BRAIN-MEDIA.DE

PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold

Wireshark kompakt

Security.Edition

Der praxisorientierte Einstieg in die Netzwerk- und Protokollanalyse mit dem freien Klassiker

Holger Reibold

Wireshark kompakt

© 2015 Brain-Media.de

Herausgeber: Dr. Holger Reibold

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Korrektur: Theresa Tting

Coverbild: kallejipp / photocase.de

Druck: COD

ISBN: 978-3-95444-176-1

Inhaltsverzeichnis

Vorwort

Netzwerke – lokale, globale und drahtlose – bestimmen längst unser aller Alltag. Der Nutzen der Netzwerktechnologie ist unbestritten: Sie vereinfacht den Datenaustausch und hat das Internet in seiner heutigen Form erst möglich gemacht. Doch wie wir alle wissen, ist die Technik auch fehleranfällig und birgt so manches Gefahrenpotenzial.

Je intensiver wir auf diese Techniken setzen, umso wichtiger werden Analysewerkzeuge, mit denen Sie den Netzwerktraffic einer eingehenden Analyse unterziehen sowie Anomalien und Ungereimtheiten aufdecken können. Wireshark ist der mit Abstand beliebteste Spezialist für die Netzwerk- und Protokollanalyse. Mit Wireshark gehen Sie Problemen auf den Grund, können Sie den Datentransfer rekonstruieren und verschiedene statistische Auswertungen anstellen. Alles mit dem Ziel, die Vorgänge in Ihrem Netzwerk besser zu verstehen.

In diesem Handbuch lernen Sie, wie Sie mit dem Tool typische Administratoraufgaben bewältigen. Das Buch beschränkt sich dabei auf die wesentlichen Aktionen, die im Admin-Alltag auf Sie warten, und verzichtet bewusst auf überflüssigen Ballast. Zunächst lernen Sie Wireshark und seine wichtigsten Funktionen und Hilfsmittel kennen, mit denen Sie den lokalen, aber auch entfernten Traffic aufzeichnen können.

Die Suche nach Auffälligkeiten in den meist gigantischen Aufzeichnungen ist wie die sprichwörtliche Suche nach der Nadel im Heuhaufen. Hier kommen Sie mit den mächtigen Filterfunktionen des Sniffers schneller an Ziel. Wireshark stellt Ihnen verschiedene Hilfsmittel für die Traffic-Analyse und Auswertungen zur Verfügung. Deren Einsatz wird anhand typischer Praxisbeispiele erläutert, ebenso die Anpassungsmöglichkeiten des Programms.

Wenn Sie diesen Einstieg durchgearbeitet haben, sind Sie bestens für die grundlegenden Aufgaben der Netzwerkanalyse und alle weiteren Schritte gerüstet.

Herzlichst,

Holger Reibold

(Juni 2015)

1 Netzwerkanalyse mit Wireshark – der Einstieg

Der Job eines System- und Netzwerkadministrators ist alles andere als einfach, denn man muss nicht nur die verschiedensten Systeme und Infrastrukturkomponenten kennen, sondern auch permanent Problemen nachgehen und diese lösen.

Die Fehlersuche in einem Netzwerk ist häufig mit der sprichwörtlichen Suche nach der Nadel im Heuhaufen vergleichbar. Um zu erfahren, warum die Verbindungen zu einem lokalen Datenbankserver langsam sind und immer wieder abbrechen, warum ein DSL-Router permanent Internetverbindungen aufbaut oder welche Services Daten nach außen übermitteln, benötigen Sie einen Netzwerk-Sniffer. Der analysiert den Datentransfer über definierbare Netzwerkschnittstellen und gewährt Ihnen teilweise tiefe Einblicke in den Traffic.

All das, und noch viel mehr, kann Wireshark leisten. In der Öffentlichkeit werden Tools zur Netzwerkanalyse häufig als Hacker-Werkzeug diskreditiert, da sie auch von Hackern genutzt werden, um sich Zugang zu fremden Netzwerken zu verschaffen. Das absichtliche Abhören oder Protokollieren von fremden Funkverbindungen ist verboten, außer man besitzt hierfür die explizite Zustimmung des Netzbetreibers. Ungewolltes Abhören ist nach dem deutschen Telekommunikationsgesetz nicht strafbar. Allerdings sind die Speicherung, Weitergabe oder Verwendung der auf diesem Weg erlangten Informationen und Daten ebenfalls nicht zulässig.

