

Inhaltsverzeichnis

Danksagungen	17
Über dieses Buch	19
Vorwort von Gerald Combs	21
o Wichtige Bedienelemente und Datenfluss im Netzwerk	23
o.1 Was Wireshark alles kann	24
o.1.1 Allgemeine Analyse	25
o.1.2 Fehlersuche	26
o.1.3 Sicherheitsprüfungen (Netzwerkforensik)	26
o.1.4 Programmanalyse	27
o.2 Die passende Wireshark-Version	27
o.3 Wie Wireshark Datenverkehr aufzeichnet	28
o.3.1 Der Aufzeichnungsvorgang beruht auf speziellen Treibern ..	29
o.3.2 dumbcap legt Abbruchbedingungen fest	30
o.3.3 Die Core Engine ist eine wahre Goldgrube	30
o.3.4 Grafische Benutzeroberfläche per GTK+	30
o.3.5 Zum Öffnen von Aufzeichnungsdateien wird die Wiretap-Bibliothek verwendet	30
o.4 Eine beispielhafte Analysesitzung mit Wireshark	31
o.5 Der Unterschied zwischen Paket und Frame	32
o.5.1 Merkmale eines Frames	32
o.5.2 Merkmale eines Pakets	33
o.6 Verfolgen eines HTTP-Pakets im Netzwerk	33
o.6.1 Punkt 1: Was wird beim Client angezeigt?	35
o.6.2 Punkt 2: Was wird jenseits des ersten Switches angezeigt? ..	35
o.6.3 Punkt 3: Was wird jenseits des Routers angezeigt?	36
o.6.4 Punkt 4: Was wird jenseits des NAT-Routers angezeigt? ..	37
o.6.5 Punkt 5: Was wird beim Server angezeigt?	38
o.6.6 Der Ort der Aufzeichnung ist von Bedeutung	38
o.6.7 Obacht: Standardmäßige Weiterleitung eines Switches ..	38

Inhaltsverzeichnis

o.7	Wireshark-Dokumentation und Ressourcen	39
o.7.1	Nutzen Sie das Wireshark-Protokoll-Wiki!	39
o.7.2	Auf ask.wireshark.org werden Ihre Fragen beantwortet	40
o.8	Analyse von Datenverkehr in Wiresharks Hauptfenster	42
o.8.1	Öffnen einer Aufzeichnungsdatei (aber bitte mit der Hauptwerkzeugeiste)	42
o.8.2	Machen Sie sich klar, wann das Hauptmenü verwendet werden muss	43
o.8.3	Verwenden Sie die Werkzeugeiste, falls möglich	44
o.8.4	Die Filterwerkzeugeiste meistern	45
o.8.5	Zusammenfassung des Datenverkehrs in der Liste der Pakete	45
o.8.6	Mehr zur Detailansicht der Pakete	50
o.8.7	Mit der Bytesicht zum Nerd werden	51
o.8.8	Beachten Sie die Statusleiste	52
o.8.9	Praktische Übung 1: Pakete verschaffen einen ersten Eindruck vom Netzwerk	53
o.9	Analyse typischen Datenverkehrs	59
o.9.1	Analyse des Datenverkehrs beim Websurfen	60
o.9.2	Analyse des Hintergrundrauschens	61
o.9.3	Praktische Übung 2: Aufzeichnen und Klassifizieren des Hintergrundrauschens	64
o.10	Aufzeichnungsdateien anderer Programme öffnen	65
o.10.1	Praktische Übung 3: Öffnen einer Netzwerkmonitor-Datei	67
o.11	Aufgaben	68
I	Wiresharks Ansichten und Einstellungen anpassen	69
I.1	Spalten zur Paketliste hinzufügen	70
I.I.1	Die einfache Methode: Rechtsklick	70
I.I.2	Die komplizierte Methode: Einstellungen	71
I.I.3	Spalten verbergen, entfernen, umordnen, ausrichten und bearbeiten	72
I.I.4	Spalteninhalte sortieren	73
I.I.5	Spalteninhalte exportieren	74
I.I.6	Praktische Übung 4: Das Datenfeld http.host als Spalte hinzufügen	74
I.2	Arbeitsweise der Wireshark-Dissektoren	76
I.2.1	Der Frame-Dissektor	76

