?	329
What Triggers Keep Alive ACK?	329
What Triggers Out-of-Order?.....	330
What Triggers Fast Retransmission?.....	330
What Triggers Window Update?.....	330
What Triggers Window is Full?	331
What Triggers TCP Ports Reused?.....	331
What Triggers 4 NOP in a Row?.....	331
Case Study: Expert Info Catches Remote Access Headaches.....	333
Summary	337
Practice What You've Learned	337
Review Questions	338
Answers to Review Questions	339

Chapter 14: TCP/IP Analysis Overview	341
TCP/IP Functionality Overview	342
When Everything Goes Right	343
Follow the Multi-Step Resolution Process	343
Step 1: Port Number Resolution	345
Step 2: Network Name Resolution (Optional)	345
Step 3: Route Resolution—When the Target is Local	346
Step 4: Local MAC Address Resolution	346
Step 5: Route Resolution—When the Target is Remote	346
Step 6: Local MAC Address Resolution for a Gateway	347
Build the Packet	347
Case Study: Absolving the Network from Blame	350
Summary	351
Practice What You've Learned	351
Review Questions	352
Answers to Review Questions	353
Chapter 15: Analyze Domain Name System (DNS) Traffic	355
The Purpose of DNS	356
Analyze Normal DNS Queries/Responses	357
Analyze DNS Problems	359
Dissect the DNS Packet Structure	362
Transaction ID	363
Flags	363
Question Count	365
Answer Resource Record (RR) Count	365
Authority RRs Count	365
Additional RRs Count	365
Queries	365
Answer RRs	366
Authority RRs	366
Additional RRs	366
Resource Record Time to Live (TTL) Value	366
Filter on DNS/MDNS Traffic	367
Case Study: DNS Killed Web Browsing Performance	368
Summary	371
Practice What You've Learned	371
Review Questions	373
Answers to Review Questions	374
Chapter 16: Analyze Address Resolution Protocol (ARP) Traffic	375
Identify the Purpose of ARP	376
Analyze Normal ARP Requests/Responses	377
Analyze Gratuitous ARPs	379
Analyze ARP Problems	380

Dissect the ARP Packet Structure	382
Hardware Type	382
Protocol Type	382
Length of Hardware Address	382
Length of Protocol Address	382
Opcode	382
Sender's Hardware Address	383
Sender's Protocol Address	383
Target Hardware Address	383
Target Protocol Address	383
Filter on ARP Traffic	383
Case Study: Death by ARP	384
Case Study: The Tale of the Missing ARP	385
Summary	387
Practice What You've Learned	387
Review Questions	388
Answers to Review Questions	389
Chapter 17: Analyze Internet Protocol (IPv4/IPv6) Traffic	391
Identify the Purpose of IP	392
Analyze Normal IPv4 Traffic	393
Analyze IPv4 Problems	394
Dissect the IPv4 Packet Structure	395
Version Field	395
Header Length Field	396
Differentiated Services Field and Explicit Congestion Notification	396
Total Length Field	397
Identification Field	397
Flags Field	397
Fragment Offset Field	398
Time to Live Field	399
Protocol Field	400
Header Checksum Field	400
IPv4 Source Address Field	400
IPv4 Destination Address Field	400
Options Field	401
IPv4 Broadcast/Multicast Traffic	401
An Introduction to IPv6 Traffic	402
Dissect the IPv6 Packet Structure	403
Version Field	403
Traffic Class Fields (DiffServ, ECT and ECN-CE)	403
Flow Label Field	403
Payload Length Field	403
Next Header Field	404
Hop Limit Field	404
Source IPv6 Address Field	404
Destination IPv6 Address Field	404

Basic IPv6 Addressing	405
Auto Configuration Mode (no DHCP Server) (M=0 and O=0)	408
DHCPv6 Stateful Mode (M=1)	408
DHCPv6 Stateless Mode (M=0 and O=1)	408
6to4 Tunneling (IPv6 Tunneled Inside IPv4)	409
Teredo	410
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	411
Sanitize Your IP Addresses in Trace Files	411
Set Your IPv4 Protocol Preferences	413
Reassemble Fragmented IP Datagrams	413
Enable GeoIP Lookups	413
Interpret the Reserved Flag as a Security Flag (RFC 3514) <g>	413
Troubleshoot Encrypted Communications	413
Filter on IPv4 Traffic	415
Filter on IPv6 Traffic	415
Case Study: Everyone Blamed the Router	416
Case Study: It's Not the Network's Problem!	417
Case Study: IPv6 Addressing Mayhem	418
Summary	420
Practice What You've Learned	420
Review Questions	422
Answers to Review Questions	423
Chapter 18: Analyze Internet Control Message Protocol (ICMPv4/ICMPV6)	
Traffic	425
The Purpose of ICMP	426
Analyze Normal ICMP Traffic	427
Analyze ICMP Problems	429
Dissect the ICMP Packet Structure	430
Type	430
Code	431
Checksum	433
Basic ICMPv6 Functionality	434
Filter on ICMP and ICMPv6 Traffic	438
Case Study: The Dead-End Router	439
Summary	440
Practice What You've Learned	440
Review Questions	441
Answers to Review Questions	442
Chapter 19: Analyze User Datagram Protocol (UDP) Traffic	445
The Purpose of UDP	446
Analyze Normal UDP Traffic	447
Analyze UDP Problems	448

Dissect the UDP Packet Structure.....	450
Source Port Field.....	450
Destination Port Field.....	450
Length Field.....	451
Checksum Field.....	451
Filter on UDP Traffic.....	451
Case Study: Troubleshooting Time Synchronization.....	452
Summary.....	453
Practice What You've Learned.....	453
Review Questions.....	454
Answers to Review Questions.....	455
Chapter 20: Analyze Transmission Control Protocol (TCP) Traffic	457
The Purpose of TCP.....	458
Analyze Normal TCP Communications.....	459
The Establishment of TCP Connections.....	459
When TCP-based Services are Refused.....	460
The Termination of TCP Connections.....	461
How TCP Tracks Packets Sequentially.....	463
How TCP Recovers from Packet Loss.....	465
Improve Packet Loss Recovery with Selective Acknowledgments.....	467
Understand TCP Flow Control.....	470
Understand Nagling and Delayed ACKs.....	471
Analyze TCP Problems.....	473
Dissect the TCP Packet Structure.....	477
Source Port Field.....	477
Destination Port Field.....	477
Stream Index [Wireshark Field].....	477
Sequence Number Field.....	477
Next Expected Sequence Number [Wireshark Field].....	477
Acknowledgment Number Field.....	477
Data Offset Field.....	477
Flags Field.....	478
Window Field.....	479
Checksum Field.....	479
Urgent Pointer Field.....	479
TCP Options Area (Optional).....	480
Filter on TCP Traffic.....	482
Set TCP Protocol Preferences.....	483
Validate the TCP Checksum if Possible.....	483
Allow Subdissector to Reassemble TCP Streams.....	483
Analyze TCP Sequence Numbers.....	485
Relative Sequence Numbers.....	486
Window Scaling is Calculated Automatically.....	486
Track Number of Bytes in Flight.....	487
Try Heuristic Sub-Dissectors First.....	487
Ignore TCP Timestamps in Summary.....	487
Calculate Conversation Timestamps.....	488

Case Study: Connections Require Four Attempts	489
Summary	490
Practice What You've Learned.....	490
Review Questions.....	492
Answers to Review Questions.....	493
Chapter 21: Graph IO Rates and TCP Trends	495
Use Graphs to View Trends.....	496
Generate Basic IO Graphs.....	497
Filter IO Graphs.....	498
Coloring	499
Styles and Layers	499
X and Y Axis	500
Smoothing.....	500
Print Your IO Graph	501
Generate Advanced IO Graphs.....	501
SUM(*) Calc.....	501
MIN(*), AVG(*) and MAX(*) Calc Values.....	503
COUNT(*) Calc.....	504
LOAD(*) Calc	505
Compare Traffic Trends in IO Graphs.....	506
Graph Round Trip Time	508
Graph Throughput Rates	510
Graph TCP Sequence Numbers over Time	511
Interpret TCP Window Size Issues	511
Interpret Packet Loss, Duplicate ACKs and Retransmissions	514
Case Study: Watching Performance Levels Drop	515
Case Study: Graphing RTT to the Corporate Office	516
Case Study: Testing QoS Policies	519
Summary	520
Practice What You've Learned.....	520
Review Questions.....	522
Answers to Review Questions.....	523
Chapter 22: Analyze Dynamic Host Configuration Protocol (DHCPv4/DHCPv6)	
Traffic.....	525
The Purpose of DHCP	526
Analyze Normal DHCP Traffic.....	526
Analyze DHCP Problems	530
Dissect the DHCP Packet Structure.....	532
Message Type	532
Hardware Type	532
Hardware Length	532
Hops.....	532
Transaction ID	532
Seconds Elapsed	532
BOOTP Flags.....	532
Client IP Address	532
Your (Client) IP Address	532

Next Server IP Address	532
Relay Agent IP Address	533
Client MAC Address	533
Server Host Name	533
Boot File Name	533
Magic Cookie	533
Option	533
An Introduction to DHCPv6	534
Display BOOTP-DHCP Statistics	536
Filter on DHCP/DHCPv6 Traffic	537
Case Study: Declining Clients	538
Summary	540
Practice What You've Learned	540
Review Questions	542
Answers to Review Questions	543
Chapter 23: Analyze Hypertext Transfer Protocol (HTTP) Traffic	545
The Purpose of HTTP	546
Analyze Normal HTTP Communications	547
Analyze HTTP Problems	551
Dissect HTTP Packet Structures	554
HTTP Methods	555
Host	555
Request Modifiers	555
Filter on HTTP or HTTPS Traffic	556
Export HTTP Objects	558
Display HTTP Statistics	558
HTTP Load Distribution	558
HTTP Packet Counter	559
HTTP Requests	559
Graph HTTP Traffic Flows	561
Choose Packets	561
Choose Flow Type	561
Choose Node Address Type	561
Set HTTP Preferences	563
Analyze HTTPS Communications	564
Analyze SSL/TLS Handshake	565
Analyze TLS Encrypted Alerts	569
Decrypt HTTPS Traffic	570
Export SSL Keys	574
Case Study: HTTP Proxy Problems	575
Summary	576
Practice What You've Learned	576
Review Questions	578
Answers to Review Questions	579

Chapter 24: Analyze File Transfer Protocol (FTP) Traffic	581
The Purpose of FTP	582
Analyze Normal FTP Communications.....	583
Analyze Passive Mode Connections	586
Analyze Active Mode Connections	588
Analyze FTP Problems.....	589
Dissect the FTP Packet Structure	591
Filter on FTP Traffic	594
Reassemble FTP Traffic.....	595
Case Study: Secret FTP Communications	596
Summary	598
Practice What You've Learned.....	598
Review Questions.....	600
Answers to Review Questions.....	601
Chapter 25: Analyze Email Traffic	603
The Purpose of POP	604
Analyze Normal POP Communications	605
Analyze POP Problems	606
Dissect the POP Packet Structure.....	608
Filter on POP Traffic.....	610
The Purpose of SMTP	611
Analyze Normal SMTP Communications	612
Analyze SMTP Problems	613
Dissect the SMTP Packet Structure.....	614
Filter on SMTP Traffic.....	616
Case Study: SMTP Problem—Scan2Email Job	617
Summary	618
Practice What You've Learned.....	618
Review Questions.....	619
Answers to Review Questions.....	620
Chapter 26: Introduction to 802.11 (WLAN) Analysis	621
Analyze WLAN Traffic.....	622
Analyze Signal Strength and Interference	623
Capture WLAN Traffic	626
Compare Monitor Mode vs. Promiscuous Mode	626
Select the Wireless Interface.....	627
Set Up WLAN Decryption.....	628
Select to Prepend Radiotap or PPI Headers	631
Compare Signal Strength and Signal-to-Noise Ratios	635
Understand 802.11 Traffic Basics	636
Data Frames	636
Management Frames	636
Control Frames	638
Analyze Normal 802.11 Communications	638
Dissect the 802.11 Frame Structure.....	640

