

# Inhaltsverzeichnis

	<b>Danksagungen</b> .....	13
	<b>Über dieses Buch</b> .....	15
	<b>Vorwort von Gerald Combs</b> .....	17
<b>0</b>	<b>Wichtige Bedienelemente und Datenfluss im Netzwerk</b> .....	19
0.1	Was Wireshark alles kann .....	20
0.1.1	Allgemeine Analyse .....	21
0.1.2	Fehlersuche .....	22
0.1.3	Sicherheitsprüfungen (Netzwerkforensik) .....	22
0.1.4	Programmanalyse .....	23
0.2	Die passende Wireshark-Version .....	23
0.3	Wie Wireshark Datenverkehr aufzeichnet .....	24
0.3.1	Das Mitschneiden beruht auf speziellen Treibern .....	25
0.3.2	dumpcap legt Abbruchbedingungen fest .....	26
0.3.3	Die Core Engine ist eine wahre Goldgrube .....	26
0.3.4	Grafische Benutzeroberfläche per Qt-Framework .....	26
0.3.5	Das GTK+-Toolkit wird ausgemustert .....	26
0.3.6	Zum Öffnen von Mittschnittdateien wird die Wiretap-Bibliothek verwendet .....	27
0.4	Eine beispielhafte Analysesitzung mit Wireshark .....	27
0.5	Der Unterschied zwischen Paket und Frame .....	28
0.5.1	Merkmale eines Frames .....	28
0.5.2	Merkmale eines Pakets .....	29
0.5.3	Merkmale eines Segments .....	29
0.6	Verfolgen eines HTTP-Pakets im Netzwerk .....	30
0.6.1	Punkt 1: Was wird beim Client angezeigt? .....	31
0.6.2	Punkt 2: Was wird jenseits des ersten Switches angezeigt? .....	32
0.6.3	Punkt 3: Was wird jenseits des Routers angezeigt? .....	32
0.6.4	Punkt 4: Was wird jenseits des NAT-Routers angezeigt? ...	33
0.6.5	Punkt 5: Was wird beim Server angezeigt? .....	34

0.6.6	Der Ort der Aufzeichnung ist von Bedeutung . . . . .	34
0.6.7	Obacht: Standardmäßige Weiterleitung eines Switches . . . .	34
0.7	Wireshark-Dokumentation und Ressourcen . . . . .	35
0.7.1	Nutzen Sie das Wireshark-Protokoll-Wiki! . . . . .	36
0.7.2	Auf ask.wireshark.org werden Ihre Fragen beantwortet . . . .	37
0.8	Analyse von Datenverkehr im Wireshark-Hauptfenster . . . . .	38
0.8.1	Öffnen einer Mitschnittdatei (aber bitte mit der Hauptwerkzeuggeste). . . . .	39
0.8.2	Machen Sie sich klar, wann die Werkzeuggeste verwendet werden muss. . . . .	40
0.8.3	Verwenden Sie die Werkzeuggeste, falls möglich . . . . .	41
0.8.4	Die Filterwerkzeuggeste meistern. . . . .	44
0.8.5	Zusammenfassung des Datenverkehrs in der Paketliste. . . .	44
0.8.6	Mehr zur Detailansicht der Pakete . . . . .	50
0.8.7	Mit der Byteansicht zum Nerd werden . . . . .	51
0.8.8	Beachten Sie die Statusleiste . . . . .	52
0.9	Analyse typischen Datenverkehrs. . . . .	60
0.9.1	Analyse des Datenverkehrs beim Websurfen. . . . .	61
0.9.2	Analyse des Hintergrundsrauschens . . . . .	63
0.10	Mitschnittdateien anderer Programme öffnen . . . . .	66
0.11	Aufgaben . . . . .	69
1	<b>Wiresharks Ansichten und Einstellungen anpassen. . . . .</b>	71
1.1	Spalten zur Paketliste hinzufügen . . . . .	72
1.1.1	Die einfache Methode: Rechtsklick. . . . .	72
1.1.2	Die komplizierte Methode: Einstellungen . . . . .	73
1.1.3	Spalten verbergen, entfernen, umordnen, ausrichten und bearbeiten . . . . .	74
1.1.4	Spalteninhalte sortieren . . . . .	75
1.1.5	Spalteninhalte exportieren. . . . .	76
1.2	Arbeitsweise der Wireshark-Dissektoren. . . . .	78
1.2.1	Der Frame-Dissektor . . . . .	78
1.2.2	Der Ethernet-Dissektor übernimmt . . . . .	79
1.2.3	Der IPv4-Dissektor macht weiter . . . . .	79
1.2.4	Der TCP-Dissektor fährt fort . . . . .	80
1.2.5	Der HTTP-Dissektor beendet den Vorgang . . . . .	80
1.3	Verarbeitung von Datenverkehr, der nicht über Standardports läuft. . . . .	81
1.3.1	Verwendung von Nicht-Standardportnummern . . . . .	81