I.2.2	Der Ethernet-Dissektor übernimmt	77
I.2.3	Der IPv4-Dissektor macht weiter	77
I.2.4	Der TCP-Dissektor fährt fort	78
I.2.5	Der HTTP-Dissektor beendet den Vorgang	78
I.3	Verarbeitung von Datenverkehr, der nicht über Standardports läuft	78
I.3.1	Portnummernzuweisung	79
I.3.2	Verwendung eines Dissektors erzwingen	79
I.3.3	Wenn die Portnummer nicht erkannt wird	80
I.3.4	Arbeitsweise heuristischer Dissektoren	80
I.3.5	Dissektoren anpassen (falls möglich)	80
I.3.6	Praktische Übung 5: Verwendung des HTTP-Dissektors für Datenverkehr auf Port 81	81
I.4	Darstellungsweise bestimmter Arten von Datenverkehr ändern	83
I.4.1	Benutzerschnittstelle konfigurieren	83
I.4.2	Namensauflösung konfigurieren	83
I.4.3	Definition von Filterausdrücken	84
I.4.4	Protokolle und Anwendungen konfigurieren	84
I.4.5	Praktische Übung 6: Wichtige Wireshark-Einstellungen konfigurieren	85
I.5	Wireshark für verschiedene Aufgaben einrichten (Profile)	89
I.5.1	Profile: Grundlagen	89
I.5.2	Anlegen eines neuen Profils	90
I.5.3	Praktische Übung 7: Ein neues Profil anhand des Standardprofils erstellen	90
I.6	Speicherort der Wireshark-Konfigurationsdateien	91
I.6.1	Das globale Konfigurationsverzeichnis	92
I.6.2	Das persönliche Konfigurationsverzeichnis	92
I.6.3	Praktische Übung 8: Importieren eines Profils	93
I.7	Spalten mit Zeitangaben zum Aufspüren von Latenzproblemen verwenden	95
I.7.1	Pfadlatenz: Anzeichen und Ursachen	96
I.7.2	Client-Latency: Anzeichen und Ursachen	97
I.7.3	Server-Latency: Anzeichen und Ursachen	97
I.7.4	Latenzprobleme durch Ändern der Einstellung für die Time-Spalte finden	98
I.7.5	Latenzprobleme mittels TCP-Delta-Spalte lokalisieren	99

1.7.6	Lassen Sie sich nicht täuschen: Manche der Verzögerungen sind normal	101
1.7.7	Praktische Übung 9: Pfad- und Server-Latenzen aufspüren	103
1.8	Aufgaben	106
2	Ermittlung des besten Aufzeichnungsverfahrens und Anwendung von Aufzeichnungsfilters	109
2.1	Der geeignete Ort zur Aufzeichnung, um geringen Datendurchsatz zu beheben	110
2.1.1	Der ideale Ausgangspunkt.....	110
2.1.2	Wechseln Sie, falls nötig, den Standort.....	111
2.2	Aufzeichnung des Datenverkehrs im Ethernet-Netzwerk	112
2.3	Aufzeichnung des Datenverkehrs im drahtlosen Netzwerk.....	113
2.3.1	Was können Sie mit dem WLAN-Adapter Ihres Systems beobachten?	113
2.3.2	AirPcap-Adapter sorgen für vollständige WLAN-Sichtbarkeit.....	114
2.4	Aktive Schnittstellen	115
2.4.1	Welche Schnittstelle erkennt Datenverkehr?	115
2.4.2	Verwendung mehrerer Schnittstellen.....	116
2.5	Umgang mit großen Datenverkehrsaufkommen	117
2.5.1	Warum beobachten Sie so viel Datenverkehr?	117
2.5.2	Das beste Argument für die Verwendung von Aufzeichnungsfilters	118
2.5.3	Aufzeichnen in einer Dateigruppe	118
2.5.4	Navigation in Dateigruppen.....	119
2.5.5	Auch eine Möglichkeit: Cascade Pilot®	119
2.5.6	Praktische Übung 10: Aufzeichnen in Dateigruppen	121
2.6	Spezielle Aufzeichnungsverfahren zum Aufspüren unregelmäßig auftretender Probleme	122
2.6.1	Dateigruppen im Rotationsverfahren	123
2.6.2	Nach dem Auftreten des Problems abbrechen.....	124
2.6.3	Praktische Übung 11: Aufzeichnen einer Dateigruppe im Rotationsverfahren spart Plattenplatz	124
2.7	Menge des zu verarbeitenden Datenverkehrs begrenzen.....	126
2.7.1	Wenn Wireshark ins Stocken gerät.....	126
2.7.2	Wenn die Portspiegelung ins Stocken gerät.....	127