Filter on All WLAN Traffic	641
Analyze Frame Control Types and Subtypes	642
Customize Wireshark for WLAN Analysis	647
Case Study: Cruddy Barcode Communications	648
Case Study: Cooking the WLAN	650
Summary	652
Practice What You've Learned	652
Review Questions	655
Answers to Review Questions	656
Chapter 27: Introduction to Voice over IP (VoIP) Analysis	659
Understand VoIP Traffic Flows	660
Session Bandwidth and RTP Port Definition	663
Analyze VoIP Problems	665
Packet Loss	665
Jitter	666
Examine SIP Traffic	667
SIP Commands	667
SIP Response Codes	668
Examine RTP Traffic	672
Play Back VoIP Conversations	674
RTP Player Marker Definitions	675
Create a VoIP Profile	676
Filter on VoIP Traffic	676
Case Study: Lost VoIP Tones	677
Summary	679
Practice What You've Learned	679
Review Questions	680
Answers to Review Questions	681
Chapter 28: Baseline "Normal" Traffic Patterns	683
Understand the Importance of Baselining	684
Baseline Broadcast and Multicast Types and Rates	685
Baseline Protocols and Applications	685
Baseline Boot up Sequences	686
Baseline Login/Logout Sequences	687
Baseline Traffic during Idle Times	687
Baseline Application Launch Sequences and Key Tasks	687
Baseline Web Browsing Sessions	688
Baseline Name Resolution Sessions	688
Baseline Throughput Tests	688
Baseline Wireless Connectivity	689
Baseline VoIP Communications	689
Case Study: Login Log Jam	690
Case Study: Solving SAN Disconnects	691
Summary	692
Practice What You've Learned	692
Review Questions	694
Answers to Review Questions	695

Chapter 29: Find the Top Causes of Performance Problems	697
Troubleshoot Performance Problems	698
Identify High Latency Times.....	699
Filter on Arrival Times	700
Filter on the Delta Times	701
Filter on the Time since Reference or First Packet	701
Filter on TCP Conversation Times	702
Point to Slow Processing Times	702
Practice Working with Time Issues	703
Find the Location of Packet Loss	706
Watch Signs of Misconfigurations	708
Analyze Traffic Redirections.....	709
Watch for Small Payload Sizes	710
Look for Congestion.....	711
Identify Application Faults.....	711
Note Any Name Resolution Faults.....	712
An Important Note about Analyzing Performance Problems	713
Case Study: One-Way Problems	714
Case Study: The Perfect Storm of Network Problems	715
Summary	719
Practice What You've Learned.....	719
Review Questions.....	721
Answers to Review Questions.....	722
Chapter 30: Network Forensics Overview	723
Compare Host vs. Network Forensics	724
Gather Evidence	724
Avoid Detection	725
Handle Evidence Properly	728
Recognize Unusual Traffic Patterns	729
Color Unusual Traffic Patterns.....	730
Check Out Complementary Forensic Tools	731
Case Study: SSL/TLS Vulnerability Studied	732
Summary	734
Practice What You've Learned.....	734
Review Questions.....	736
Answers to Review Questions.....	737
Chapter 31: Detect Scanning and Discovery Processes	739
The Purpose of Discovery and Reconnaissance Processes.....	740
Detect ARP Scans (aka ARP Sweeps).....	740
Detect ICMP Ping Sweeps	742
Detect Various Types of TCP Port Scans.....	743
TCP Half-Open Scan (aka “Stealth Scan”).....	744
TCP Full Connect Scan.....	746
Null Scans.....	747
Xmas Scan	748

FIN Scan.....	749
ACK Scan.....	749
Detect UDP Port Scans	751
Detect IP Protocol Scans.....	752
Understand Idle Scans.....	753
Know Your ICMP Types and Codes	756
Try These Nmap Scan Commands.....	757
Analyze Traceroute Path Discovery	757
Detect Dynamic Router Discovery	760
Understand Application Mapping Processes	760
Use Wireshark for Passive OS Fingerprinting.....	763
Detect Active OS Fingerprinting	765
Identify Attack Tools	768
Identify Spoofed Addresses in Scans.....	769
Case Study: Learning the Conficker Lesson.....	770
Summary.....	772
Practice What You’ve Learned	772
Review Questions	774
Answers to Review Questions	775
Chapter 32: Analyze Suspect Traffic	777
What is “Suspect” Traffic?	778
Identify Vulnerabilities in the TCP/IP Resolution Processes.....	778
Port Resolution Vulnerabilities	779
Name Resolution Process Vulnerabilities	781
MAC Address Resolution Vulnerabilities.....	782
Route Resolution Vulnerabilities	783
Identify Unacceptable Traffic	783
Find Maliciously Malformed Packets	784
Identify Invalid or ‘Dark’ Destination Addresses	786
Differentiate Between Flooding and Denial of Service Traffic.....	787
Find Clear Text Passwords and Data.....	789
Identify Phone Home Traffic	790
Catch Unusual Protocols and Applications	791
Locate Route Redirection that Uses ICMP.....	793
Catch ARP Poisoning.....	794
Catch IP Fragmentation and Overwriting.....	796
Spot TCP Splicing.....	797
Watch Other Unusual TCP Traffic.....	798
Identify Password Cracking Attempts.....	798
Build Filters and Coloring Rules from IDS Rules	800
Header Signatures	801
Sequence Signatures.....	801
Payload Signatures	801
Sample Wireshark Filters from IDS/IPS Rules	801

Case Study: The Flooding Host.....	803
Case Study: Catching Keylogging Traffic.....	804
Case Study: Passively Finding Malware	805
Summary	806
Practice What You've Learned.....	806
Review Questions.....	808
Answers to Review Questions.....	809
Chapter 33: Effective Use of Command-Line Tools.....	811
Understand the Power of Command-Line Tools	812
Use Wireshark.exe (Command-Line Launch).....	813
Wireshark Syntax.....	813
Customize Wireshark's Launch.....	815
Capture Traffic with Tshark	817
Tshark Syntax	817
View Tshark Statistics	821
Gather Host Name with Tshark	823
Examine Service Response Times (SRT) with Tshark	825
Tshark Examples.....	826
Dealing with Bug 2234	827
List Trace File Details with Capinfos.....	828
Capinfos Syntax.....	828
Capinfos Examples	829
Edit Trace Files with Editcap	831
Editcap Syntax	831
Editcap Examples	833
Merge Trace Files with Mergecap.....	834
Mergecap Syntax	835
Mergecap Examples.....	835
Convert Text with Text2pcap.....	836
Text2pcap Syntax	837
Text2pcap Examples.....	838
Capture Traffic with Dumpcap.....	839
Dumpcap Syntax.....	839
Dumpcap Examples	840
Understand Rawshark.....	841
Rawshark Syntax	841
Case Study: Getting GETS and a Suspect	843
Summary	844
Practice What You've Learned.....	844
Review Questions.....	846
Answers to Review Questions.....	847

Appendix A: Resources on the Book Website	849
Video Starters	850
Chanalyzer Pro/Wi-Spy Recordings (.wsx Files)	850
MaxMind GeoIP Database Files (.dat Files).....	851
PhoneFactor SSL/TLS Vulnerabilities Documents/Trace Files.....	851
Wireshark Customized Profiles	851
Practice Trace Files.....	852
Index.....	913

List of Tips

Download the Supplements from <i>www.wiresharkbook.com</i>	xxxi
Wireshark is Constantly Changing	8
Avoid Prison Time	12
Get Notified of New Wireshark Releases	31
Access the Wireshark Developer Guide	35
No Interface? No Capture!	38
Avoid File Merge Issues	44
Frames vs. Packets	44
Overloading HTTP Object Export	45
Use Packet Marking to Identify Interesting Packets	47
Use the Perfect Time Display Format for Troubleshooting	52
Don't Let Wireshark Flood a DNS Server	53
Editing Wireshark's <i>Services</i> File is OK, but...	54
Compare Packets with Side-by-Side Views	56
Practice Jumping Between Corresponding Packets	57
See Packet Counts Without Capturing Anything	58
Disabling a Protocol May Blind You	61
Reassemble Streams for Faster Interpretations	63
When Wireshark Doesn't Recognize RTP Traffic	70
Learn Where Your Wireshark Components Reside	76
The Packet Number Never Changes	77
Don't Kill Wireshark Performance	87
Easily Resolve a Single IP Address	88
Get Notified When New Wireshark Versions are Released	90
Hubs are Only a Half-Duplex Option	107
Watch Timestamp Issues on Multiple NIC Captures	109
Cheating on Your Spanning [Contributor: Jim Aragon]	115
Monitor Mode Blocks Other Connectivity	118
Toggle Capture Interface Information to IPv4 Addresses	120
Experiment with Remote Capture Traffic	122
Select Multiple Criteria for Capture Stop	125
Easily Remove Duplicate Packets in Your Capture	126

xxiv Contents

Understand Why There are Checksum Errors on YOUR Traffic Only	127
Wireshark Says “Where,” but Not Always “Why”	129
Use Capture Filters Sparingly and Display Filters Generously	136
Avoid <code>host</code> Capture Filters with Web Browsing Sessions	143
When to Use MAC Capture Filters Instead of IP Address Filters	143
Make Wireshark More Efficient	160
Add a TCP Window Size Field Column to Spot Problems	162
Be Careful when Hiding Interfaces	163
Network Name Resolution Can Slow Wireshark to a Crawl	167
Warnings about Using a Special Wireshark <code>hosts</code> File	167
Warnings about SNMP Object Dissection Support	169
Use New Filter Expression Buttons for Faster Troubleshooting	170
Checksum Validation Settings	173
Checksum Errors and Coloring Rules	184
Coloring Rules are Processed in Order Top to Bottom	185
Use Packet Marking to Save Non-Contiguous Packets	188
Handshakes Provide a Nice Snapshot of Latency	208
Characterize All Protocols and Applications Used by a Host	224
Database Communications are Weird Interesting!	230
ARP Packets Do Not Match IP Address Filters	231
Use Flow Graphs to Spot Web Browsing Issues	235
Use Your Display Filters in Command Line Capture	252
How to Ensure Your Display Filter is Saved	254
Understand Wireshark Warnings on Using <code>!=</code>	260
Add an <i>Inclusion</i> Field with <i>Exclusion</i> Field Filters	264
Consider VLC Player to Play Back Exported Video Files	279
Create from a <i>Master Profile</i> First	296
Be Careful Sharing Profiles	296
Import Some Profiles	298
Avoid the “Needle in the Haystack Issue” by Saving Subsets	309
Print Packet Summaries in Landscape Mode	310
Use Your Own Screen Capture Utility	313
Check out Cascade Pilot™ for Graphing	314
Check Expert Notes AND Warnings	322