1.3.2	Arbeitsweise heuristischer Dissektoren . . . . .	82
1.3.3	Verwendung eines Dissektors erzwingen . . . . .	82
1.3.4	Dissektoren anpassen (falls möglich) . . . . .	83
1.4	Darstellungsweise bestimmter Arten von Datenverkehr ändern. . . . .	84
1.4.1	Benutzerschnittstelle konfigurieren . . . . .	84
1.4.2	Mitschnitteinstellungen anpassen . . . . .	84
1.4.3	Definition von Filterausdrücken . . . . .	85
1.4.4	Namensauflösung konfigurieren . . . . .	85
1.4.5	Protokolle und Anwendungen konfigurieren . . . . .	86
1.5	Wireshark für verschiedene Aufgaben einrichten (Profile) . . . . .	92
1.5.1	Profile: Grundlagen . . . . .	92
1.5.2	Anlegen eines neuen Profils . . . . .	92
1.6	Speicherort der Wireshark-Konfigurationsdateien . . . . .	94
1.6.1	Das globale Konfigurationsverzeichnis . . . . .	95
1.6.2	Das persönliche Konfigurationsverzeichnis . . . . .	95
1.7	Spalten mit Zeitangaben zum Aufspüren von Latenzproblemen verwenden . . . . .	98
1.7.1	Pfadlatenz: Anzeichen und Ursachen. . . . .	98
1.7.2	Client-Latenz: Anzeichen und Ursachen . . . . .	99
1.7.3	Server-Latenz: Anzeichen und Ursachen . . . . .	100
1.7.4	Latenzprobleme durch Ändern der Einstellung für die Time-Spalte finden. . . . .	100
1.7.5	Latenzprobleme mittels TCP-Delta-Spalte lokalisieren. . . . .	102
1.7.6	Lassen Sie sich nicht täuschen: Manche Verzögerungen sind normal. . . . .	104
1.8	Aufgaben . . . . .	109
<b>2</b>	<b>Ermittlung des besten Aufzeichnungsverfahrens und Anwendung von Mitschnittfiltern . . . . .</b>	<b>111</b>
2.1	Der geeignetste Ort zur Aufzeichnung, um geringen Datendurchsatz zu beheben . . . . .	112
2.1.1	Der ideale Ausgangspunkt. . . . .	113
2.1.2	Wechseln Sie, falls nötig, den Standort . . . . .	113
2.2	Aufzeichnung des Datenverkehrs im Ethernet-Netzwerk . . . . .	114
2.3	Aufzeichnung des Datenverkehrs im drahtlosen Netzwerk. . . . .	115
2.3.1	Was können Sie mit dem WLAN-Adapter Ihres Systems beobachten? . . . . .	115
2.3.2	AirPcap-Adapter sorgen für vollständige WLAN-Sichtbarkeit . . . . .	116