Für Netzwerkadministratoren gehört Wireshark dennoch zur Grundausstattung eines Werkzeugkastens.

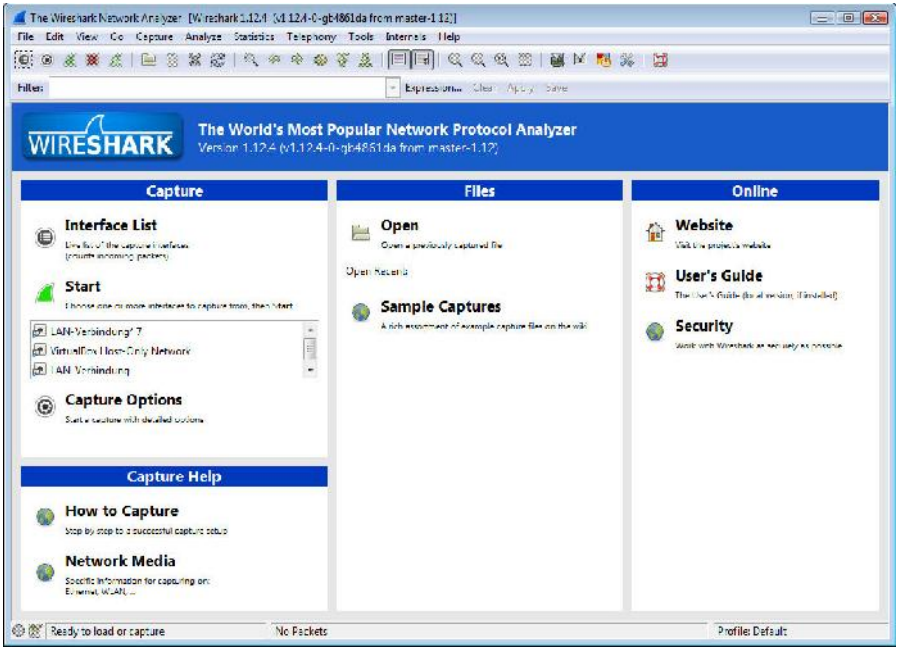
1.1 Wireshark kennenlernen

Wireshark, das früher Ethereal hieß, ist ein freies Programm zur Analyse von Netzwerkkommunikationsverbindungen. Man bezeichnet solche Programme auch als Sniffer. Das Programm stellt entweder während oder nach der Aufzeichnung des Datenverkehrs einer Netzwerkschnittstelle die Daten in Form einzelner Pakete dar.

Das Besondere an dem Sniffer: Die Daten werden übersichtlich und für den Menschen nachvollziehbar analysiert und aufbereitet. Sie können die Darstellung der Mitschnitte mit Filtern gezielt auf bestimmte Informationen beschränken und sogar

Statistiken des Datenflusses erstellen oder binäre Inhalte wie beispielsweise Bilder extrahieren.

Eine weitere Besonderheit: Wireshark ist für alle relevanten Plattformen verfügbar. Sie können den Sniffer also unter Linux, Mac OS X und Windows einsetzen. Unter Windows zeichnet Wireshark den Datenverkehr transparent mit Hilfe von WinPcap auf. WinPcap gehört auch zum Standardinstallationspaket der Windows-Variante.



Ein erster Blick auf die Benutzeroberfläche des freien Netzwerk-Sniffers Wireshark.

Was macht Wireshark nun zu etwas Besonderem? Und warum sollte dieses Programm in jeden Admin-Werkzeugkasten gehören? Einige Besonderheiten des Programms hatte ich ja bereits angesprochen, aber Wireshark kann noch weit mehr, als nur den Netzwerktraffic aufzeichnen und visualisieren.

Ich möchte mich an dieser Stelle nicht lange aufhalten und Ihnen die Grundlagen der TCP/IP-Technologie, das OSI-Schichtenmodell etc. näher bringen. Sie sollten – und haben vermutlich – schon Bekanntschaft mit den Netzwerkgrundlagen ge-

macht. Falls nicht, sollten Sie sich ein wenig bei Wikipedia in die Materie einlesen. Es genügt vollkommen, wenn Sie grundlegende Netzwerkkenntnisse mitbringen. Alles Weitere erlernen Sie dann in der Praxis.