Always Double-Check Expert Findings	323
Use a <code>tcp.analysis.flags</code> Filter Expression Button	326
What Makes an Item a Warning vs. a Note?	327
When to Consider Trashing a Trace File	328
Window Update Packets Were Colorized Incorrectly (prior to Wireshark 1.8)	330
Disable Wireshark's Expert Feature... with Caution	332
Use the Best TCP Setting for Analyzing HTTP Traffic	349
Quickly Detect DNS Errors	364
ARP is Local Only	376
Watch Out for Proxy ARP	380
Use the IP ID Field to Spot Looping Packets	397
Microsoft Changed Their IPv6 SLAAC Default Setting	408
IPv6 Address Sanitization	411
Measure Round Trip Time Using an ICMP Filter	427
You Should Know About Jon Postel	431
Extending ICMP	437
FIN Doesn't Mean "Shut Up"	461
Follow Along with the Trace File	463
Move Wireshark Around when Packet Loss is Identified	467
Send Buffers and Application Limitation Issues	471
The TCP Window Size > Zero Can Still Stop Data Transfer	471
Watch for SYN/ACKs After a Full Handshake	475
Filter on the TCP Flags Summary Line	479
Watch Out for Altered Options	481
Watch Out for Bytes in Flight Values During SACK	487
Use Wireshark's TCP Timestamp for Troubleshooting	487
Empty Graphs May Indicate You Selected the Wrong Packet	496
Red is Bad, Green is Good—Using Color Assumptions	499
Consider Using a Logarithmic Scale on Your IO Graph	500
Use the IO Graph to Prioritize Your Troubleshooting Focus	503
Understand and Plot TCP Packet Loss Recovery Processes	505
Use Capinfos <code>-S</code> Setting to Time-Shift Trace Files	507
Screen Capture those TCP Time-Sequence Graphs	511
The Time-Sequence Graph Reigns Supreme	513

Using <code>tcp.analysis.rtt</code> vs. <code>tcp.time_delta</code>	518
Disable Stream Reassembly to See HTTP More Clearly	550
Watch Out For Cache-Loaded Web Pages	550
Don't Troubleshoot Large Delays before FIN or Reset Packets	552
Don't Use the <code>http</code> Filter to Analyze Web Browsing	556
Create a Flow Graph to Spot Web Site Dependencies	561
Follow Along with an HTTPS Handshake Analysis	565
Delays Before Encrypted Alerts May be OK	570
Is There a Worm in the Trace File?	604
Rule Out the Wired Network to Point to the WLAN	622
Get Help Setting Up WLAN Capture	627
The Missing Details Button	628
Let Wireshark Resolve WLAN Decryption Key Conflicts	628
Put Most Often Used Decryption Keys on Top of the Key List	630
Use a Radiotap or PPI Header to Filter on WLAN Channels	632
Translate WLAN Type/Subtype Values to Hex for Easy Filtering	643
Filter on a Conversation Before Sorting the Time Column	699
Beware of <code>frame.time_delta_displayed</code>	701
Use Packet Marking to Speed Up Your Troubleshooting	704
Use a <code>tcp.len</code> Column to Easily See Payload Size	710
4 NOPS Expert Warning	718
Use Nmap on Your Network (with Permission)	740
Watch for Microsoft-Limited Connection Attempts	744
Don't Create a Black Hole	756
Generate Your HTTP User-Agent Value	764
You Need to Order the Nmap Book...Now!	767
Anyone Can Spoof a MAC Address!	769
Filter on Upper OR Lower Case Characters	781
Filter on the Macof Signature	788
Catch the Traffic When You Run Malicious Tools	795
Add Wireshark to Your Path	812
View Numerous Statistics with One Tshark Command Line	821
Use Editcap to Split a Large Trace into File Sets	831
Merge Traces to Compare Them Side by Side in an IO Graph	834

Index

4 NOPs in a Row, 8, 331, 481, 718

802.11. See WLAN analysis

A

accelerator keys, 40, 47

ACKed Lost Segment, 896

Active Directory Migration Tool (ADMT) troubleshooting, 149

address resolution

gateway MAC address resolution, 347

MAC address resolution, 343, 346

vulnerabilities, 782

Address Resolution Protocol (ARP). See ARP analysis

AirPcap adapters. See also WLAN

as a complementing tool, 34

hardware add-on, 2

overview, 118

passive mode, 35

Analyze menu, 59–63

apply and prepare as a filter, 60

conversation filter, 63

Decode As function, 61

display filter macros, 60

display filters, 59

enabled protocols, 60

Expert Info, 63

follow UDP, TCP or SSL streams, 63

user specified decodes, 62

annotations in trace files, 41, 50, 84, 164, 306–8

Anyplace Control, remote capture option, 121

application analysis

baselining packet lengths, 229

BitTorrent Tracker communications, 145

case study for, 238

causes of MTU size issues, 230

file transfer applications, 230

maps.google.com, *analyzing traffic to*, 23

tasks for the network analyst, 10

Twitter traffic analysis, 270

virus detection programs, phone home behavior of, 790

web browsing endpoint analysis, 227

application mapping, 760–62

Apply as Column feature, 88

Arkin, Ofir, 767

ARP analysis, 375–87

analyzing problems, 380

ARP cache, 346–47

broadcast, 346

capture filter syntax, 383

case study of troubleshooting, 385

display filter for requests, 251

display filter syntax, 383

example display filters, 383

gratuitous process, 379

local capture only, 376

not visible in IP address list, 231

opcodes, 382

overview, 343, 376

packet structure, 382

ping analysis, 740

poisoning, 380, 794

protocol settings, 172

proxy, 380

proxy response filter, 383

RFC 826, 376

scan analysis, 740

standard lookup requests, 377

static address bootup uses, 379

storm detection, 172, 381

target hardware address, 382

target protocol address, 382

unicast responses not seen, 380

attack signatures, 800–802

header signatures, 801

LDPinch Trojan Loader, 801

locations, 800

payload signatures, 801
 sequence signatures, 801
 Weevely PHP backdoor, 802
 Win32 Rimecud Trojan, 802

automatic scrolling feature, warnings about, 164
avoiding detection of your Wireshark system, 725–28, 734

B

baselining, 683–93

application launch and key tasks, 687
 bootup sequence, 686
 broadcasts and multicasts, 685
 detecting unusual traffic by, 791
 elements of, 685
 idle time, 687, 695
 key uses of, 684
 login/logout sequences, 687
 name resolution sessions, 688
 overview, 684
 protocols and applications, 685
 saving traffic subsets, 309
 suspect traffic does not match, 778
 throughput tests, 688
 VoIP communications, 689
 web browsing sessions, 688
 wireless connectivity, 689

Bejtlich, Richard, 92

Berkeley Packet Filter (BPF) format, 250

Bjørlykke, Stig, 167

Bluetooth traffic, capturing, 38

BOOTP. See DHCPv4 analysis

broadband internet modem, troubleshooting, 130

broadcasts

addresses, 226
 excessive numbers of, 401
 lookups vs. announcements, 401

browsing problems with Flow Graphs, 235

buffer size, 126

C

CACE Technologies, 2

canonical name, 358, See also DNS analysis

Capinfos, 828–30

examples of, 829
 overview, 828
 syntax, 828

capture filters, 135–51

“Not my MAC” filter, application analysis
 with, 144
 based on TCP flags, 141
 byte offset, 146
cfilters file
 default *cfilters* file, 137
 global settings, 156
 in corporate profile, 298
 in profiles, 296
 in security profile, 300
 in troubleshooting profile, 297
 in VoIP profile, 299
 in WLAN profile, 298
 manually editing the *cfilters* file, 147
 sample *cfilters* file, 148
 update overrides, 158
 DNS traffic, 145
 exclusion filters, 144
 filter by address or host name, 141
 filter by application, 145
 filtering by protocol, 141
 identifier, 139
 My MAC for application analysis, 143
 operators, 145
 overview, 136
 portrange filter, 145
 primitives, 140
 profiles used in, 137
 qualifiers, 139
 sample formats for, 140
 sharing the *cfilters* file, 148
 tcpdump filter syntax, 136
 UDP for SIP and RTP traffic, 299
 use in multiple interfaces, 138
 warnings regarding, 136
 warnings using “host”, 143

Capture menu

- capture filters, 59
- capture interface list, 58
- capture options, 58
- capture traffic, 103–34**
 - AirPcap, 34–35
 - analyzer placement for measuring round trip time, 104
 - analyzer placement in WLAN networks, 117–18
 - analyzer placement overview, 104
 - automatic stop, 125
 - capture interfaces window, 119–20
 - default interface, 162
 - dual captures, 119
 - half-duplex capture with a hub, 107
 - half-duplex networks, analyzing, 107
 - interface details, 120
 - interfaces not seen, 119
 - interfering programs, 126
 - libpcap, 34–35
 - port mirroring. *See* port spanning
 - port spanning, 113
 - cheating, 116
 - destination span port, 113
 - egress traffic, 113
 - example span commands, 114
 - ingress traffic, 113
 - monitor port, 113
 - source span port, 113
 - source span VLAN, 113
 - spanning VLANs, 115
 - promiscuous mode
 - definition of, 117
 - enabling, 163
 - errors on WLAN capture, 626
 - scanning with NetScanTools Pro, 727
 - remote capture
 - active and passive mode, 123
 - analyzer agents, 112
 - example configuration, 121
 - hosts permitted to access, 121
 - overview, 121–23
 - rpcapd, 132
 - rpcapd configuration parameters, 122
 - rpcapd daemon, 121
 - saving capture configurations, 123

- restarting, 59
- setting preferences, 162
- simultaneous multiple adapter capture, 120
- stopping, 59
- testing a hub, 107
- using the ring buffer, 125
- WinPcap, 34–35

Cascade Pilot, 34, 314**case studies**

- "Securely Invisible" Network, 22
- Absolving the Network from Blame, 350
- Application Analysis
 - Optimize Website Accelerator, 238–42
- Capturing Traffic at Home, 130
- Catching Keylogging Traffic, 804
- Catching Viruses and Worms, 271
- Chatty Browser, 270
- Colorizing SharePoint Connections During Login, 191
- Connections Require Four Attempts, 489
- Cooking the WLAN, 650–51
- Cruddy Barcode Communications, 648–49
- Customizing Wireshark for the Customer, 301
- Dead-End Router, 439
- Death by ARP, 384
- Declining Clients, 538–39
- Detecting Database Death, 93–94
- DNS Killed Web Browsing
 - Performance, 368–70
- Dual Capture Points the Finger, 128–29
- Everyone Blamed the Router, 416
- Expert Info Catches Remote Access
 - Headaches, 333–36
- Finding VoIP Quality Issues, 243–44
- Flooding Host, 803
- Getting GETS and a Suspect, 843
- Graphing RTT to the Corporate Office, 516–18
- HTTP Proxy Problems, 575
- It's Not the Network's Problem, 417
- Kerberos UDP to TCP Issue, 149–50
- Learning the Conficker Lesson, 770–71
- Login Log Jam, 690
- Lost VoIP Tones, 677–78
- Non-Standard Web Server Setup, 176
- Passively Finding Malware, 805