2.7.3	Anwendung von Aufzeichnungsfilters	128
2.8	Datenverkehr anhand der MAC- oder IP-Adresse aufzeichnen	129
2.8.1	Ein- und ausgehenden Datenverkehr einer bestimmten IP-Adresse aufzeichnen	130
2.8.2	Ein- und ausgehenden Datenverkehr eines IP-Adressbereichs aufzeichnen.....	131
2.8.3	Datenverkehr zu Broadcast- oder Multicast-Adressen aufzeichnen.....	131
2.8.4	Datenverkehr anhand der MAC-Adresse aufzeichnen	132
2.8.5	Praktische Übung 12: Nur den Datenverkehr der eigenen IP-Adresse aufzeichnen.....	132
2.8.6	Praktische Übung 13: Den Datenverkehr aller MAC-Adressen außer der eigenen aufzeichnen	134
2.9	Datenverkehr,eines bestimmten Programms aufzeichnen	136
2.9.1	Portnummern.....	136
2.9.2	Kombination von Portfiltern	136
2.10	ICMP-Datenverkehr aufzeichnen.....	137
2.10.1	Praktische Übung 14: Erstellen, Speichern und Anwenden eines DNS-Aufzeichnungsfilters	138
2.11	Aufgaben	139
3	Anwendung von Anzeigefiltern	141
3.1	Korrekte Syntax von Anzeigefiltern	142
3.1.1	Die Syntax der einfachsten Anzeigefilter	142
3.1.2	Syntaxprüfung bei Eingabe des Anzeigefilters.....	145
3.1.3	Lernen Sie die Feldbezeichnungen kennen.....	145
3.1.4	Automatische Vervollständigung bei Eingabe des Anzeigefilters	146
3.1.5	Vergleichsoperatoren	147
3.1.6	Verwendung von Filterausdrücken.....	148
3.1.7	Praktische Übung 15: Datenverkehr eines HTTP-Servers per automatischer Vervollständigung finden.....	149
3.2	Bearbeiten und Verwenden der Standardanzeigefilter.....	153
3.2.1	Praktische Übung 16: Standardfilter als Vorlage für eigene Filter verwenden.....	155
3.3	Korrekt nach HTTP-Datenverkehr filtern	156

3.3.1	Test eines Anwendungsfilters, der TCP-Portnummern verwendet	157
3.3.2	Vorsicht beim Filtern nach der Bezeichnung einer TCP-Anwendung	158
3.3.3	Praktische Übung 17: Nach HTTP-Datenverkehr filtern....	159
3.4	Warum Ihr dhcp-Anzeigefilter nicht funktioniert.....	160
3.5	Nach IP-Adresse, IP-Adressbereichen oder Subnetzen filtern.....	161
3.5.1	Nach Datenverkehr eines einzelnen Computers filtern	161
3.5.2	Nach Datenverkehr eines Adressbereichs filtern.....	162
3.5.3	Nach Datenverkehr eines Subnetzes filtern	162
3.5.4	Praktische Übung 18: Nach Datenverkehr eines Subnetzes für Online-Backups filtern.....	162
3.6	Nach einem Feld in einem Paket filtern	163
3.6.1	Flink filtern: Als Filter anwenden	163
3.6.2	Kreativ filtern: Filter übernehmen.	165
3.6.3	Verwenden der »...«-Filterergänzungen	166
3.6.4	Praktische Übung 19: Nach DNS-Fehlern und HTTP-Statuscode 404 filtern.....	168
3.7	Nach TCP- oder UDP-Unterhaltungen filtern.....	169
3.7.1	Nach einer Unterhaltung filtern	170
3.7.2	Nachverfolgen eines Datenstroms.	170
3.7.3	Statistikfenster: Nach einer Unterhaltung filtern.....	171
3.7.4	Nach einer TCP-Unterhaltung anhand der Indexnummer filtern	172
3.7.5	Praktische Übung 20: Dateiübertragungen im Hintergrund aufspüren	173
3.8	Anzeigefilter mit mehreren Ausschluss- und Einbeziehungskriterien.....	174
3.8.1	Logische Operatoren.....	175
3.8.2	Warum Ihr Filter ip.addr != nicht funktioniert	175
3.8.3	Warum Ihr Filter !tcp.flags.syn == 1 nicht funktioniert.....	175
3.9	Verwendung von Klammern.....	176
3.9.1	Praktische Übung 21: TCP-Verbindungsversuche zu einem Client aufspüren	176
3.10	Warum wird das Eingabefeld für Anzeigefilter gelb?	178
3.10.1	Roter Hintergrund: Syntaxprüfung ist fehlgeschlagen	178
3.10.2	Grüner Hintergrund: Syntaxprüfung bestanden.....	179