Wenn Sie Wireshark das erste Mal unter Windows starten, wird vermutlich folgende Fehlermeldung ausgegeben:

```
The NPF driver isn't running
```

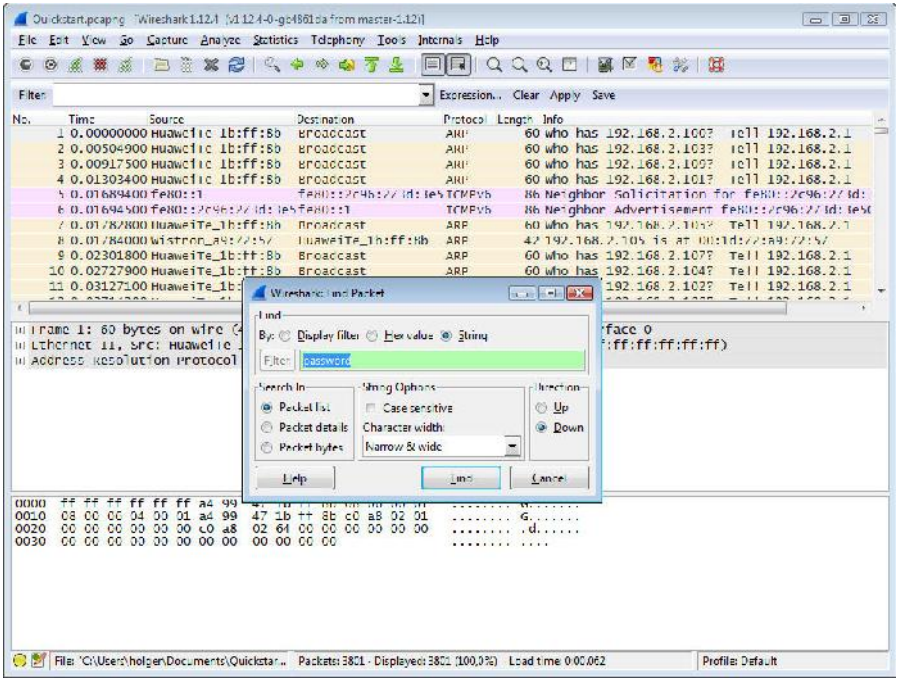
Die besagt, dass der Treiber für die Netzwerkschnittstellen nicht geladen werden konnte. Die Lösung ist einfach: Starten Sie Wireshark als Administrator. Dazu markieren Sie den Wireshark-Eintrag in der Schnellstart- oder Taskleiste mit der rechten Maustaste und führen den Befehl *Als Administrator ausführen* aus.

In diesen einleitenden Abschnitten möchte ich Ihnen in Kurzform zeigen, wie Sie mit Wireshark arbeiten und welche Möglichkeiten Ihnen der Sniffer bietet. Nach dem Start finden Sie im linken Fensterbereich unter *Capture* die Netzwerkschnittstellen, die Wireshark aktuell erkennt und nutzen kann. Prinzipiell kann Wireshark auch Remote-Schnittstellen überwachen; darauf kommen wir später zu sprechen.

Um den Traffic, der über die erste Netzwerkschnittstelle läuft, aufzuzeichnen und zu analysieren, wählen Sie in der Interface-Liste den Eintrag *Eth0* oder *LAN-Verbindung* aus. Dann starten Sie die Aufzeichnung mit einem Klick auf die grüne Haiflosse. Im Wireshark-Hauptfenster können Sie nun verfolgen, wie der Roh-Traffic aussieht, der über die erste Netzwerkschnittstelle läuft.

Starten Sie nun Ihren E-Mail-Client und den Browser. Der E-Mail-Client prüft standardmäßig Ihr Postfach auf neue E-Mails. Dazu müssen eine Verbindung zu dem E-Mail-Server hergestellt und die Zugangsdaten an diesen übermittelt werden. Ähnliches passiert, wenn Sie im Browser die Web-Schnittstelle Ihres Postfaches ansteuern oder sich bei einen Online-Dienst oder Shop anmelden.

Stoppen Sie dann die Aufzeichnung, indem Sie auf die rote Schaltfläche *Stop the running live capture* in der Symbolleiste klicken. Wireshark hält die Aufzeichnung an und Sie können sich als Nächstes an die Auswertung machen. Die Analyse stellt Ihnen verschiedenste Möglichkeiten zur Verfügung. Eine der wichtigsten Optionen ist die Suche.