- Perfect Storm of Network Problems, 715–18
- Pruning the Puke, 21
- Saving Subsets of Traffic to Isolate Problems, 315–16
- Secret FTP Communications, 596–97
- SMTP Problem - Scan2Email Job, 617
- Solving SAN Disconnects, 691
- SSL/TLS Vulnerability Studied, 732–33
- Tale of the Missing ARP, 385–86
- Testing QoS Policies, 519
- Time Column Spots Delayed ACKs, 214–15
- Troubleshooting Time Synchronization, 452
- Unknown Host Identified, 288
- Using Filters and Graphs to Solve Database Issues, 269
- Watching Performance Levels Drop, 515
- cfilters file, 137, See also capture filters*
- Character Generator (chergen), 761*
- checksum errors*
 - coloring rule, 184
 - disabling coloring rule, 127
 - invalid IP header, 251
 - newer Wireshark defaults, 127
 - task offloading, 120, 127
 - validation settings, 173
- Cisco*
 - ACL rules, 72
 - Cisco IOS, 114
 - Cisco Nexus 7000 Series switches, 34
 - Cisco PIX firewall TCP sequence number randomization issue, 617
 - CSCsw70786 - SACK stripped off, 19
 - port security issues, 115
 - span command example, 114*
- code_swarm, 30*
- coloring rules, 181–96*
 - ARP, 182
 - bad TCP traffic, 182, 325
 - colorfilters file*
 - global version, 182
 - in corporate profile, 298
 - in profiles, 296
 - in security profile, 300
 - in troubleshooting profile, 297
 - in VoIP profile, 299
 - in WLAN profile, 299
 - update overrides, 158
- copying vs. import/export, 184
- default placement of new rule (Wireshark 1.8 and later), 185
- defaults, 55, 182
- disable all, 183
- disabling checksum errors, 127
- HSRP state change, 182
- HTTP error detection, 185
- identifying the source, 184
- importing/exporting, 184
- incorrect coloring prior to Wireshark 1.8, 330
- LDPinch Loader Binary Request coloring rule, 801
- low time to live value, 182
- order of processing, 185
- OS fingerprinting signatures, 766
- OSPF state change, 182
- overview, 182
- reDuh backdoor coloring rule, 800
- striped traffic, 428
- TCP resets, 182
- unusual traffic patterns, 730
- using names for filtering, 325
- Weeveily PHP backdoor coloring rule, 802
- Win32 Rimecud.A coloring rule, 802
- Win32 Sykipot GET coloring rule, 802
- Window Update excluded from Bad TCP, 55
- Colton, busy little dude, 8*
- columns*
 - Apply as Column feature, 86
 - default, 161
 - default packet length, 710
 - display filtering on, 256
 - hide/display, 60
 - occurrence of a field, 86
 - re-ordering, 161
 - settings, 86
 - tcp.len, 710
- Combs, Gerald, xxvii, xxxvi, 30, 32*
- Command and Control (C&C) servers, 724, 730, 779, See also security analysis*

Comments in trace files. See Annotations in trace files

compare

- packets side-by-side, 56
- trace files in IO Graphs, 506
- using merged files to graph performance comparison, 506
- using summaries for, 211

connectivity tests, analyzing, 427

conversations

- coloring, 187
- definition of, 226
- lists, 228
- saving information, 314
- statistics, 226
- vs. endpoints, 65

copy feature, 85

Cummings, JJ, 92

CVE-2009-3103 – malicious SMBv2 packets, 784

D

data link layer, two parts of, 15

Data Protection Directive, European Union, 12

database traffic

- case study analyzing, 93
- unique characteristics of, 229

DCE RPC traffic, 791

decryption

- key management, 628
- SSL data tab, 574

default gateway, location of, 346

Degioanni, Loris, 30

delta time analysis, 205. See also time analysis

DHCPv4 analysis, 525–33

- Acknowledgment, 528
- analyzing problems, 530
- Boot File Name field, 533
- BOOTP Flags field, 532
- BOOTP-DHCP statistics, 536
- capture filter syntax, 537
- capture filter warning, 531
- Cisco router as a Relay Agent, 529
- client and server ports, 526
- client inside address lease time, 527

- Client IP Address field, 532
- Client MAC Address field, 533
- client outside address lease time, 527
- Decline, 528
- Discover process, 447, 528
- Discover-Offer-Request-Acknowledgment sequence, 527
- display filter examples, 251, 537
- duplicate address problems, 530
- Hardware Length field, 532
- Hardware Type field, 532
- Hops field, 532
- Information, 528
- Lease Time (LT), 528
- Magic Cookie, 533
- Message Type field, 532
- Message Type field values, 528
- Negative Acknowledgment, 528
- Next Server IP Address field, 532
- Offer, 528
- Options list, 533
- overview, 343, 526
- packet structure, 532
- Rebind Time (T2), 528
- rebinding state, 528
- relay agent display filter, 251
- Relay Agent IP Address field, 533
- relay agents, 529
- Release, 528
- Renewal Time (T1), 528
- Request, 528
- Request-Acknowledgment sequence, 527
- Seconds Elapsed field, 532
- Server Host Name field, 533
- Transaction ID field, 532
- Your (Client) IP Address field, 532

DHCPv6 analysis, 534–36

- Advertise, 534
- capture filter syntax, 537
- client and server ports, 534
- display filter examples, 537
- message type list, 535
- multicast discovery address, 534
- overview, 534
- Request, 534
- Solicit, 534

Differentiated Services Code Point (DSCP), 300, 396, 403, 676

disabling protocols

disabled_protos file in profiles, 296
warnings, 61

discovery processes

analyzing scans, 745
application mapping with NULL probes, 761
idle scans using zombies, 753
OS fingerprinting
 active process, 765
 coloring rules, 766
 display filters, 767
 ICMP-based, 767
 passive process, 763
 sample display filter for, 300
 signatures, 765
 User-Agent information, 763–64
path discovery mechanisms, 757
ping scan analysis, 742
port scans, 743
stealth scan signature, 744
traceroute
 ICMP, TCP and UDP variations, 428
 overriding default TTL values, 399

Dispensa, Steve, 570**display filters, 249–75**

application analysis, 270
Apply as Filter, 60, 257
applying to IP destination statistics, 231
auto-complete, 253
color coding of, 264
common mistakes, 266
conversation directions, 258
conversations and endpoints, 258
creating for Expert Info elements, 326
dfilters file
 global settings, 156
 in corporate profile, 298
 in profiles, 296
 in security profile, 300
 in troubleshooting profile, 297
 in VoIP profile, 299
 in WLAN profile, 298
 manually editing, 267
 update overrides, 158
dfilters_macros file, 264–65
DSCP example, 300
examples of expressions, 255

expressions, 255
field names in status area, 259
filter expression buttons, 51, 80, 170
filtering on offset and bytes, 252
filtering on time values, 701
Firefox browser, display filter for, 557
identify existence of field, 261
IPv4 address, 266
IPv6 address, 266
IPv6 examples, 415
IRC JOIN packets, 781
LDPinch Loader Binary Request filter, 801
macros, 264
maximum entries to list, 80
offset filters, 262
operators, 260
OS fingerprinting, 767
overview, 36, 250
parentheses, 261
prepare as filter, 257
recently used setting, 80
reDuh backdoor filter, 800
reordering filter list, 267
saving, 254
syntax, 259, 415
TCP analysis flags, 251, 261
TCP conversation timestamp filtering, 702
TCP flag summary line, 479
upper or lower case ASCII, 263
use for comparing, 211
used for coloring rules, 259
using expressions, 255
using regular expressions (RegEx), 263
using with Tshark, 252
validity checking mechanism, 253, 264
warning against using
 frame.time_delta_displayed, 701
Weeveily PHP backdoor filter, 802
Win32 Rimecud.A filter, 802
Win32 Sykipot GET filter, 802

dissectors

Decode As function, 61, 779
dissector tables, 73
for VoIP, 662
forcing, 61
handoff process, 36
learn to create, 35
none available for application, 289
overview, 36

DNS analysis, 355–72

- Additional RRs Count, 365
- Answer Resource Record (RR) Count, 365
- authoritative answer, 364
- Authority RRs Count, 365
- cache, 781
- cache timeout, 349
- cached information, 348
- canonical name (CNAME), 24, 358, 781
- capture filter examples, 145
- concurrent resolution, 167
- display filter examples, 367
- DNS Transaction ID matching, 363
- examples of problems, 429
- filter on error responses, 367
- Flags field, 363
- host name filter, 251
- mDNS filtering, 367
- network name resolution overview, 345
- No Such Name response, 359
- overview, 343, 356
- packet structure, 362
- pointer query filter, 367
- ports used for UDP or TCP, 362
- problem examples, 359
- PTR queries from Wireshark, 53
- Query format, 365
- query process, 357
- query type, 365
- Question Count, 365
- recursion, 364
- Resource Record TTL field, 366
- response codes, 364
- response process, 357
- retries, 361
- sample analysis process for, 24
- Server Failure responses, 359
- Transaction ID field, 363
- truncation, 364
- unsolicited response packet, 768

Domain Name System (DNS). *See* **DNS analysis**

Dual-Tone Multi-Frequency (DTMF), 660, See also VoIP analysis

Dumpcap, 839–40

- examples of use, 840
- memory requirements, 127

- overview, 839
- syntax of, 839
- t to use separate threads, 840

Duplicate ACKs, 329

duplicate IPv4 addresses, 376

duplicate IPv6 addresses, 343

duplicate packets

- in dual captures, 128
- removal with Editcap, 831
- VPN client causes, 126

Dynamic Host Configuration Protocol (DHCP).

See **DHCPv4 analysis and DHCPv6 analysis**

E**Edit menu, 47–51**

- configuration profiles, 50
- Edit or Add Packet Comment, 50
- mark packets, 47
- preferences, 50
- time reference, 48
- time shift, 49

Editcap, 831–33

- adjusting timestamps, 832
- examples of use, 833
- overview, 831
- split a trace file, 832
- syntax, 831
- truncate packets, 832
- use in dual captures, 119

electronic surveillance, 12, See also legal issues

encrypted communications, 413, See also SSL/TLS analysis

encryption validation, use of, 789

endpoints

- definition of, 226
- lists, 228
- saving information, 314

Enhanced Interior Gateway Routing Protocol (EIGRP), 752

Errors & Omissions, 12, See also legal issues

Ethereal

- creation of, 30
- name change from, 30

Ethernet

- header structure, 262
- Maximum Transmission Unit (MTU), 229
- packet sizes, 229
- source address filter, 262

Ettercap, 795**Expert Info, 321–39**

- 4 NOPs in a Row, 331
- ACKed Lost Packet, 328
- button color classifications, 322
- chats, 41, 322
- color coding of button, 41
- coloring scheme, 41
- debates regarding development, 327
- depicting packet loss, 323
- description, 468
- Duplicate ACKs
 - definition of, 328
 - graphing, 504
 - Time-Sequence graph depiction of, 514
- duplicate IP addresses detected, 794
- enabling LEDs, 323
- errors, 41, 322
- expanding packet lists, 323
- Fast Retransmission, 330
- Fast Retransmission and Retransmission
 - under Notes (Wireshark 1.8 and later), 323
- Fast Retransmissions moved to Notes, 322
- Keep Alive, 328
- Keep Alive ACK, 329
- LEDs on tab labels, 41
- notes, 41, 322
- Out-of-order, 330
- overview, 322
- Previous Segment Not Captured, 323, 328
- Retransmissions, 327
- TCP Ports Reused, 331
- validating discoveries, 323
- warnings, 41, 322
- Window is Full, 331
- Window Update, 330

- Zero Window, 329
- Zero Window Probe, 329
- Zero Window Probe ACK, 329

Expert Info Composite

- data files cannot be Window Updates, 330

exporting

- CSV format, 311
- HTTP objects, 45
- HTTP objects warning, 45
- packet bytes, 314
- raw data format, 314
- SSL Keys, 45
- to Excel, 311–13

F**file identifiers, 283****File menu, 43–46**

- export, 45
- file set, 44
- import, 44
- merge, 43
- open recent, 43

file sets, 44

- booktcpset*.pcapng* sample, 44
- multiple stop criteria, 125
- naming convention, 124
- next file criteria, 124
- overview, 124
- used for optimization, 126
- viewing, 44
- working with large trace files, 226

File Transfer Protocol (FTP). See FTP analysis**firewall effect on traffic, 17. See also security analysis, firewalls****fragmentation, 393. See also IPv4 analysis****frame sizes**