3.10.3	Gelber Hintergrund: Syntaxprüfung mit Warnung bestanden	179
3.11	Nach Stichwörtern filtern	179
3.11.1	Einfache Stichwortsuche in Frames mit contains	180
3.11.2	Einfache Stichwortsuche in Datenfeldern mit contains	180
3.11.3	Groß-/Kleinschreibung bei der Stichwortsuche	180
3.11.4	Mit matches mehrere Wörter suchen	181
3.11.5	Praktische Übung 22: Stichwortsuche in einer Aufzeichnungsdatei	182
3.12	Jokerzeichen in Anzeigefiltern	183
3.12.1	Reguläre Ausdrücke mit »«	183
3.12.2	Variable Anzahl wiederholter Jokerzeichen	183
3.12.3	Praktische Übung 23: Jokerzeichen zwischen Stichwörtern	184
3.13	Filter verwenden, um verzögerte Pakete aufzuspüren	185
3.13.1	Nach hohen Delta-Zeiten filtern (frame.time_delta)	185
3.13.2	Nach hohen TCP-Delta-Zeiten filtern (tcp.time_delta)	185
3.13.3	Praktische Übung 24: Anzeigefilter importieren	186
3.14	Anzeigefilter als Schaltflächen	188
3.14.1	Erstellen von Filterschaltflächen	188
3.14.2	Bearbeiten, Umordnen, Löschen und Deaktivieren von Filterschaltflächen	189
3.14.3	Filterschaltflächen in der preferences-Datei bearbeiten	190
3.15	Praktische Übung 25: Erstellen und Importieren von HTTP-Filterschaltflächen	191
3.16	Aufgaben	193
4	Einfärbung und Export interessanter Pakete	195
4.1	Anzeige der angewendeten Einfärbungsregeln	196
4.1.1	Praktische Übung 26: Hinzufügen einer Einfärbungsregel-Spalte	197
4.2	Einfärbungsregel für Prüfsummenfehler deaktivieren	199
4.2.1	Einzelne Einfärbungsregeln deaktivieren	199
4.2.2	Paketeinfärbung komplett deaktivieren	200
4.3	Einfärbungsregel zum Hervorheben verzögerter Pakete	200
4.3.1	Einfärbungsregel neu erstellen	200
4.3.2	Einfärbungsregeln per Kontextmenü	202
4.3.3	Praktische Übung 27: Einfärbungsregel zum Hervorheben von FTP-Benutzernamen, Kennwörtern usw.	203