2.3.3	Npcap-Treiber zur Erkennung von WLAN/Loopback verwenden . . . . .	116
2.4	Aktive Schnittstellen . . . . .	118
2.4.1	Welche Schnittstelle erkennt Datenverkehr? . . . . .	118
2.4.2	Verwendung mehrerer Schnittstellen. . . . .	118
2.5	Umgang mit großen Datenverkehrsaufkommen . . . . .	119
2.5.1	Warum beobachten Sie so viel Datenverkehr? . . . . .	119
2.5.2	Das beste Argument für die Verwendung von Mitschnittfiltern . . . . .	120
2.5.3	Aufzeichnen in einen Dateisatz. . . . .	120
2.5.4	Navigation in Dateisätzen . . . . .	121
2.5.5	Auch eine Möglichkeit: SteelCentral® Packet Analyzer. . . . .	121
2.6	Spezielle Aufzeichnungsverfahren zum Aufspüren unregelmäßig auftretender Probleme. . . . .	125
2.6.1	Dateisätze und der Ringpuffer. . . . .	125
2.6.2	Nach dem Auftreten des Problems abbrechen. . . . .	126
2.7	Menge des zu verarbeitenden Datenverkehrs begrenzen. . . . .	128
2.7.1	Wenn Wireshark ins Stocken gerät. . . . .	128
2.7.2	Wenn die Portspiegelung ins Stocken gerät. . . . .	129
2.7.3	Anwendung von Mitschnittfiltern. . . . .	130
2.8	Datenverkehr anhand der MAC- oder IP-Adresse aufzeichnen . . . . .	132
2.8.1	Ein- und ausgehenden Datenverkehr einer bestimmten IP-Adresse aufzeichnen . . . . .	132
2.8.2	Ein- und ausgehenden Datenverkehr eines IP-Adressbereichs aufzeichnen . . . . .	133
2.8.3	Datenverkehr zu Broadcast- oder Multicast-Adressen aufzeichnen. . . . .	133
2.8.4	Datenverkehr anhand der MAC-Adresse aufzeichnen . . . . .	134
2.9	Datenverkehr eines bestimmten Programms aufzeichnen . . . . .	138
2.9.1	Portnummern . . . . .	138
2.9.2	Kombination von Portfiltern . . . . .	139
2.10	ICMP-Datenverkehr aufzeichnen. . . . .	140
2.11	Aufgaben . . . . .	142
<b>3</b>	<b>Anwendung von Anzeigefiltern . . . . .</b>	<b>143</b>
3.1	Korrekte Syntax von Anzeigefiltern . . . . .	144
3.1.1	Die Syntax der einfachsten Anzeigefilter . . . . .	144
3.1.2	Syntaxprüfung bei Eingabe des Anzeigefilters . . . . .	146
3.1.3	Lernen Sie die Feldbezeichnungen kennen . . . . .	147

3.1.4	Automatische Vervollständigung bei Eingabe des Anzeigefilters . . . . .	148
3.1.5	Vergleichsoperatoren . . . . .	149
3.1.6	Verwendung von Filterausdrücken . . . . .	150
3.2	Bearbeiten und Verwenden der Standardanzeigefilter . . . . .	155
3.3	Korrekt nach HTTP-Datenverkehr filtern . . . . .	158
3.3.1	Test eines Anwendungsfilters, der TCP-Portnummern verwendet . . . . .	158
3.3.2	Vorsicht beim Filtern nach der Bezeichnung einer TCP-Anwendung . . . . .	159
3.4	Warum Ihr dhcp-Anzeigefilter nicht funktioniert . . . . .	162
3.5	Nach IP-Adresse, IP-Adressbereichen oder Subnetzen filtern . . . . .	163
3.5.1	Nach Datenverkehr eines einzelnen Computers filtern . . . . .	164
3.5.2	Nach Datenverkehr eines Adressbereichs filtern . . . . .	164
3.5.3	Nach Datenverkehr eines Subnetzes filtern . . . . .	165
3.6	Nach einem Feld in einem Paket filtern . . . . .	166
3.6.1	Flink filtern: Als Filter anwenden . . . . .	167
3.6.2	Kreativ filtern: Filter vorbereiten . . . . .	169
3.6.3	Verwenden der »...«-Filterergänzungen . . . . .	169
3.7	Nach TCP- oder UDP-Verbindungen filtern . . . . .	173
3.7.1	Nach einer Verbindung filtern . . . . .	174
3.7.2	Nachverfolgen eines Datenstroms . . . . .	175
3.7.3	Statistikfenster: Nach einer Verbindung filtern . . . . .	175
3.7.4	Nach einer TCP-Verbindung anhand der Indexnummer filtern . . . . .	176
3.8	Anzeigefilter mit mehreren Ausschluss- und Einbeziehungskriterien . . . . .	178
3.8.1	Logikoperatoren . . . . .	178
3.8.2	Warum Ihr Filter ip.addr != nicht funktioniert . . . . .	179
3.8.3	Warum Ihr Filter !tcp.flags.syn == 1 nicht funktioniert . . . . .	179
3.9	Verwendung von Klammern . . . . .	180
3.10	Warum wird das Eingabefeld für Anzeigefilter gelb? . . . . .	182
3.10.1	Roter Hintergrund: Syntaxprüfung ist fehlgeschlagen . . . . .	182
3.10.2	Grüner Hintergrund: Syntaxprüfung bestanden . . . . .	182
3.10.3	Gelber Hintergrund: Syntaxprüfung mit Warnung bestanden . . . . .	183
3.11	Nach Stichwörtern filtern . . . . .	183
3.11.1	Einfache Stichwortsuche in Frames mit contains . . . . .	183