Die Analyse der Aufzeichnung kann beginnen.

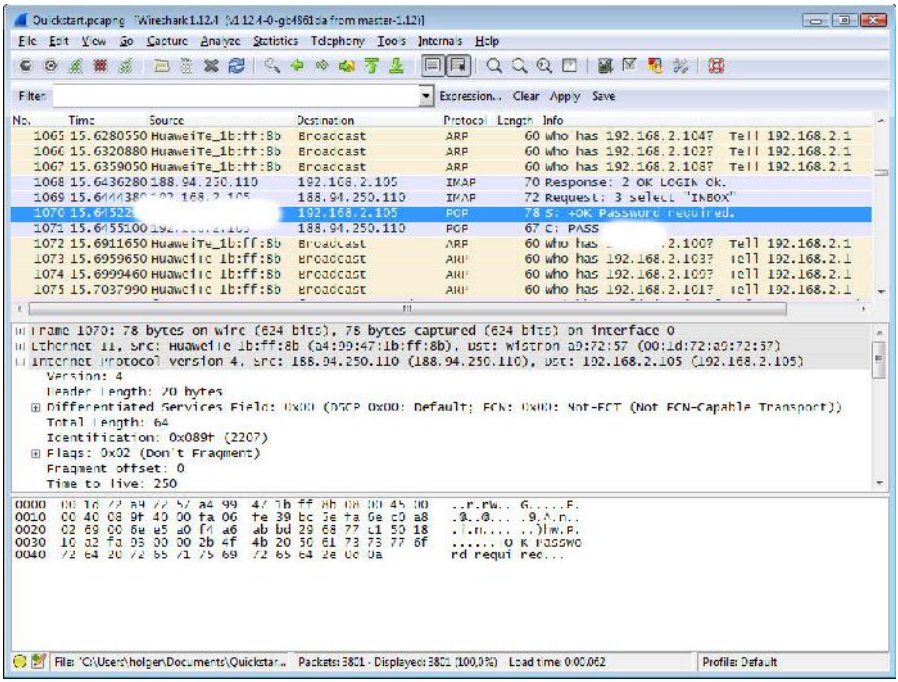
Um die Suche zu öffnen, führen Sie die Tastenkombination *Strg + N* aus. Wireshark präsentiert Ihnen den Suchdialog, der Ihnen verschiedene Suchoptionen und -parameter anbietet. Im Bereich *By* verwenden wir in diesem Quickstart die Option *String*, um eine bestimmte Zeichenfolge zu suchen.

Die weiteren Suchoptionen für die Einschränkung der Suche sind die folgenden:

- Suche in
- String-Optionen
- Richtung

Die Suche starten Sie mit einem Klick auf die Schaltfläche *Find*. Im vorliegenden Beispiel verwenden wir den Suchbegriff *Password*. Der steht für das Passwort, das für das Einloggen in den E-Mail-Server und den Online-Dienst benötigt wird.

Wireshark markiert die Fundstelle in der Aufzeichnung und Sie können direkt ermitteln, im welchem Zusammenhang ein Passwort an welchen Dienst übertragen wurde. Sie werden dabei häufig feststellen, dass die Passwörter unverschlüsselt übertragen werden. Damit sind sie für Hacker ein gefundenes Fressen.



Wireshark hat schnell und einfach den Traffic identifiziert, der für die Passwortübermittlung zuständig ist.

Da Wireshark automatisch das gefundene Paket markiert und ansteuert, ist es einfach, die relevanten Informationen auszuwerten. Damit haben Sie einen ersten Eindruck, was Sie mit Wireshark konkret anfangen können.

1.2 Bedienelemente

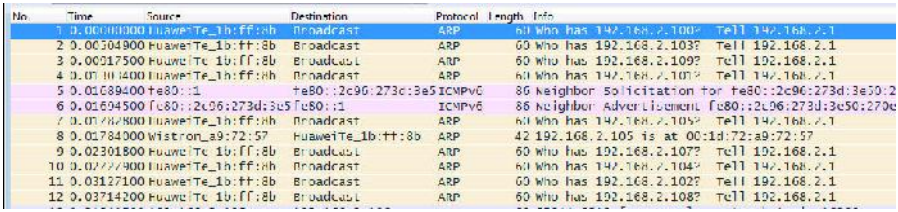
Bevor wir uns den weiteren Möglichkeiten widmen, die Wireshark bietet, möchte ich noch kurz auf die wesentlichen Bedienelemente der Benutzeroberfläche zu sprechen kommen.