- low Maximum Transmission Unit (MTU)
 - size, 392, 423
- Maximum Segment Size (MSS)
 - option, 480
- Maximum Segment Size (MSS) value, 229
- small Maximum Segment Size (MSS)
 - value, 471

frames vs. packets, 44

FTP analysis, 581–99

- 331 Password Required, 585
- 425 Error—Possible bounce attack/FXP transfer, 590
- Active Mode file transfer, 588
- capture filter syntax, 594
- client commands list, 583, 591
- command channel, 283, 582, 585
- connection problems, 589
- CWD (change working directory) command, 586
- data channel, 585
- detect password errors, 799
- display filter examples, 594
- display filter expressions, 255
- display filter syntax, 586, 594
- NLST (directory list) command, 588
- overview, 582
- packet structure, 591
- PASS (password) command, 585
- passive mode operations, 586
- passive mode problem, 589
- PASV (passive mode) command, 586
- reassembling traffic, 595
- resolution processes preceding, 344
- response codes, 592
- RETR (retrieve) command, 586
- secret connection case study, 596
- server response codes, 583
- single-byte transfer, 797
- USER command, 585

G

GeoIP mapping

- example of use, 227
- IPv6 support, 168, 228
- MaxMind databases, 168
- overview, 168
- step-by-step setup, 168
- support for, 50
- suspicious flags on map, 228
- unusual results, 228

Go menu, 56–57

- Go to Corresponding Packet, 57

graphing, 495–521

- advanced IO Graph
 - AVG(*) calc value, 503
 - COUNT(*) calc value, 504
 - launching, 501
 - LOAD(*) calc value, 505
 - logarithmic comparison of analysis flags, 505
 - MAX(*) calc value, 503
 - MIN(*) calc value, 503
 - overview, 501
 - SUM(*) calc value, 501
- advanced IO Graphs
 - MIN, MAX and AVG, 66
- Flow Graphs
 - saving in ASCII format, 234, 314
 - spotting browsing problems, 235
- IO Graphs
 - appear empty, 496
 - beacon problems, 637
 - color assumptions, 499
 - comparing trace files in, 506
 - logarithmic scale use, 500
 - overview of basic, 497
 - printing, 501
 - save feature limitations, 314
 - Smoothing, 500
 - styles, 499
 - TCP payload lengths, 710
 - tick interval, 497
 - units and scale, 497
 - use to prioritize problems, 503
 - using colors in, 499
 - using display filters with, 498
 - X axis and the Y axis, 500
- overview of basic, 496
- RTT vs. delta graphing, 518
- TCP Round Trip Time graph
 - depicting Duplicate ACKs, 509
 - depicting packet loss, 509
 - overview of, 508
- TCP Time-Sequence graph
 - better than Window Scaling graph, 513
 - delayed ACKs on, 471
 - empty, 511
 - I bar format, 511

- interpreting the receive window, 511
- overview, 511
- plotting direction, 511
- tcptrace compared to Stevens graph, 511
- Window Size graph, 511

H

Help menu, 74–76

- configuration and program folders, 76
- Wireshark authors list, 32
- Wireshark version, 75

High Technology Crime Investigation Association (HTCIA), 728

hosts file, 167

HTTP analysis, 545–77

- 301/302 redirections, 559
- 304 Not Modified status code, 550
- 403 Forbidden status code, 553
- 404 Not Found status code, 551, 559, 711
- 4xx Client Error detection, 559
- 5xx Server Error detection, 559
- Allow subdissector to reassemble TCP streams setting, 174, 550
- applying display filters to statistics, 558
- best TCP setting for analysis, 349
- capture filter for non-standard ports, 556
- capture filter syntax, 556
- determining web site redirections and dependencies, 559
- display filter examples, 557
- display filter syntax, 556
- error coloring rule, 551
- example of analyzing, 4
- exporting objects, 281, 558
- Flow Graphs, 561
- follow the stream of a POST process, 281
- GET and POST, 68
- GET filter, 251
- GET request for /., 548
- Host field, 555
- If-Modified-Since modifier, 556
- listing requests, 559
- Load Distribution, 558
- Methods list, 555

- non-standard port case study, 176
- overview, 546
- packet counter, 236, 559
- packet structures, 554
- port preference setting, 563, 781
- POST problem, 553
- preferences, 174
- reassemble HTTP objects, 281
- redirection, 234
- Request Modifiers, 555
- requests, Flow Graphing, 236
- response codes, 236
- round trip time evaluations, 208
- slow download, 323
- spoofed User-Agent warning, 764
- statistics, 68, 558
- Status Code list, 548
- User-Agent definition, 763
- website's database problem, 552
- Wireshark default port numbers, 547

I

ICMPv4 analysis, 425–40

- Address Mask Requests, 767
- analyzing ICMP problems, 429
- black hole detection, 420
- capture filter syntax, 438
- Code list, 431
- Destination Unreachable
 - Destination Host Unknown responses, 432
 - Destination Network Unknown responses, 432
 - display filter, 252
 - fragmentation problems, 432, 438
 - Host Unreachable or Network Unreachable, 346
 - Port Unreachable responses, 360, 432
 - protocol unreachable responses, 431
 - purpose of, 426
- display filter for unusual ping packets, 438
- display filter syntax, 438
- Echo Requests and Echo Replies (“pings”), 427
- errors in coloring rules, 182
- excessive redirects, 429

- Fragmentation Needed, but Don't Fragment Bit Set, 393
- ICMP-based pings, limitations of, 740
- Information Requests, 767
- MTU size issues, 230
- OS fingerprinting display filter, 438
- overview, 343, 426
- packet structure, 430
- path discovery, 757
- redirection, 346, 426, 429, 433, 793
- required fields, 430
- Router Advertisement, 439, 760
- Router Solicitations, 439, 760
- Timestamp Requests, 767
- Type list, 430
- ICMPv6 analysis, 434–38**
 - capture filter syntax, 438
 - code descriptions, 436
 - display filter examples, 438
 - Echo Request/Reply example, 434
 - errors in coloring rules, 182
 - Neighbor Advertisement, 406
 - Neighbor Solicitation, 406
 - overview, 343, 426, 434
 - registered type numbers, 434
 - Router Advertisement, 406
 - Router Solicitation, 406
- IEEE OUI list, 165**
- ignore packets, 42, 48**
- interface list**
 - missing Details button, 628
 - opening, 38
- Internals menu, 73–74**
 - dissector tables, 73
 - supported protocols, 74
- Internet Assigned Numbers Authority (IANA), 91, See also Websites**
- Internet Control Message Protocol (ICMP). See ICMPv4 analysis and ICMPv6 analysis**
- Internet Explorer**
 - causing client performance problems, 711
 - detected in User-Agent string, 764
 - HTTP User-Agent designations, 763
- Internet Group Management Protocol (IGMP), 232**
- Internet Protocol (IP). See IPv4 analysis and IPv6 analysis**
- Internet Relay Chat (IRC). See IRC analysis**
- Internet Storm Center (ISC), 743**
- Intrusion Detection System (IDS), 724**
- IO Graphs, 66**
- IPsec**
 - Authentication Header (AH), 413
 - Encapsulating Security Payload (ESP), 413
- IPv4 analysis, 391–421**
 - 0.0.0.0 source address, 400
 - address conflict, 380
 - address details, 231
 - address display filter mistakes, 266
 - capture filter syntax, 415
 - Destination Address field, 400
 - Differentiated Services field, 396
 - display filter examples, 415
 - duplicate IP addresses
 - detection, 172, 343
 - disabling detection, 381
 - gratuitous ARPs, 379
 - enable GeoIP lookups, 413
 - Explicit Congestion Notification, 396
 - filtering on fragments, 415
 - Flags field, 397
 - fragmentation
 - and the TTL field, 399
 - Don't Fragment bit, 397
 - overview, 393
 - overwriting, 796
 - problems, 394
 - purpose, 393
 - reassembly, 413
 - Fragmentation
 - Offset field, 398
 - Header Length field, 396
 - header structure, 262
 - ID field, 397
 - idle scan, 754
 - initializing the stack, 379
 - invalid destination addresses, 786
 - Mobile IP filter, 255
 - Options field, 401
 - overview, 342, 392
 - packet structure, 395
 - preferences, 413
 - Protocol field, 400
 - protocol scans, 752

- sanitize IP addresses, 411
- Source Address field, 400
- spoofed address detection, 769
- Total Length field, 397
- traffic overview, 393
- TTL field, 399
 - decremented by routers, 399
 - expiration, 399
 - low value, 757
 - starting values for, 399
 - TTL Exceeded in Transit, 433
- unusual addresses, 394
- Version field, 395

IPv6 analysis, 402–11

- 6to4 Tunneling, 409
- address compression, 405
- address display filter, 266
- address display filter mistakes, 266
- anycast address definition, 405
- basic addressing overview, 405
- broadcast not used in, 405
- capture filters for, 415
- Classless Inter-Domain Routing (CIDR)
 - representation, 405
- Destination IP Address field, 404
- display filters for, 415
- DNS AAAA record, 19
- Duplicate Address Detection (DAD) in IPv6, 343, 406
- extension headers, 404
- Flow Label field, 403
- Hop Limit field, 404
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 411
- multicast address definition, 405
- Next Header field, 404
- overview, 342, 392, 402
- packet structure, 403
- Payload Length field, 403
- sanitize addresses, 411
- Source IP Address field, 404
- Teredo, 410
- Traffic Class field, 403
- unicast address definition, 405
- Version field, 403

IRC analysis

- display filter samples, 300
- in protocol hierarchy, 225

- JOIN command, 779
- using non-standard port, 779

K**Keep Alive, 328****Keep Alive ACK, 329, See also Expert Info****Kerberos troubleshooting, 149****keyboard shortcuts, 188****L****Lamping, Ulf, 38****large trace files, 124****latency**

- delay before FIN/Reset, 552
- detect with the Time column, 52
- high latency paths, 466
- high server latency example, 209
- identify high TCP time deltas, 487
- practice detecting issues, 703
- queuing depicted by Round Trip Time graph, 509
- relationship to slow performance, 200
- snapshot of, 208
- spotting client latency issues, 209
- spotting server latency issues, 209
- unacceptable times, 699

LDPinch Trojan Loader, 801**legal issues, 12**

- consult counsel, 12
- Electronic Communications and Privacy Act (ECPA), "Wiretap Act", 12
- Errors & Omissions rider, 12
- Foreign Intelligence Surveillance Act (FISA), 12
- Health Insurance Portability and Accountability Act (HIPAA), 12
- local laws, 12
- non-disclosure agreement, 11
- Personally Identifiable Information (PII), 12
- policies regarding analysis, 11
- prison, avoiding, 12
- related to analysis, 11

Logmein, remote capture option, 121
loopback address, 394
Lotus Notes, misconfiguration of, 22
Lyon, Gordon "Fyodor", 731, 740

M

macros, 264, See also display filters
mailing lists, 90
main toolbar, 77–79
 capture toolbar icons, 77
 color and scroll toolbar icons, 78
 filter, color and configuration toolbar icons, 79
 finding a packet, 78
 help toolbar icon, 79
 navigation toolbar icons, 77
 trace file and print toolbar icons, 77
 viewer toolbar icons, 78
manuf file
 editing, 165
 overview, 156
marked packets
 clearing, 188
 fast navigation with, 47
 for faster troubleshooting, 704
 saving, 188
 toggling on and off, 188
 use for comparing, 211
Mathieson, Martin, 676
memory requirements, Dumpcap vs. Tshark, 127
merge trace files (GUI), 43–44
Mergecap, 119, 834–35
 examples of, 835
 overview, 834
 syntax, 835
 using with non-aggregating taps, 109
MetaGeek Wi-Spy products, 117, 624, 623–25, 652–53, 850
Microsoft. See also SMB analysis
 different IPv6 settings, 408
 Security Bulletin MS09-050, 785
 Service Pack 2 for XP, 744
Mobile IP, filtering for, 255

monitor mode, 117, See also WLAN analysis
most active connections, detection of, 226
Mu Dynamics (pcapr.net sponsor), 38
multicast analysis
 address range, 401
 Apple mDNS traffic, 356
 burst statistics, 233
 excessive, 401
 IGMP support, 232
 in endpoint window, 226
 multicast DNS (mDNS), 356
 setting burst thresholds, 233
 storms, 416
multifunctional device (MFD), case study of, 617
Multiprotocol Label Switching (MPLS), effect on network traffic, 18

