

Inhaltsverzeichnis

1	Grundlagen	9
1.1	Was ist Wireshark und was nicht?	9
1.2	Unterschied zwischen Paket-Sniffer und Protokollanalysator	9
1.3	Wozu wird ein Protokollanalysator eingesetzt?	10
1.4	Auf welchen Geräten kann Wireshark installiert werden?	10
1.5	Rechtliche Grundlagen	11
1.6	Wie arbeiten Protokollanalysatoren?	12
1.7	Installation	12
1.7.1	Installation auf Windows-Rechnern	13
1.7.2	Installation auf Linux-Rechnern	14
1.7.3	Installation auf MAC-Rechnern	15
1.8	Ein Schnellstart	15
1.9	Die notwendige Theorie	16
1.9.1	Referenzmodelle ISO/OSI und TCP/IP	16
1.9.2	Netzwerkadressen und Netzwerkgeräte	18
1.9.3	Strukturierte Verkabelung	20
2	Bedienung und grundsätzliche Einstellungen	22
2.1	Das Wireshark Hauptfenster	23
2.1.1	Bereich 1 – Paketliste.	23
2.1.2	Bereich 2 – Paketdetails	24
2.1.3	Bereich 3 – Paket-Bytes	24
2.2	Navigation im Hauptfenster	25
2.3	Paketdetails im Detail	27
2.5	Die Werkzeugleiste	28
2.6	Die Filterleiste	29
2.7	Die Statusleiste	29
2.8	Die Kontextmenüs.	30
3	Erste Netzwerkanalyse / Quickstart	32
3.1	Erste Schritte	33
3.2	Filterung.	34
3.3	Erste Analyse: ping	35
3.4	Aufruf einer Webseite mit einem Browser	37
3.4.1	HypertextTransfer Protokoll, HTTP	38
3.4.2	HypertextTransfer Protokoll secure, HTTPS	40
3.4.3	Quick UDP Internet Communication, QUIC.	40
3.5	User Datagram Protocol (UDP)	41
3.6	Transport Control Protocol (TCP)	42
3.7	Erste Analyse der Transportprotokolle	43
3.8	Internet Protocol (IPv4)	46
3.9	Zeitmessung	47
3.10	Datenverkehr im Ruhezustand	48
4	Analyse für Fortgeschrittene	49
4.1	Mitschnitt speichern/exportieren	49
4.2	Gespeicherte Mitschnitte öffnen	51
4.3	Pakete suchen und finden.	52

4.4	Ungewöhnliche Verbindungen entdecken.	53
4.5	Zeitmessung für Fortgeschrittene	54
4.6	Kommentare einfügen	55
4.7	Infos aus der Statuszeile.	56
4.8	Die Experteninfos	57
4.9	Datenströmen folgen	58
4.10	Statistiken	60
4.10.1	Eigenschaften der Mitschnittdatei	61
4.10.2	Aufgelöste Adressen.	62
4.10.3	Protokollhierarchie	63
4.10.4	Verbindungen und Endpunkten.	64
4.10.5	Paketlängen	66
4.11	Geo-IP – oder „Wo befinden sich die Kommunikationspartner?“	66
4.11.1	GeoIP einrichten	66
4.11.2	Landkarte anzeigen	69
4.11.3	GeoIP filtern.	70
4.12	Graphische Ausgaben.	71
4.12.1	IO-Graph.	71
4.12.2	Datenstrom verfolgen.	72
4.12.3	Stream-Graph	74
5	Filter – die interessanten Daten finden	81
5.1	Anzeigefilter, Display-Filter.	82
5.1.1	Filtern auf Layer 2 (Ethernet-Adressen).	84
5.1.2	Filtern auf Layer 3 (IP-Adressen)	85
5.1.3	Filtern auf Layer 4 (Ports)	85
5.1.4	Weitere Anzeigefilter.	86
5.1.5	Nach Zeichenketten filtern	86
5.1.6	Filter drag n drop.	87
5.1.7	Filter über die Kontext-Menüs erstellen	88
5.1.8	Konversationsfilter, Verbindungsfilter	89
5.1.9	Filtern auf Bits und Bytes	90
5.1.10	Filterausdrücke verwalten.	91
5.1.11	Filterbutton erstellen.	92
5.1.12	Filter reagiert zu langsam.	92
5.2	Aufzeichnungsfiler	93
6	Wireshark den Bedürfnissen anpassen	98
6.1	Wireshark Schnellstart einrichten	98
6.2	Mit Profilen arbeiten	99
6.3	Einstellungen.	100
6.3.1	Layout.	100
6.3.2	Hinzufügen und Ändern von Spalten im Paketfenster.	102
6.3.3	Mitschnitt-Einstellungen.	104
6.3.4	Protokolleinstellungen anpassen.	105
6.3.5	Namens- und Adressauflösung	106
6.4	Aufzeichnungsoptionen, Capture Interfaces.	108
6.4.1	Aufzeichnungsoptionen	108
6.4.2	Aufzeichnungsoptionen – Ausgabe	109
6.4.3	Aufzeichnungsoptionen-Optionen.	110
6.5	Einfärberegeln.	111