4.4	Einfärben einer einzelnen Unterhaltung	205
4.4.1	Vorübergehendes Einfärben einer Unterhaltung per Kontextmenü	205
4.4.2	Vorübergehende Einfärbung entfernen	207
4.4.3	Praktische Übung 28: Vorübergehende Einfärbungsregeln erstellen	207
4.5	Interessante Pakete exportieren	208
4.5.1	Praktische Übung 29: Export einer einzelnen TCP-Unterhaltung	209
4.6	Paketdetails exportieren	211
4.6.1	Dekodierte Pakete exportieren	211
4.6.2	Festlegen, was exportiert wird	212
4.6.3	Beispiel einer Textausgabe	212
4.6.4	Beispiel einer CSV-Ausgabe	213
4.6.5	Praktische Übung 30: Exportieren der Werte einer hinzugefügten Spalte	214
4.7	Aufgaben	217
5	Tabellen und Diagramme erstellen und auswerten	219
5.1	Herausfinden, wer im Netzwerk mit wem kommuniziert	220
5.1.1	Unterhaltungen im Netzwerk untersuchen	221
5.1.2	Nach Unterhaltungen filtern	222
5.2	Auffinden der »geschwätzigen« Rechner	223
5.2.1	Sortieren nach Bandbreitennutzung von Unterhaltungen	223
5.2.2	Sortieren nach Bandbreitennutzung einzelner Hosts	224
5.2.3	Praktische Übung 31: Nach der aktivsten TCP-Unterhaltung filtern	225
5.2.4	Praktische Übung 32: GeoIP einrichten	227
5.3	Im Netzwerk sichtbare Programme anzeigen	229
5.3.1	Anzeigen der Protokollhierarchie	229
5.3.2	Aufgeführte Protokolle und Anwendungen	230
5.3.3	Suche nach verdächtigen Protokollen, Anwendungen oder unerkannten Daten	230
5.3.4	Entschlüsseln der Prozentwerte in der Protokollhierarchie	231
5.3.5	Praktische Übung 33: Verdächtige Protokolle und Anwendungen aufspüren	233
5.4	Bandbreitennutzung von Anwendungen und Hosts grafisch darstellen	234

5.4.1	Datenverkehr vor der Diagrammerstellung exportieren	234
5.4.2	Diagrammerstellung mit ip.addr	236
5.4.3	Diagrammerstellung mit ip.src	237
5.4.4	Diagrammerstellung mit tcp.port oder udp.port	237
5.4.5	Praktische Übung 34: Vergleich des Datenverkehrs eines Subnetzes mit dem übrigen Datenverkehr	239
5.5	TCP-Fehler erkennen	240
5.5.1	Verwenden der Schaltfläche zur Anzeige von Experten-Infos	240
5.5.2	Nicht rekonstruierte Pakete	240
5.5.3	Nach Paketen mit TCP-Analyse-Flags filtern	241
5.6	Fehlermeldungen im Experten-Infos-Fenster	242
5.6.1	Paketverluste, Paketwiederherstellung und schadhafte Aufzeichnungsdateien	242
5.6.2	Asynchrone und mehrere Pfade	243
5.6.3	Aufrechterhaltung von Verbindungen	244
5.6.4	Überfüllter Empfangspuffer	244
5.6.5	Wiederverwendung von TCP-Verbindungen	245
5.6.6	Möglicherweise ein Routerproblem	245
5.6.7	Fehlkonfiguration oder ARP-Poisoning	246
5.6.8	Praktische Übung 35: Erkennen eines überlasteten Clients	246
5.7	Diagramme verschiedener Netzwerkfehler	247
5.7.1	Diagramm sämtlicher TCP-Analyse-Flags (außer Window-Update)	248
5.7.2	Diagramme einzelner TCP-Analyse-Flags	249
5.7.3	Praktische Übung 36: Diagramm von Problemen bei der Dateiübertragung	249
5.8	Aufgaben	252
6	Datenverkehr rekonstruieren	253
6.1	Browsersitzungen rekonstruieren	254
6.1.1	TCP-Datenströme nachverfolgen	254
6.1.2	Herausfiltern des Datenstroms, Suchen und Speichern	255
6.1.3	Praktische Übung 37: Per Rekonstruktion versteckte HTTP-Botschaften entdecken	256
6.2	Rekonstruktion einer per FTP übertragenen Datei	257
6.2.1	Praktische Übung 38: Eine Datei aus einer FTP-Datenübertragung extrahieren	259