3.11.2	Einfache Stichwortsuche in Datenfeldern mit contains . . . .	184
3.11.3	Groß-/Kleinschreibung bei der Stichwortsuche. . . . .	185
3.11.4	Mit matches mehrere Wörter suchen . . . . .	185
3.12	Jokerzeichen in Anzeigefiltern . . . . .	187
3.12.1	Reguläre Ausdrücke mit ».«. . . . .	187
3.12.2	Variable Anzahl wiederholter Jokerzeichen . . . . .	188
3.13	Filter verwenden, um verzögerte Pakete aufzuspüren . . . . .	189
3.13.1	Nach hohen Delta-Zeiten filtern (frame.time_delta) . . . . .	189
3.13.2	Nach hohen TCP-Delta-Zeiten filtern (tcp.time_delta) . . . . .	190
3.14	Anzeigefilter als Schaltflächen . . . . .	193
3.14.1	Erstellen von Filterknöpfen . . . . .	193
3.14.2	Bearbeiten, Umordnen, Löschen und Deaktivieren von Filterschaltflächen . . . . .	194
3.14.3	Filterausdrücke in der preferences-Datei bearbeiten . . . . .	194
3.15	Aufgaben . . . . .	198
4	<b>Einfärbung und Export interessanter Pakete.</b> . . . . .	199
4.1	Anzeige der angewendeten Einfärbungsregeln . . . . .	200
4.2	Einfärbungsregel für Prüfsummenfehler deaktivieren. . . . .	202
4.2.1	Einzelne Einfärbungsregeln deaktivieren. . . . .	202
4.2.2	Paketeinfärbung komplett deaktivieren . . . . .	203
4.3	Einfärbungsregel zum Hervorheben verzögerter Pakete . . . . .	204
4.3.1	Einfärbungsregel neu erstellen . . . . .	204
4.3.2	Einfärbungsregeln per Kontextmenü erstellen . . . . .	206
4.4	Einfärben einer einzelnen Verbindung . . . . .	208
4.4.1	Vorübergehendes Einfärben einer Verbindung per Kontextmenü. . . . .	208
4.4.2	Vorübergehende Einfärbung entfernen . . . . .	209
4.5	Verwendung der intelligenten Scrollleiste . . . . .	210
4.5.1	Manuelle Navigation in der intelligenten Scrollleiste . . . . .	211
4.5.2	Navigation mit dem Kontextmenü der intelligenten Scrollleiste . . . . .	211
4.6	Interessante Pakete exportieren . . . . .	214
4.7	Paketdetails exportieren. . . . .	217
4.7.1	Dekodierte Pakete exportieren. . . . .	217
4.7.2	Festlegen, was exportiert wird . . . . .	218
4.7.3	Beispiel einer Textausgabe . . . . .	219
4.7.4	Beispiel einer CSV-Ausgabe. . . . .	219
4.8	Aufgaben . . . . .	223

<b>5</b>	<b>Tabellen und Diagramme erstellen und auswerten</b> . . . . .	<b>225</b>
5.1	Herausfinden, wer mit wem im Netzwerk kommuniziert. . . . .	227
5.1.1	Verbindungen im Netzwerk untersuchen . . . . .	227
5.1.2	Nach Verbindungen filtern . . . . .	228
5.2	Auffinden der »geschwätzigsten« Rechner . . . . .	229
5.2.1	Sortieren nach Bandbreitennutzung von Verbindungen . . .	229
5.2.2	Sortieren nach Bandbreitennutzung einzelner Hosts. . . . .	230
5.3	Im Netzwerk sichtbare Programme anzeigen. . . . .	235
5.3.1	Anzeigen der Protokollhierarchie . . . . .	235
5.3.2	Aufgeführte Protokolle und Anwendungen filtern und einfärben. . . . .	235
5.3.3	Suche nach verdächtigen Protokollen, Anwendungen oder nicht erkannten Daten. . . . .	236
5.4	Bandbreitennutzung von Anwendungen und Hosts grafisch darstellen . . . . .	238
5.4.1	Datenverkehr vor der Diagrammerstellung exportieren . . .	238
5.4.2	Diagrammerstellung mit ip.addr . . . . .	239
5.4.3	Diagrammerstellung mit ip.src . . . . .	240
5.4.4	Diagrammerstellung mit tcp.port oder udp.port . . . . .	241
5.5	TCP-Fehler erkennen . . . . .	243
5.5.1	Verwenden der Schaltfläche zur Anzeige von Experten-Infos . . . . .	243
5.5.2	Schweregrad der Experten-Infos . . . . .	244
5.5.3	Nach Paketen mit TCP-Analyse-Flags filtern . . . . .	246
5.6	Fehlermeldungen im Experten-Infos-Fenster . . . . .	246
5.6.1	Paketverluste, Paketwiederherstellung und schadhafte Mitschnittdateien . . . . .	247
5.6.2	Asynchrone und mehrere Pfade . . . . .	248
5.6.3	Aufrechterhaltung von Verbindungen . . . . .	249
5.6.4	Überfüllter Empfangspuffer . . . . .	249
5.6.5	Wiederverwendung von TCP-Verbindungen . . . . .	250
5.6.6	Möglicherweise ein Routerproblem . . . . .	250
5.6.7	Fehlkonfiguration oder ARP-Poisoning . . . . .	251
5.7	Diagramme verschiedener Netzwerkfehler . . . . .	252
5.7.1	Diagramm sämtlicher TCP-Analyse-Flags (außer Window-Update) . . . . .	253
5.7.2	Diagramme einzelner TCP-Analyse-Flags . . . . .	254
5.8	Aufgaben . . . . .	257

