

Inhaltsverzeichnis

Vorwort	3
1 Grundlagen	9
1.1 Wie arbeiten Sniffer?	9
1.2 Rechtliche Grundlagen	9
1.3 Ein Schnellstart	10
1.4 Die notwendige Theorie	11
1.4.1 Referenzmodelle	11
1.4.2 Adressen im Netzwerk	14
1.4.3 Netzwerkgeräte	14
1.4.4 Verkabelung	16
2 Bedienung	19
2.1 Startbildschirm und Hauptfenster	19
2.2 Navigation im Hauptfenster	23
2.3 Sprache einstellen	23
2.4 Die Werkzeugleiste	25
2.5 Die Filterleiste	25
2.6 Die Statuszeile	26
2.7 Kontextmenüs	26
2.8 Der intelligente Scrollbalken	28
3 Erste Netzwerkanalyse	29
3.1 Erste Schritte	30
3.2 Filterung	32
3.3 Erste Analyse: ping	32
3.4 Webseitenaufruf mit einem Browser	34
3.5 HypertextTransfer Protocol (HTTP)	34
3.6 Transport Control Protocol (TCP)	36
3.6.1 TCP-Verbindungsaufbau	38
3.6.2 TCP-Datenaustausch	39
3.6.3 TCP-Verbindungsabbau	40
3.6.4 TCP FlowGraph	41
3.7 Internet Protocol (IP)	43
3.8 Ethernet	44
3.9 Protokollfluss	44

3.10	Zeitmessung	45
3.11	Aufruf einer Standardseite	46
3.12	Datenverkehr im Ruhezustand	47
4	Fortgeschrittene Analyse	49
4.1	Mitschnitt speichern/exportieren	49
4.2	Gespeicherte Mitschnitte öffnen	49
4.3	Pakete suchen/finden	50
4.4	Vergessene Passwörter ermitteln	52
4.5	Ungewöhnliche Verbindungen entdecken	53
4.6	Zeitmessung	53
4.7	Kommentare einfügen	54
4.8	Die Statuszeile	55
4.9	Experteninfo	55
4.10	Dem Datenstrom folgen (Follow TCP Stream)	57
4.11	Statistics	59
4.11.1	Capture File Properties	60
4.11.2	Protocol Hierarchy	61
4.11.3	Conversations und Endpoints	61
4.11.4	Packet Length	64
4.12	Landkarte der IP-Adressen	64
4.13	Objekte extrahieren	68
4.14	Grafische Ausgaben	68
4.14.1	IO-Graph	68
4.14.2	Datenstrom verfolgen	70
4.14.3	Stream-Graph	72
5	Filter	77
5.1	Display- oder Anzeigefilter	78
5.1.1	Filtern auf Layer 2 (Ethernet-Adressen)	80
5.1.2	Filtern auf Layer 3 (IP-Adressen)	80
5.1.3	Filtern auf Layer 4 (Ports)	81
5.1.4	Weitere Anzeigefilter	81
5.1.5	Nach Zeichenketten filtern	82
5.1.6	Filter über die Kontext-Menüs erstellen	82
5.1.7	Konversationsfilter	83
5.1.8	Filtern auf Bits und Bytes	84
5.1.9	Filterausdrücke verwalten	85
5.1.10	Filterbutton erstellen	86
5.2	Capture- oder Aufzeichnungsfilters	86
5.2.1	Capture-Filter auf Layer 2 (MAC-Adressen)	89
5.2.2	Capture-Filter auf Layer 3 (IP-Adressen)	89
5.2.3	Capture-Filter auf Layer 4 (Ports)	89
5.2.4	Sonstige Capture-Filtereinstellungen	89
5.2.5	Kombinierte Capture-Filterausdrücke	90
6	Konfiguration von Wireshark	91
6.1	Profile	91
6.2	Preferences	93
6.2.1	Layout (Preferences)	94
6.2.2	Hinzufügen und Ändern von Spalten im Paketfenster (Preferences)	94
6.2.3	Capture-Einstellungen (Preferences)	96

6.2.4	Protokolle anzeigen (Preferences)	96
6.3	Namens- und Adressauflösung	97
6.3.1	Grundeinstellungen	98
6.3.2	Manuelle Adressauflösung	98
6.4	Aufzeichnungsoptionen, Capture Interfaces	99
6.4.1	Aufzeichnungsoptionen, Capture Interfaces Input	99
6.4.2	Aufzeichnungsoptionen, Capture Interfaces Output	101
6.4.3	Aufzeichnungsoptionen, Capture Interfaces Options	101
6.5	Einfärberegeln	102
7	Aus der Praxis	103
7.1	DNS-Fehler	103
7.2	IP-Analyse	104
7.2.1	Fehlerhafte IP-Konfiguration	104
7.2.2	ARP-Nachfolger Neighbor Discovery Protocol NDP	105
7.2.3	Dynamic Host Configuration Protocol (DHCP)	105
7.2.4	DHCPv6	107
7.3	IPv6-Display-Filter	107
7.4	Web-Probleme	108
7.4.1	HTTP-Requests	110
7.5	TCP-Analyse	110
7.5.1	Fehlender Verbindungsaufbau	110
7.5.2	TCP-Antwortzeiten	111
7.5.3	Fehlende TCP-Segmente (Lost Segments)	113
7.5.4	Delayed Acknowledgements	114
7.5.5	Zero Window	114
7.6	Protokollauflösung ein-/ausschalten	115
7.7	Top Talker finden	117
7.8	Experteninfo	117
7.9	Langzeitaufnahmen	118
7.10	Online-Tools	120
7.11	Firewall-Regeln erstellen	121
8	WLAN-Sniffing	123
8.1	Physikalische Grenzen	123
8.2	Vorbereitung	124
8.3	Filtereinstellungen bei WLAN	126
8.4	Verschlüsseltes WLAN	127
8.5	Weitere Hilfsmittel	127
9	Platzieren des Sniffers	131
9.1	Port-Spiegelung (SPAN)	131
9.2	Remote-SPAN	132
9.3	Hub einschleifen	133
9.4	TAP einschleifen	134
9.5	Sniffing-PC als Bridge	135
9.6	SPAN out of the box (SOB)	136
9.7	Sicheres Arbeiten	136
9.8	Geräte sniffen selbst	137
9.8.1	FRITZ!Box	137
9.8.2	Cisco	137
9.8.3	TK-Anlagen	138

9.9	Sniffing bei virtuellen Maschinen	139
9.9.1	VirtualBox	139
9.9.2	VMWare	140
9.10	Ungewöhnliche Sniffing-Methoden	140
9.10.1	MAC-Flooding	140
9.10.2	Speziallösung Address-Spoofing	141
9.10.3	Netzstruktur ändern	142
10	Installation von Wireshark	145
10.1	Windows	145
10.2	Ubuntu	146
10.3	Linux-Installation aus den Paketquellen	148
10.4	Linux-Installation aus dem Quellcode	148
10.5	Smartphones	148
11	Tastenkombinationen	151
Index		152