N

name resolution
 in basic communications, 345
 MAC name resolution, 165
 network name resolution
 disable for optimization, 126
 DNS PTR queries, 167
 in basic FTP communication, 343
 performance impact, 167
 warning, 53
 resolve a single IP address, 88
 settings, 165
 transport name resolution, 168
 vulnerabilities, 781
 Wireshark capabilities, 53
navigating
 corresponding packets, 57
 find feature, 78
 new packet window, 56
Network Address Translation (NAT), effect on network traffic, 17
network analysis, general
 definition, 2
 example analyzing HTTP sessions, 348
 overview of tasks, 14
 skills required for, 2
Network Time Protocol. See NTP

Nmap analysis and use, 760–62, 765–67

- ACK scan, 749
- address spoofing, 769
- ARP scan, 740
- coloring rule for detection, 730
- commands, 757
- dealing with connection number restrictions, 744
- detecting idle scans, 754
- detecting through User-Agent, 764
- FIN scan, 749
- get the Nmap book, 767
- ICMP code field value, 729
- ICMP-based ping sweep, 731, 742
- IP protocol scan, 752
- sample scan, 98
- syntax in this book, xxxiii
- UDP scan, 752
- using decoys, 769
- www.nmap.org site, 740
- Xmas scan, 748

normal network communications, overview of, 343***Norton virus detection signature updates, 790******NTP***

- crossing time zones, 204
- overview, 119

Nutter, Ron, 114**O*****Open Shortest Path First (OSPF) analysis, 232, 343******Open Systems Interconnection (OSI) model, 15******OpenStreetMap, 228******optimization***

- case study of removing unnecessary traffic, 21
- of Wireshark, 125–27
- optimization tasks for network analysts, 10

OS fingerprinting. See discovery processes***other tools and products***

- Amap, 760
- Bit-Twist and Bit-Twiste (packet editing), 411
- Cain and Abel, 731, 794
- Chanalyzer Pro and Wi-Spy, 623–25
- Ettercap, 731, 794
- Hping2, 731
- John the Ripper, 731
- Kismet, 731
- Macof, 787
- MetaGeek Wi-Spy and Chanalyzer, 624, *See also* MetaGeek Wi-Spy products
- Metasploit Framework, 731
- Nessus, 731
- Netcat, 731
- NetScanTools Pro
 - OS fingerprinting, 729
 - overview, 726, 767
 - signature in ICMP Echo Requests, 768
 - top security tools, 731
- Nikto, 731
- Nmap
 - Gordon Lyon, creator, 731, 740
 - Nmap Network Scanning book, 740
 - overview, 740
 - scan command examples, 757
- SnagIt by TechSmith, 313
- Snort, 731
- Suricata, 801
- tcpdump, 731
- VLC Player, 279
- Xprobe2, 767, 768

Out-of-Order packets, 330**P*****packet loss, 327******packet number value, 77******packet, building the, 347******packet-tcp.c file, 322***

panes

- configuring, 40, 160
- Packet Bytes pane, 40
- Packet Details pane, 40
- Packet List pane, 40

Parsons, Keith (Institute for Network Professionals), 643

Patton, Michael (Ethernet Codes Master Page), 165

pcap-ng format, capability of, 163, See also annotations in trace files

PhoneFactor, 570

POP analysis, 604–10

- analyzing problems, 606
- capture filter syntax, 610
- DELE (delete) command, 605
- display filter syntax, 610
- ERR response, 606
- overview, 604
- packet structure, 608
- Request command list, 608
- RETR command, 608
- spam clogged mailboxes, 607

port numbers

- change defined, 780
- ephemeral/temporary, 447
- resolution, 343–45

portable Wireshark

- download PortableApps, 106
- overview, 105
- WinPcap use, 105

Postel, Jon, 431

preference settings, 156–75

- capture, 50
- customizing user interface settings, 159
- duplicate IP address and ARP storm detection, 172
- file open dialog, 159
- file recent and display list, 159
- file sharing warnings, 42
- global preference files, 156
- global preferences recommended settings, 157

- HTTP settings, 174
- in corporate profile, 298
- in security profile, 300
- in troubleshooting profile, 297
- in VoIP profile, 300
- in WLAN profile, 299
- name resolution, 50
- open recent maximum files setting, 43
- overview, 157
- overview of protocol settings, 172, 175
- personal configuration files, 157
- preferences* file in profiles, 296
- printing, 50
- protocol settings using right-click, 89
- protocols, 51
- reassemble fragmented IP datagram, 398
- restoring *preferences* file, 158
- RTP settings, 174
- SSL settings, 174
- statistics, 51
- TCP settings, 173
- user interface, 50
- warning about sharing *preferences* file, 296

Previous Segment Not Captured, 328**printing, 305–20**

- packet formats, 310
- printing packets to a file, 310
- suggestions for best results, 310
- troubleshooting, 214

profiles, 293–304

- available at wiresharkbook.com, 298
- based on existing profiles, 296
- branch office example, 294
- corporate office example, 298
- create new, 42
- directory contents, 50, 294, 296
- overview, 294
- security example, 300
- sharing with others, 42
- Status Bar column, 42
- troubleshooting example, 297
- VoIP example, 299
- WLAN example, 298

proxy server effect on network traffic, 17

Q

QoS policies, testing, 519

Quilty, Tom (BD Consulting and Investigations), 12

R

Rawshark, 841–42

overview, 841

-p for packet header timestamps, 841

syntax of, 841

Ray, Marsh, 570

Realtime Transport Control Protocol (RTCP). See VoIP analysis, RTCP

Realtime Transport Protocol (RTP). See VoIP analysis, RTP

reassembly, 277–92

coloring streams, 189

colorization of client and server traffic, 189

common file identifiers, 283

follow SSL streams, 189, 285

follow TCP streams, 63, 189, 280

follow UDP streams, 63, 189, 278

overview of follow streams, 278

rebuild HTTP object, 281

video playback, unsupported formats, 279

recent file

in profiles, 296

time display format setting, 51

reload a trace file, 56

Remote Procedure Call (RPC), 225

RFCs

2822, Internet Message Format, 611

RFC 1027, Using ARP to Implement Transparent Subnet Gateways, 380

RFC 1035, Domain Names – Implementation and Specification, 356

RFC 1122, Requirements for Internet Hosts – Communication Layers, 471

RFC 1191, Path MTU Discovery, 710

RFC 1323, TCP Extensions for High Performance, 711

RFC 1730, IMAP, 604

RFC 1939, POP, 604

RFC 1945, HTTP/1.0, 556

RFC 2001, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, 466

RFC 2018, TCP Selective Acknowledgment Options, 467

RFC 2131, Dynamic Host Configuration Protocol, 526

RFC 2246, Transport Layer Security v1.0, 564

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, 402

RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, 396

RFC 2581, TCP Congestion Control, 466, 478

RFC 2582, NewReno Modification to TCP's Fast Recovery Algorithm, 466

RFC 2582, The NewReno Modification to TCP's Fast Recovery Algorithm, 478

RFC 2597, Assured Forwarding PHB Group, 396

RFC 2598, an Expediting Forwarding PHB, 396

RFC 2671, Extension Mechanisms for DNS (EDNS0), 356

RFC 2818, HTTP over TLS, 564

RFC 3056, Connection of IPv6 Domains via IPv4 Clouds, 409

RFC 3168, The Addition of Explicit Congestion Notification (ECN), 397

RFC 3261, Session Initiation Protocol (SIP), 667

RFC 3264, An Offer/Answer Model with the Session Description Protocol (SDP), 663

RFC 3514, A Security Flag in the IPv4 Header, 413

RFC 3540, Robust Explicit Congestion Notification (ECN) Signaling with Nonces, 478

RFC 3550, Real-time Transport Protocol, 666

RFC 3665, Session Initiation Protocol (SIP) Basic Call Flow Examples, 667

RFC 3697, IPv6 Flow Label Specification, 403

RFC 4291, IP Version 6 Addressing Architecture, 402

RFC 4380, Tunneling IPv6 over UDP through Network Address Translations (NATs), 410

RFC 4566, SDP
Session Description Protocol, 663

RFC 4620, IPv6 Node Information Queries, 437

RFC 4861, Neighbor Discovery for IP version 6 (IPv6), 402

RFC 4884, Extended ICMP to Support Multi-Part Messages, 437

RFC 4941
Privacy Extensions for Stateless Address Autoconfiguration in IPv6, 408

RFC 5214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 411

RFC 5321, Simple Mail Transfer Protocol, 611

RFC 581, TCP Congestion Control, 470

RFC 768, User Datagram Protocol, 446

RFC 791, Internet Protocol, 393

RFC 792, Internet Control Message Protocol, 426

RFC 793, Transmission Control Protocol, 458

RFC 826, Ethernet Address Resolution Protocol, 376

RFC 896, Congestion Control in IP/TCP Internetworks, 471

RFC 903, A Reverse Address Resolution Protocol, 382

RFC 959, File Transfer Protocol, 582

rfmon mode, 118, See also WLAN analysis

right-click functionality, 83–89
filtering, 256, 260

Riverbed Technology
acquisition of CACE Technologies, 30
AirPcap, 118

Round Trip Time graph, 508, See also graphing

route resolution
identify local target, 346
identify remote target, 346
overview, 343
vulnerabilities, 783

routing

analyzing routed networks, 116

asymmetrical indication of, 328

decrementing the time to live, 16

general forwarding behavior, 16

how traffic is forwarded, 16

overview of, 16

stripping off and reapplying a MAC header, 16

RSA key exchange, 285

S

sanitize IP addresses, 411

SANS, 743

saving in various formats, 310

Secure Socket Layer (SSL). See SSL/TLS analysis

security analysis

bot-infected host processes, 790

brute force password crack attempts, 798

cfilters file use in, 300

clear text passwords, detecting, 789

dark destination addresses, 786

denial of service
address spoofing uses, 769
flooding traffic, 787
ping attack, 426
SMBv2 vulnerability, 784

detecting unencrypted communications, 11

detecting unknown hosts, 288

dfilters file use in, 300

dictionary password crack attempts, 799

discovery and reconnaissance
overview, 740

elements of a security profile, 300

evidence handling procedures, 728

example of network forensics process, 8

find JOIN command, 781

firewalls
ACL rules, 72
case study, 575
effect on network traffic, 17
responses from firewalled hosts, 744