<b>6</b>	<b>Datenverkehr rekonstruieren</b> .....	259
6.1	Browsersitzungen rekonstruieren .....	260
6.1.1	TCP-Datenströme nachverfolgen .....	260
6.1.2	Herausfiltern des Datenstroms, Suchen und Speichern ....	261
6.2	Rekonstruktion einer per FTP übertragenen Datei .....	263
6.3	Exportieren übertragener HTTP-Objekte .....	268
6.3.1	Überprüfen der TCP-Einstellungen .....	268
6.3.2	Anzeige sämtlicher HTTP-Objekte der Mitschnittdatei ....	269
6.4	Aufgaben .....	272
<b>7</b>	<b>Kommentare in Mitschnittdateien und Paketen</b> .....	273
7.1	Anmerkungen zur Mitschnittdatei .....	275
7.2	Paketkommentare hinzufügen .....	276
7.2.1	Speichern im .pcapng-Format .....	277
7.2.2	Hinzufügen einer Kommentarspalte .....	277
7.2.3	Erster Schritt: Nach Paketen mit Kommentaren filtern ....	280
7.2.4	Zweiter Schritt: Dekodierte Pakete exportieren .....	280
7.3	Aufgaben .....	284
<b>8</b>	<b>Kommandozeilenwerkzeuge</b> .....	285
8.1	Aufteilen einer großen Mitschnittdatei in einen Satz von Dateien .....	286
8.1.1	Wireshark-Programmverzeichnis zur Pfadvariablen hinzufügen .....	286
8.1.2	Mit capinfos Dateigröße und Paketzahl ermitteln .....	287
8.1.3	Aufteilen einer Mitschnittdatei anhand der Paketzahl ....	287
8.1.4	Aufteilen einer Mitschnittdatei anhand der verstrichenen Zeit .....	288
8.1.5	Verwendung von Dateisätzen .....	289
8.2	Mitschnittdateien zusammenführen .....	291
8.2.1	Vergewissern Sie sich, dass dem System Wiresharks Programmverzeichnis bekannt ist .....	292
8.2.2	mergcap und der Parameter -w .....	292
8.3	Paketerfassung auf der Kommandozeile .....	294
8.3.1	dumpcap oder tshark? .....	294
8.3.2	Paketerfassung mit dumpcap .....	294
8.3.3	Paketerfassung mit tshark .....	295
8.3.4	Host-Informationen speichern und Mitschnittdateien verwenden .....	296

8.4	Mitschnittfilter auf der Kommandozeile verwenden . . . . .	299
8.5	Anzeigefilter auf der Kommandozeile verwenden . . . . .	300
8.6	Exportieren von Datenfeldern und Statistiken einer Mitschnittdatei mit tshark. . . . .	302
8.6.1	Exportieren von Datenfeldern . . . . .	303
8.6.2	Exportieren von Statistiken . . . . .	304
8.6.3	Exportieren des Datenfelds http.host . . . . .	305
8.7	Mehr über Wireshark und die Analyse von Netzwerken erfahren . . . . .	307
8.8	Aufgaben . . . . .	308
<b>A</b>	<b>Lösungen zu den Aufgaben . . . . .</b>	<b>309</b>
<b>B</b>	<b>Beschreibung der Mitschnittdateien . . . . .</b>	<b>329</b>
<b>C</b>	<b>Glossar . . . . .</b>	<b>337</b>
	<b>Stichwortverzeichnis . . . . .</b>	<b>355</b>