

# 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    |
| <b>Chapter 1: The World of Network Analysis .....</b>                     | <b>1</b> |
| 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        |
| <b>Chapter 2: Introduction to Wireshark.....</b>                  | <b>29</b> |
| 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        |
| <b>Chapter 3: Capture Traffic.....</b>                           | <b>103</b> |
| 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        |
| <b>Chapter 4: Create and Apply Capture Filters .....</b>               | <b>135</b> |
| 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        |
| <b>Chapter 5: Define Global and Personal Preferences .....</b>         | <b>155</b> |
| 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        |
| <b>Chapter 6: Colorize Traffic.....</b>                           | <b>181</b> |
| 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        |
| <b>Chapter 7: Define Time Values and Interpret Summaries.....</b> | <b>199</b> |
| 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        |
| <b>Chapter 8: Interpret Basic Trace File Statistics.....</b>                      | <b>221</b> |
| 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        |
| <b>Chapter 9: Create and Apply Display Filters .....</b>                          | <b>249</b> |
| 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        |
| <b>Chapter 10: Follow Streams and Reassemble Data.....</b>         | <b>277</b> |
| 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        |
| <b>Chapter 11: Customize Wireshark Profiles.....</b>               | <b>293</b> |
| 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        |
| <b>Chapter 12: Annotate, Save, Export and Print Packets .....</b>         | <b>305</b> |
| 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        |
| <b>Chapter 13: Use Wireshark's Expert System.....</b>                     | <b>321</b> |
| Let Wireshark's Expert Information Guide You.....                         | 322        |
| Launch Expert Info Quickly .....  | 322        |
| Colorize Expert Info Elements .....                                       | 325        |
| Filter on TCP Expert Information Elements.....                            | 326        |
| Understand TCP Expert Information .....                                   | 327        |
| What Triggers TCP Retransmissions?.....                                   | 327        |
| What Triggers Previous Segment Lost? .....                                | 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        |



|  |            |
|--|------------|
| <b>Chapter 14: TCP/IP Analysis Overview .....</b>                          | <b>341</b> |
| 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        |
| <b>Chapter 15: Analyze Domain Name System (DNS) Traffic .....</b>          | <b>355</b> |
| 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        |
| <b>Chapter 16: Analyze Address Resolution Protocol (ARP) Traffic .....</b> | <b>375</b> |
| 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        |
| <b>Chapter 17: Analyze Internet Protocol (IPv4/IPv6) Traffic .....</b>   | <b>391</b> |
| 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        |
| <b>Chapter 18: Analyze Internet Control Message Protocol (ICMPv4/ICMPV6)</b> |            |
| <b>Traffic .....</b>   | <b>425</b> |
| 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        |
| <b>Chapter 19: Analyze User Datagram Protocol (UDP) Traffic .....</b>        | <b>445</b> |
| 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        |
| <b>Chapter 20: Analyze Transmission Control Protocol (TCP) Traffic .....</b> | <b>457</b> |
| 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        |
| <b>Chapter 21: Graph IO Rates and TCP Trends .....</b>                         | <b>495</b> |
| 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        |
| <b>Chapter 22: Analyze Dynamic Host Configuration Protocol (DHCPv4/DHCPv6)</b> |            |
| <b>Traffic.....</b>  | <b>525</b> |
| 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        |
| <b>Chapter 23: Analyze Hypertext Transfer Protocol (HTTP) Traffic .....</b> | <b>545</b> |
| 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        |

|   |            |
|---|------------|
| <b>Chapter 24: Analyze File Transfer Protocol (FTP) Traffic .....</b> | <b>581</b> |
| 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        |
| <b>Chapter 25: Analyze Email Traffic .....</b>                        | <b>603</b> |
| 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        |
| <b>Chapter 26: Introduction to 802.11 (WLAN) Analysis .....</b>       | <b>621</b> |
| 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        |
| <b>Chapter 27: Introduction to Voice over IP (VoIP) Analysis .....</b> | <b>659</b> |
| 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        |
| <b>Chapter 28: Baseline "Normal" Traffic Patterns .....</b>            | <b>683</b> |
| 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        |



|  |            |
|--|------------|
| <b>Chapter 29: Find the Top Causes of Performance Problems .....</b> | <b>697</b> |
| 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        |
| <br>   |            |
| <b>Chapter 30: Network Forensics Overview .....</b>                  | <b>723</b> |
| 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        |
| <br>   |            |
| <b>Chapter 31: Detect Scanning and Discovery Processes .....</b>     | <b>739</b> |
| 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        |
| <b>Chapter 32: Analyze Suspect Traffic .....</b>                  | <b>777</b> |
| 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        |
| <b>Chapter 33: Effective Use of Command-Line Tools.....</b> | <b>811</b> |
| 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        |

|  |            |
|--|------------|
| <b>Appendix A: Resources on the Book Website .....</b>         | <b>849</b> |
| 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        |
| <b>Index.....</b>  | <b>917</b> |