flooding traffic, 787

- forensic tools list, 731, *See also* other tools and products
- gathering evidence, 724
- general issues, 11–12
- host forensics, 724
- idle scan process, 753
- LDPinch Loader Binary Request filter or coloring rule, 801
- malicious FTP program, 779
- maliciously malformed packets, 784
- man-in-the-middle attack, 380
- network floods, 787
- network forensics, 724, 737
- password cracking attempts, 798
- password detection using Follow the TCP Stream, 789
- phone home traffic, 790
- placing Wireshark to analyze, 724
- poisoning detection, 794
- port resolution vulnerabilities, 779
- protecting trace files, 11
- reDuh filter or coloring rule, 800
- spoofed address detection, 769
- spoofing a MAC address, 769
- SSL/TLS vulnerabilities, 732
- Suricata IDS/IPS, 801
- suspect traffic, overview of, 778
- SYN floods, 479
- tasks for the network analyst, 10
- TCP window size issues, 300
- TLS renegotiation process flaw, 570
- unassigned MAC addresses, 786
- unknown hardware addresses, 107
- unusual traffic
 - detecting protocols and applications, 791
 - recognizing patterns, 729
 - sample display for ICMP traffic, 300
- unwanted “sniffers”, 11
- using Nmap with decoys, 769
- vulnerabilities in flow diagram, 778
- vulnerabilities in the TCP/IP resolution processes, 778
- Weevely PHP backdoor filter or coloring rule, 802
- Win32 Rimecud.A filter or coloring rule, 802
- Win32 Sykipot GET filter or coloring rule, 802
- Server Message Block (SMB)*. *See SMB analysis*
- Session Description Protocol (SDP)*. *See VoIP analysis, SDP*
- Session Initiation Protocol (SIP)*. *See VoIP analysis, SIP*
- Sharkfest conference*, 8
- Sharpe, Richard*, 38
- Simple Mail Transfer Protocol (SMTP)*. *See SMTP analysis*
- Simple Network Management Protocol (SNMP)*. *See SNMP analysis*
- Sister Gerald, Head of Discipline*, xxix
- SLOCCount, value of Wireshark code*, 32
- SMB analysis*
 - filter for SMBv2 vulnerability, 785
 - object exporting, 47
 - SMB header Process ID High field, 784
 - SMBv2 protocol vulnerability, 784
 - SMBv2, Negotiate Protocol Request, 784
- SMTP analysis, 611–17*
 - 553 Invalid Recipient, 614
 - 554 Transaction Failed, 613
 - analyzing problems, 613
 - capture filter syntax, 616
 - common reply code list, 615
 - default port, 611
 - detecting a relay test, 613
 - display filter examples, 616
 - display filter syntax, 616
 - EHLO designation for mail extensions, 612
 - ESMTP mail extensions, 612
 - HELO designation, 612
 - MAIL FROM command, 612
 - overview, 611
 - packet structure, 614
 - RCPT TO command, 612
- SnagIt screen capture utility*, 511
- SNMP analysis*
 - default MIBs, 169
 - MIB dissection support, 169
 - SNMP MIB path setting, 169
- Spanning Tree Protocol (STP)*, 787

SSL/TLS analysis, 564–74

- analyzing communication, 568
- cipher suites, 565
- colors when following stream, 189
- decrypted stream, 286
- decryption example, 285–87, 574
- decryption with Wireshark, 174, 570
- display filter for, 557
- export SSL keys, 313
- follow stream example, 285
- handshake analysis, 565–69
- handshake display filter, 565
- HTTP preferences – SSL/TLS Ports, 563
- HTTPS port setting, 174
- overview, 564
- PhoneFactor files, 851
- port number, non-standard, 565
- preferences, 174
- random bytes, 565, 567
- RSA key configuration, 570
- RSA *keys* directory, 570
- stream index, 280
- TCP preferences affect on, 564
- TCP preferences effect on, 174
- vulnerability, 576, 732

statistics, 221–46

- basic overview of, 222
- BOOTP-DHCP, 67
- Collectd, 67
- compare, 67
- conversation list, 66
- conversations, 65, 226, 228
- destinations, 231
- DHCP, 536
- endpoint list, 66
- endpoints, 65
- Flow Graphs, 67
- HART-IP, 67
- HTTP, 236
- IO Graphs, 66
- IP addresses, 231
- menu overview, 64
- packet lengths, 65, 229
- Protocol Hierarchy, 65, 222
- "Data" designation in, 792
- missing protocols, 223
- overview, 222, 791
- using, 224

- protocol types, 232
- Sametime, 68
- service response time, 66
- settings, 171
- summary, 65
- WLAN, 237

Statistics menu, 64–69

- ANCP, 67
- BACnet, 67
- HTTP, 68
- IP Addresses, 68
- IP Destinations, 68
- IP Protocol Types, 68
- ONC-RPC programs, 68
- TCP stream graphs, 68
- UDP multicast streams, 68
- WLAN traffic, 69

Status Bar

- display filter information, 250
- dropped packet indication, 328, 787
- file information column, 41
- ignored packets, 48
- interpreting, 41
- packet information column, 42
- profile column, 42, 294
- selected field names, 259

Stevens graph, compared to tcptrace graph, 511

subset operators, 262, See also display filters

summary information

- comparing, 212
- overview, 210

Suricata, 111**switched network analysis**

- analyzing floods, 787
- forwarding of broadcasts, 107
- forwarding of broadcasts and multicasts, 16
- forwarding of multicasts, 107
- forwarding to unknown hardware
 - address, 107
- general forwarding behavior, 15–16
- network analysis issues, 107
- span example*, 114
- spanning VLANs, 114–15
- use of MAC address table, 15

T

TAP (Test Access Port), 108–12

- aggregating, 110
- delays during capture, 108
- fail open, 108
- full-duplex analysis, 108
- in-line, 108
- installation of, 109
- intelligent, 112
- link aggregation, 112
- non-aggregating, 109
- regenerating, 111
- viewing physical layer errors, 108

task offloading, 127, See also checksum errors

TCP analysis, 457–91

- ACK bit, 478
- ACK bit display filter, 252, 478
- ACK bit interpretation, 478
- ACK scan signatures, 749
- Acknowledgment Number field, 477
- Allow Subdissector to Reassemble TCP Streams setting, 483
- analysis flags, 212
 - tcp.analysis.duplicate_ack, graphing, 504
 - tcp.analysis.lost_segment, graphing, 504
 - tcp.analysis.retransmission, graphing, 504
- Analyze TCP Sequence Numbers setting, 485
- backoff algorithm, 467, 503
- Calculate Conversation Timestamps setting, 488
- Calculated Window Size field, 87
- capture filter based on flags, 141
- capture filter syntax, 482
- Checksum field, 479
- congestion window, 470
- Congestion Window Reduced (CWR) flag, 478
- connection problems, 473
- connection termination with FIN, 461
- conversations list for, 226
- Data Offset field, 477
- delayed ACKs, 464, 471
- Destination Port field, 477

- disable relative sequence numbers, 463
- display filter syntax, 482
- dissector file, 327
- End of Options List (EOL) option, 332, 480
- exporting and graphing analysis flags, 313
- failed connections, 473
- filtering on flag summary line, 479
- filtering on TCP-based problems, 326
- FIN bit, 478
- FIN bit display filter, 479
- FIN bit interpretation, 461, 479
- FIN scan signatures, 749
- Flags field, 478
- full connect scan signatures, 746
- graphing Duplicate ACKs, 66
- graphing window size issues, 511
- half-open scan signature, 744
- handshake problems, 474
- handshake process, 459
- Ignore TCP Timestamps setting, 487
- indications of firewall blocking, 460
- initial sequence number, 463
- invalid checksums, 251
- multiple handshake processes, 234
- Nagle algorithm, 471
- No Operation (NOP) option, 480
- Nonce field, 478
- null scan signatures, 747
- Options, 480
- overview, 342, 458
- packet loss analysis
 - cause of packet loss, 327
 - congestion window changes, 470
 - graphing, 504
 - locating the source of, 429
 - recovery process, 465
 - recovery without SACK, 706
 - Time-Sequence graph depiction of, 514
 - upstream or downstream, 706
- packet structure, 477
- port scans, 743
- preference settings recommendation, 173
- protocol settings, 483
- Push bit, 478
- Push bit display filter, 478
- Push bit interpretation, 478
- receive window, 470

- Relative Sequence Numbers and Window
 - Scaling setting, 463, 486
 - Reset bit, 478
 - Reset bit display filter, 479
 - Reset bit interpretation, 479
 - Retransmission Timeout (RTO) value, 467
 - retransmissions, 327, *See also* Expert Info
 - advanced IO Graphing, 504
 - IO Graphing, 498
 - Retransmission Timeout (RTO)
 - value, 327
 - three identical ACKs trigger, 465
 - Time-Sequence graph depiction of, 514
 - security evasion techniques, 797
 - security issues related to window size, 300
 - Selective ACK
 - left edge and right edge, 468
 - option during packet loss recovery, 481
 - SACK overview, 467
 - SACK Permitted option, 481
 - Sequence Number field, 477
 - sequence number randomization, 617
 - sequencing/acknowledgment process, 463
 - service refusals, 460
 - skipped sequence numbers, 465
 - sliding window, 470
 - Source Port field, 477
 - splicing, 797
 - SYN bit, 478
 - SYN bit display filter, 479
 - SYN bit interpretation, 479
 - SYN/ACK filter, 231
 - SYN/FIN coloring rule, 184
 - TCP Stream Index value, 477
 - TCP Timestamp option, 481
 - Throughput graph overview, 510
 - Time-Sequence graphing, 511, *See also*
 - graphing
 - traceroutes, 759
 - Track Number of Bytes in Flight issue, 487
 - traffic to watch, 798
 - Urgent bit, 478
 - Urgent bit display filter, 478
 - Urgent bit interpretation, 478
 - Urgent Pointer field, 479
 - Validate the TCP Checksum setting, 483
 - watch the TCP handshake, 331, 481
 - Window Scale (WSOPT) option, 480
 - window scaling calculation, 486
 - window scaling not calculated, 486
 - Window Size field, 162, 479
 - Window Size field display filter, 251, 479
 - window size small issue, 162
 - Window Zero condition, 711
 - xmas scan signatures, 748
 - Zero Window case study, 515
- TCP Ports Reused, 331**
- TCP/IP, 341–52**
- communications overview, 342
 - etc/services* file, 779
 - resolution process, 343
- Telephony menu, 70–71**
- RTP, 70
 - SIP, 70
 - VoIP calls, 71
- Text2pcap, 836–38**
- examples of, 838
 - overview, 836
 - syntax, 837
- throughput graphing, 510, *See also* graphing**
- time analysis**
- *REF* designation, 48
 - adding Time columns, 206
 - adjusting timestamps with Editcap, 832
 - comparing time settings, 203
 - date and time of day, 201, 203
 - delta time, 49
 - differences between two instances of
 - Wireshark, 109
 - how Wireshark applies timestamps, 200
 - nanosecond time resolution, 203
 - seconds since beginning of capture, 51, 202
 - seconds since Epoch, 201
 - seconds since previous captured
 - packet, 202
 - seconds since previous displayed
 - packet, 52, 202
 - setting a time reference, 206
 - setting the Time column value, 201
 - shifting trace file time with Capinfos, 507
 - time reference overview, 48
 - Time Shift, 699
 - time zones, exchanging trace files
 - across, 204

timestamp accuracy and resolution, 203
troubleshooting with time, 49

Time-Sequence graphing, 511, See also graphing

Tools menu, 72–73

Firewall ACL rules, 72
Lua, 73

trace files. See also Appendix A and end of chapters

on *www.pcapr.net*, 38
on *www.wiresharkbook.com*, 852–911

traffic shaping, definition of, 19

training

booking courses, xxxvi
Wireshark University, xxxvi

Transmission Control Protocol (TCP). See TCP analysis

Transport Layer Security (TLS). See SSL/TLS analysis

Trivial File Transfer Protocol (TFTP), 225, 791

troubleshooting

application faults, 10, *See also* application analysis
bottom-up method, 698
columns to set, 87
congestion, 711
dealing with intermittent problems, 315
elements of a troubleshooting profile, 297
example of, 6–8
filtering on delta times, 701
filtering on the arrival time, 700
filtering on time since reference or first packet, 701
finger pointing, 5
identifying unacceptable traffic, 783
important note, 713
misconfigurations, 708
name resolution faults, 712
needle in the haystack issue, 13, 104
overview, 698
packet loss, 706
prioritize problems, 503
redirections, 709
resolution process issues, 698
slow communication example, 703
slow processing times, 702

small payload sizes, 710

Step 1 - Plan, 6
Step 2 - Capture, 6
Step 3 - Analyze, 6
Step 4 - Repeat if Necessary, 7
symptoms of performance problems, 698
tasks for the network analyst, 9
using the Time column, 699