7	Aus der Praxis	112
7.1	Infos über die Physikalische Schicht (OSI-Layer 1)	112
7.2	Ethernet-Analyse	113
7.3	IP-Analyse	113
7.3.1	Internet-Protokoll	114
7.3.2	ARP-Analyse von ARP-Betrieb und ARP-Problemen	115
7.3.3	DHCP	118
7.3.4	ICMP – Protokollanalyse und Fehlerbehebung	119
7.3.4.1	Analyse von IPv4 Routing-Problemen	121
7.3.4.2	TTL-Fehler	123
7.3.4.3	Doppelte IP-Adressen	124
7.3.4.4	Analyse von IP-Fragmentierungsfehlern	124
7.4	Analyse der Transportprotokolle	128
7.4.1	UDP-Analyse	128
7.4.2	Fehlerbehebung bei TCP-Verbindungsproblemen	129
7.4.3	Fehlerbehebung bei Problemen mit TCP-Sendewiederholungen	135
7.4.4	Regulärer TCP-Sequenz-/Bestätigungsmechanismus	140
7.4.5	TCP-Sliding Window-Mechanismus	141
7.4.6	Fehlersuche beim TCP-Durchsatz	143
7.5	Weitere Protokolle	146
7.5.1	Domain Name System, DNS	146
7.5.2	File Transfer Protokoll, FTP	148
7.5.3	HTTP-Verkehr (HTTP Flow Analyse)	150
7.6	Mail-Protokolle	153
7.6.1	POP3-Kommunikation	154
7.6.2	IMAP-Kommunikation	155
7.6.3	SMTP-Kommunikation	156
7.7	Protokollauflösung ein-/ausschalten	157
8	Wireshark Spezialanwendungen	159
8.1	Top-Talker finden – die „Hitparade“ der Vielsprecher	159
8.2	Experteninfos	160
8.3	Langzeitaufnahmen	161
8.3.1	Ringpuffer verwenden	162
8.3.2	Mitschnittlänge limitieren	162
8.4	Das Konsolenprogramm tshark	163
8.4.1	Dateiformate konvertieren	164
8.4.2	Mitschnitte an der Konsole filtern	164
8.4.3	URLs automatisch aus Mitschnitt exportieren	164
8.4.4	Protokollhierarchie ausgeben	165
8.5	Das Konsolenprogramm termshark	166
8.6	Firewall Regeln definieren	169
9	Wireshark Analyse einiger IPv6 Protokolle	170
9.1	Einführung in IPv6-Adressen	171
9.2	Aufbau von IPv6-Adressen	172
9.2.1	Scopes	172
9.2.2	Unicast-Adressen	173
9.2.3	Multicast-Adressen	174
9.2.4	Anycast-Adressen	174
9.3	IP(v4)- versus IPv6-Header	175

9.4	Untersuchungen an IPv6-Protokollen	176
9.4.1	Neighbour Discovery Protokoll (NDP)	176
9.4.2	Duplicate Address Detection (DAD)	177
9.4.3	IPv6 Extension Headers	178
9.4.4	ICMPv6	179
9.4.5	IPv6 Fragmentierung	180
9.4.6	Router-Solicitation und Router-Advertisement	181
9.5	DHCPv6	182
9.5.1	Stateless DHCPv6	183
9.5.2	Statefull DHCPv6	183
10	Voice over IP (VoIP)	185
10.1	SIP-Arbeitsprinzip, Nachrichten und Statuscodes	187
10.1.1	SIP-Registrierung	188
10.2	SIP-Statuscodes	192
10.3	Session Description Protocol (SDP)	193
10.4	Real-Time Transfer Protocol (RTP)	196
10.4.1	RTP Stream Analyse	198
10.5	Telefonanruf aufzeichnen, abhören und exportieren	199
10.6	Analyse von Verzögerungen	200
10.7	Wiedergabe von Videos	201
11	Wi-Fi-Sniffing	203
11.1	Die unterschiedlichen WLAN-Standards	203
11.2	Physikalische Grenzen	204
11.3	Vorbereitung	205
11.4	aircrack-ng	205
12	Internet der Dinge, IoT	208
12.1	IEEE 802.15.4	209
12.2	Sigfox	210
12.3	IEEE 802.11 ah	210
12.4	LoRaWAN	211
12.5	IP-Anpassungen an IoT	212
13	Platzieren des Analysators und Abgreifen der Daten	216
13.1	Daten an Quelle abgreifen	216
13.2	Wireshark in die Datenleitung einschleifen	217
13.3	Switch Port Analyser (SPAN), Portspiegelung	218
13.3.1	Probleme bei Portspiegelung	218
13.4	TAP – Test Access Point einsetzen	220
13.4.1	Verschiedene TAP-Arten	221
13.5	SDN Sniffing Regeln verwenden	222
13.6	SPAN – TAP -SDN-Switch vergleichen	222
13.7	Tshark und TCPdump – die textbasierte Analyse	223
13.7.1	Fernzugang zum Sniffen über ssh	223
13.8	Netzwerkpakete in virtuellen Umgebungen erfassen	224
13.8.1	VirtualBox	225
13.8.2	VMWare	226
13.9	Speziallösung Address-Spoofing, Man in the middle	226