6.3	Exportieren übertragener HTTP-Objekte	261
6.3.1	Überprüfen der TCP-Einstellungen	261
6.3.2	Anzeige sämtlicher HTTP-Objekte der Aufzeichnungsdatei ..	262
6.3.3	Praktische Übung 39: Ein HTTP-Objekt aus einer Browsersitzung extrahieren	263
6.4	Aufgaben	265
7	Kommentare in Aufzeichnungsdateien und Paketen	267
7.1	Anmerkungen zur Aufzeichnungsdatei	268
7.2	Paketkommentare hinzufügen	269
7.2.1	Speichern im .pcapng-Format	270
7.2.2	Hinzufügen einer Kommentarspalte	270
7.2.3	Praktische Übung 40: Anzeige der Paketkommentare einer bösartigen Weiterleitung	271
7.3	Paketkommentare für einen Bericht exportieren	272
7.3.1	Erster Schritt: Nach Paketen mit Kommentaren filtern ..	272
7.3.2	Zweiter Schritt: Dekodierte Pakete exportieren	273
7.3.3	Praktische Übung 41: Paketkommentare einer bösartigen Weiterleitung exportieren	275
7.4	Aufgaben	277
8	Kommandozeilenwerkzeuge	279
8.1	Aufteilen einer großen Aufzeichnungsdatei in eine Gruppe von Dateien	280
8.1.1	Wireshark-Programmverzeichnis zur Pfadvariablen hinzufügen	280
8.1.2	Mit capinfos Dateigröße und Paketzahl ermitteln	281
8.1.3	Aufteilen einer Aufzeichnungsdatei anhand der Paketzahl ..	281
8.1.4	Aufteilen einer Aufzeichnungsdatei anhand der verstrichenen Zeit	282
8.1.5	Verwendung von Dateigruppen	283
8.1.6	Praktische Übung 42: Aufteilen einer Datei und Verwendung gefilterter Dateigruppen	283
8.2	Aufzeichnungsdateien zusammenführen	286
8.2.1	Vergewissern Sie sich, dass dem System Wiresharks Programmverzeichnis bekannt ist	286
8.2.2	mergecap und der Parameter -w	286
8.2.3	Praktische Übung 43: Verwendung von Jokerzeichen beim Zusammenführen von Dateien	287
8.3	Paketerfassung auf der Kommandozeile	288

8.3.1	dumpcap oder tshark?	289
8.3.2	Paketerfassung mit dumpcap	289
8.3.3	Paketerfassung mit tshark	290
8.3.4	Host-Informationen speichern und Aufzeichnungsdateien verwenden	290
8.3.5	Praktische Übung 44: Paketerfassung mit tshark und einer Abbruchbedingung	291
8.4	Aufzeichnungsfilter auf der Kommandozeile verwenden	294
8.5	Anzeigefilter auf der Kommandozeile verwenden	295
8.5.1	Praktische Übung 45: Mit tshark HTTP-GET-Anfragen extrahieren	296
8.6	Exportieren von Datenfeldern und Statistiken einer Aufzeichnungsdatei mit tshark	297
8.6.1	Exportieren von Datenfeldern	297
8.6.2	Exportieren von Statistiken	298
8.6.3	Exportieren des Datenfelds http.host	300
8.6.4	Praktische Übung 46: Mit tshark HTTP-Hostnamen und IP-Adressen extrahieren	300
8.7	Mehr über Wireshark und die Analyse von Netzwerken erfahren	301
8.8	Aufgaben	302
A	Lösungen zu den Aufgaben	303
A.1	Lösungen der Aufgaben aus Kapitel 0	303
A.2	Lösungen der Aufgaben aus Kapitel 1	305
A.3	Lösungen der Aufgaben aus Kapitel 2	308
A.4	Lösungen der Aufgaben aus Kapitel 3	309
A.5	Lösungen der Aufgaben aus Kapitel 4	311
A.6	Lösungen der Aufgaben aus Kapitel 5	313
A.7	Lösungen der Aufgaben aus Kapitel 6	316
A.8	Lösungen der Aufgaben aus Kapitel 7	317
A.9	Lösungen der Aufgaben aus Kapitel 8	319
B	Beschreibung der Aufzeichnungsdateien	321
C	Glossar	329
	Stichwortverzeichnis	347