

Inhaltsverzeichnis

Vorwort	9
1 Grundlagen	11
1.1 Wie arbeiten Sniffer?.....	11
1.2 Rechtliche Grundlagen.....	12
1.3 Ein Schnellstart	13
1.4 Referenzmodelle	14
1.5 Adressen im Netzwerk.....	17
1.6 Netzwerkgeräte.....	18
1.6.1 Layer 1	18
1.6.2 Layer 2	19
1.6.3 Layer 3	20
1.7 Verkabelung.....	20
2 Bedienung	23
2.1 Das Hauptfenster	23
2.2 Navigation im Hauptfenster	27
2.3 Die Werkzeugleiste.....	27
2.4 Die Filterleiste.....	28
2.5 Die Statuszeile	29
2.6 Kontextmenüs	29
3 Erste Netzwerkanalyse	33

3.1	Erste Schritte	34
3.2	Filterung	35
3.3	Erste Analyse: ping	36
3.4	Webseitenaufruf mit einem Browser	38
3.5	Hypertext-Transfer Protocol (HTTP).....	39
3.6	Transport Control Protocol (TCP).....	41
3.6.1	TCP-Verbindungsaufbau	43
3.6.2	TCP-Datenaustausch	44
3.6.3	TCP-Verbindungsabbau	46
3.6.4	TCP FlowGraph	46
3.7	Internet Protocol (IP).....	47
3.8	Ethernet.....	48
3.9	Protokollfluss.....	49
3.10	Zeitmessung.....	49
3.11	Aufruf einer Standardseite.....	51
3.12	Datenverkehr im Ruhezustand	52
4	Filter	53
4.1	Display- oder Anzeigefilter	54
4.1.1	Filtern auf Layer 2 (Ethernet-Adressen)	56
4.1.2	Filtern auf Layer 3 (IP-Adressen).....	57
4.1.3	Filtern auf Layer 4 (Ports).....	58
4.1.4	Weitere Anzeigefilter	58
4.1.5	Filtern auf Bits und Bytes.....	59
4.1.6	Filterbutton erstellen	61
4.2	Capture- oder Aufzeichnungsfiler	62
4.2.1	Capture-Filter auf Layer 2 (MAC-Adressen)	65
4.2.2	Capture-Filter auf Layer 3 (IP-Adressen).....	65
4.2.3	Capture-Filter auf Layer 4 (Ports).....	66
4.2.4	Sonstige Capture-Filtereinstellungen.....	66

4.2.5	Kombinierte Capture-Filterausdrücke	67
5	Fortgeschrittene Analyse	69
5.1	Gespeicherte Mitschnitte öffnen.....	69
5.2	Pakete suchen/finden.....	70
5.3	Vergessene Passwörter ermitteln.....	72
5.4	Ungewöhnliche Verbindungen entdecken.....	72
5.5	Zeitmessung	73
5.6	Experteninfo	74
5.7	Dem Datenstrom folgen (Follow TCP Stream)	75
5.8	Statistics	77
5.8.1	Summary	77
5.8.2	Protocol Hierarchy	78
5.8.3	Conversations und Endpoints	79
5.8.4	Packet Length	82
5.9	Landkarte der IP-Adressen.....	82
5.10	Objekte extrahieren.....	85
6	Anpassen von Wireshark	87
6.1	Profile	87
6.2	Preferences	89
6.2.1	Layouts	89
6.2.2	Hinzufügen und Ändern von Spalten im Paketfenster ...	90
6.2.3	Capture-Einstellungen	92
6.2.4	Namensauflösung	92
6.2.5	Protokolle anzeigen	93
6.3	Aufzeichnung	94
7	Aus der Praxis	97
7.1	DNS-Fehler	97
7.2	IP-Analyse	98

7.2.1	Fehlerhafte IP-Konfiguration	99
7.2.2	Dynamic Host Configuration Protocol (DHCP)	100
7.3	Web-Probleme	102
7.3.1	HTTP-Requests	103
7.4	TCP-Analyse	104
7.4.1	Kein Verbindungsaufbau	104
7.4.2	TCP-Antwortzeiten	104
7.4.3	Fehlende TCP-Segmente (Lost Segments)	106
7.4.4	Delayed Acknowledgements	108
7.4.5	Zero Window	108
7.5	Protokollauflösung ein-/ausschalten	109
7.6	Top Talker finden	111
7.7	Experteninfo	111
7.8	Langzeitaufnahmen	112
7.9	Graphiken	113
8	WLAN-Sniffing	115
8.1	Physikalische Grenzen	115
8.2	Vorbereitung	117
8.3	Filtereinstellungen bei WLAN	118
8.4	Weitere Hilfsmittel	119
9	Platzieren des Sniffers	123
9.1	Port-Spiegelung (SPAN)	124
9.2	Remote-SPAN	125
9.3	Hub einschleifen	126
9.4	TAP einschleifen	127
9.5	Sniffing-PC als Bridge	128
9.6	SPAN out of the box (SOB)	129
9.7	Geräte sniffen selbst	130

9.7.1	FRITZ!Box	130
9.7.2	Cisco	131
9.7.3	TK-Anlagen	131
9.8	Sniffing bei virtuellen Maschinen.....	132
9.8.1	VirtualBox	133
9.8.2	VMWare.....	134
9.9	Ungewöhnliche Sniffing-Methoden.....	134
9.9.1	MAC-Flooding	135
9.9.2	Speziallösung Address-Spoofing	136
9.9.3	Netzstruktur ändern.....	137
I	Anhang	139
A	Installation von Wireshark	141
A.1	Windows	141
A.2	Ubuntu.....	142
A.3	Linux-Installation aus dem Quellcode	144
A.4	Smartphones.....	144
B	Tastenkombinationen	145
	Index	147