Tshark

define occurrence of a field, 819
examples of, 826
gather host names, 823
hosts file use, 818
memory requirements, 127
new -S for packet separator, 818
overview, 817
-P parameter to view packets, 818
protocol hierarchy statistics, 821
reports available (-G), 820
service response types, 825
statistics, 821
syntax, 817
two-pass analysis, 817
-W n save extra file information, 820

U

UDP analysis, 445–53

capture filter for VoIP traffic, 299
capture filter syntax, 451
checksum value 0x0000, 451
display filter syntax, 451
echo port, 761
overview, 342, 446
packet structure, 450
port fields, 450
port scans, 751
pseudo-header, 451
scan evidence, 448
traceroutes, 759

UltraVNC, remote capture option, 121

update list of packets in real time, 126

User Datagram Protocol (UDP). See UDP analysis

V

View menu, 51–56

- coloring rules, 55
- colorize conversations, 54
- displayed columns, 54
- name resolution, 53
- reload, 56
- show packet in a new window, 56
- time display format, 51

view packet counts without capturing, 58

VLAN analysis, 114–15

- overview, 18
- troubleshooting case study, 21
- viewing tags, 115
- VLAN tagging with 802.1Q, 18

VoIP analysis, 659–79

- 4xx—Client Error response, 668
- 5xx—Server Error response, 668
- 6xx—Global Failure, 668
- adjust the jitter buffer value for play back, 674
- analysis overview, 660
- analyzer placement, 660
- analyzing problems, 665
- bandwidth requirements, 664
- call setup process, 661
- capture filter syntax, 676
- capture SIP and RTP traffic, 299
- case study of quality issues, 243
- display filter examples, 676
- display filter syntax, 676
- display filter upper-case warning, 676
- DTMF filter, 676
- DTMF telephony events, 660
- excessive jitter, 666
- G.729 audio data compression, 667
- graph analysis, 71
- jitter, 666
- packet loss example, 665, 666
- play back example, 675
- RTCP
 - packet types, 673
 - port numbers, 660
- RTP
 - display filter, 299
 - not decoded, 661
 - not recognized by Wireshark, 70

- play back, 674
- player markers, 675
- port numbers, 660
- preferences, 174
- stream analysis, 666
- visible channels setting, 171
- SDP information in packets, 663
- secure VoIP traffic, 660
- signaling protocol purpose, 660
- SIP
 - assured forwarding, 396
 - colorizing response codes, 676
 - Commands, 667
 - default port 5060, 660
 - display filter, 299
 - Invite packet, 668
 - Response Codes, 668
 - statistics, 671
- troubleshooting case study, 677
- troubleshooting example, 385
- Wireshark dissectors for, 662

W

Walberg, Sean, 677

Warnicke, Ed, 38

websites, 90–91, 400–401

- ask.wireshark.org, 90–91
- bugs.wireshark.org/bugzilla, 32
- emergingthreats.net, 800
- ettercap.sourceforge.net, 731
- hecker.org/mozilla/eccn, 34
- isc.sans.org, 743
- multicastdns.org, 356
- netcat.sourceforge.net, 731
- openpacket.org, 92
- sectools.org, 731
- standards.ieee.org/about/get/, 622
- www.bdcon.net, 12
- www.chappellseminars.com, xxxvi
- www.chappellU.com, xxxvi
- www.cirt.net/nikto2, 731
- www.gtk.org, 36
- www.hping.org, 731
- www.htcia.org, 728
- www.iana.org, 91, 382, 400–401, 430, 434, 477, 533, 668

www.ietf.org, 91
www.insecure.org, 862
www.kismetwireless.net, 731
www.law.cornell.edu, 12
www.maxmind.com, 851
www.metageek.net/wiresharkbook, xxxiv, 117, 624
www.metasploit.com, 731
www.mibdepot.com, 169
www.nessus.org, 318, 731
www.netoptics.com, 112
www.netscantools.com, 726, 731
www.nmap.org, 360, 740, 767, 862
www.ntp.org, 119
www.oidview.com, 169
www.openinfosecfoundation.com, 801
www.openinfosecfoundation.org, 111
www.openwall.com/john, 731
www.oxid.it, 731
www.pcapr.net, 38
www.phonefactor.com, 573, 576, 732
www.postel.org/postel.html, 431
www.riverbed.com/us/products/cascade/airpcap.php, 35
www.securityfocus.com, 768
www.snort.org, 111, 731
www.tcpdump.org, 34, 91, 126, 731
www.techsmith.com, 313, 511
www.thc.org, 760
www.videolan.org, 279
www.vimeo.com/9329501, 30
www.winpcap.org, 34, 91
www.wirelesslanprofessionals.com, 643
www.wireshark.org, 91
www.wireshark.org/develop.html, xxxi
www.wiresharkbook.com, xxxi
www.wiresharktraining.com, xxxvi, 91

Weevely PHP backdoor, 802**whining**

bad movies, Jaws III, 125
 compare feature, 67
 ice skating, a horrible idea for geeks, 5
 Mom... Mom... Mom..., 466
 no life, a bad thing?, 36
 Statistics menu clutter, 67

Wide Area Network (WAN) optimization, 19**Win32 Rimecud Trojan, 802****Win32 Sykipot Trojan Backdoor, 802****Window Full, 331****Window Probe, 329, See also Expert Info****Window Update, 330, See also Expert Info****Window Zero, 329****WinPcap**

Monitor Mode not supported, 118
rpcapd.exe, remote capture tool, 121

wireless settings. See WLAN analysis**Wireshark 1.8 and later**

capture filters on multiple interfaces, 138
 coloring rules placement, 185
 create profile based on existing profile, 296
 DNS Transaction ID added to Info column, 363
 Expert Infos LEDs, 323
 Fast Retransmissions and Retransmissions listed under Notes, 323
 filter expression buttons, 51, 80, 170
 GeoIP IPv6 support, 168, 228
 ignore TCP Timestamps in Summary, 487
 pcap-ng format default, 163
 Rawshark -p to use packet header timestamps, 841
 Retransmissions moved to Notes, 322
 saving Decode As settings, 62
 simultaneous multiple adapter capture, 120
 -t in Dumpcap to use a separate thread per interface, 840
 TCP Stream Index value change, 477
 Time Shift feature, 699
 Tshark
 new -P for packet display, 818
 new -W n to save extra information to file, 820
 -S as a packet separator, 818
 two-pass analysis, 817
 use of *hosts* file, 818
 Window Update excluded from Bad TCP coloring rule, 55, 330

Wireshark Certified Network Analyst program, xxxv

Wireshark University, xxxvi, 91**Wireshark, general**

- 64-bit version issues, 169
- blog, 91
- Bug 2234 display filters when writing to file with Tshark, 817, 827
- bug reporting, 32–33
- bug tracker mailing list, 90
- colorfilters* file global settings, 156, *See also* coloring rules
- complementing products, 34
- core developers list, 32
- creation of, 30
- customized launch in Windows, 815
- customizing the title bar, 39
- developer commits mailing list, 90
- developers mailing list, 90
- development release, 31
- disabling the TCP/IP stack, 726
- DNS PTR queries, 725
- download the latest version, 30–31
- dropping packets, 125
- ethers* file, 166
- export regulations, 33
- folder locations, 156
- GIMP Toolkit (GTK+), 36, 39
- GNU General Public License, 30
- GUI elements, 39–42
- hosts* file, 781, 818
- installation defaults, 812
- interface hiding, 163
- interface not shown, 38
- libpcap time resolution, 203
- mailing lists, 90
- manuf* file
 - contents, 156
 - update overrides, 158
- new releases, announcement of, 90
- optimization techniques, 787
- performance issues, 164
- platforms supported, 30
- preferences, 50
- Q&A forum – ask.wireshark.org, 90
- run locally, 105
- saving preferences while updating, 158
- security tool ranking, 731

services file

- manually editing, 54, 156
- overview, 54, 156
- update overrides, 158

SNMP *smi-modules* file, 156

stable release and announcements, 31

Start Page

- Capture area, 38
- Capture Help area, 38
- Files area, 38
- Online area, 38

Subversion (SVN) number, 31

system requirements, 19

training, 91

U3 version, 106

updates, 8, 31

USB version, 106

User's Guide, 38

users mailing list, 90

version/capability information, 75

WinPcap time resolution, 203

Wireshark.exe syntax, 813

Wiretap Library, 35**wiretapping, 12, *See also* legal issues****WLAN analysis, 621–54**

- 802.11 frame example, 631
- 802.11n set up in 2.4 GHz band, 652
- A/V transmitter interference, 653
- adapter failed in promiscuous mode, 131
- address fields, 642
- AirPcap
 - adapter information, 627
 - Control Panel, 628
 - multi-channel aggregator driver, 627
- analysis overview, 117
- analysis using a native adapter, 118
- analysis using AirPcap adapters, 118
- analyzer placement, 624, 626
- analyzing signal strength, 623
- association, disassociation and reassociation, 636
- authentication/deauthentication, 636
- baseline of RF activity, 624
- beacon frames, 637
- beacons in an IO Graph, 637
- capture filter for beacon frames, 298

- capture filter syntax, 641
- capture setup options, 117–18, 627
- capturing probe response packets, 147
- CCMP (WPA2) overhead, 640
- control frames, 636, 638
- cordless phone interference, 652
- CSMA/CA, 622
- data frames, 636
- decryption
 - modes, 629
- disassociation frames display filter
 - example, 299
- display filter
 - examples, 641
 - syntax, 641
- exporting and graphing retransmissions, 313
- exporting beacon frames, 312
- Extensible Authorization Protocol (EAPOL) for decryption, 629
- filtering on disassociation frames, 299
- frame control types and subtypes, 642
- frame structure, 640
- frame types, 636, 644
- frequency/channel column, 299
- host capture syntax, 298
- interference from jammer, 653
- interference sources, 623
- management frames, 636
- monitor mode
 - connectivity loss, 118
 - overview, 117, 626
- overview of WLAN analysis, 622
- packet sizes, 636
- PPI
 - header example, 634
 - header information, 631
- probe frames, 637
- problems detected on wired network, 622
- profile example, 137
- promiscuous mode
 - overview, 626
 - setting problems, 626
- Radiotap
 - header example, 633
 - header information, 631
- receive signal strength column, 635
- Retry bit, 642
- RF interference examples, 625
- RF signal analysis, 623–25
- rfmon* mode, 626, *See also* Monitor Mode
- signal strength levels, 635
- spectrum analyzer, 623, 652–53, 850
- SSID display filter, 299
- traffic overview, 636
- traffic statistics, 69
- troubleshooting case study, 650
- variable length depending on the
 - encryption type, 640
- weak signal strength display filter
 - example, 299
- WEP
 - decryption, 629
 - overhead, 640
- WinPcap – no Monitor Mode support, 626
- wireless interface selection, 627
- Wireless Toolbar, 40, 82
- Wireless Toolbar not available in earlier versions, 51
- WPA (TKIP) overhead, 640
- WPA and WPA2
 - decryption, 629

Z

Zenmap, 757, See also Nmap analysis and use zero window condition. See Window Zero Zero Window Probe ACK, 329, See also Expert Info