Die Kopfzeile zeigt Ihnen die Bezeichnung der Aufzeichnungsdatei an – sofern Sie diese gespeichert haben. Hier werden auch die Bezeichnung der überwachten Schnittstelle und die verwendete Wireshark-Version angezeigt.

Es folgt die Menüleiste, über die nahezu die gesamte Funktionalität des Analysewerkzeugs bereitsteht. Es folgt die Symbolleiste, die die am häufigsten verwendeten Befehle zur Verfügung stellt. Die Funktionen dieser Leiste sollten Sie im Laufe der Zeit aus dem Effeff kennen.

Die Filterfunktion von Wireshark.

Die Filterfunktion ist eine essentielle Funktion, mit der Sie gezielt die Darstellung der Aufzeichnungen beschränken können. Der Filter hilft Ihnen dabei, die Daten herausfiltern, die für Sie relevant sind. Die Filterfunktion erlaubt das Sichern von Filterkonfigurationen, um später auf diese zurückgreifen zu können.



Die Paketliste.

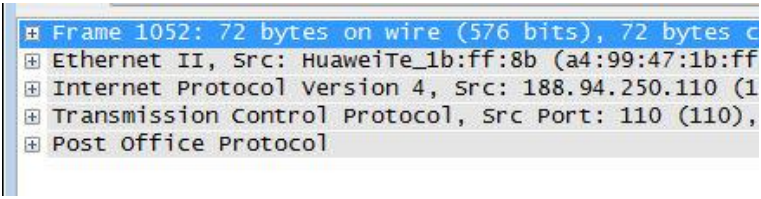
In der sogenannten Paketliste werden die aufgezeichneten Pakete aufgeführt. In der Liste werden die Pakete durchnummeriert und mit einem Zeitstempel versehen. Der Zeitstempel beginnt dabei mit dem Wert 0, der den Beginn der Aufzeichnung markiert. Die Paketliste führt folgende Spalten auf:

- Quelle
- Ziel
- Protokoll
- Länge

- Informationen

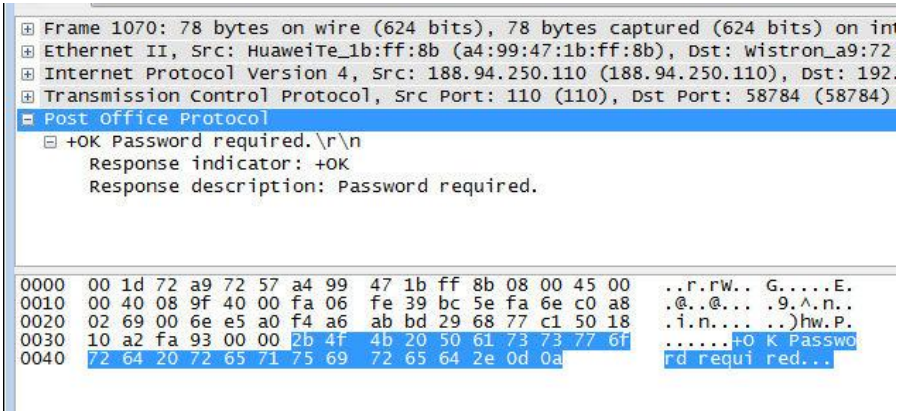
Über die Spaltenköpfe können Sie die Listeneinträge sortieren und somit beispielsweise die Darstellung nach den Zielsystemen sortieren.

Als Nächstes präsentiert Ihnen Wireshark die Liste der Paketdetails. Den Details kann man entsprechend dem OSI-Schichtenmodell die Details zu den verschiedenen Paketen entnehmen. Dabei enthält der erste Eintrag den gesamten Daten-Frame. Welche weiteren Einträge existieren, ist von Paket zu Paket unterschiedlich. Nachstehendes Beispiel zeigt beispielsweise weitere Details zu IP, TCP und POP. Über Pluszeichen bzw. Dreiecke können Sie weitere Details entnehmen.



Die Paketdetails.

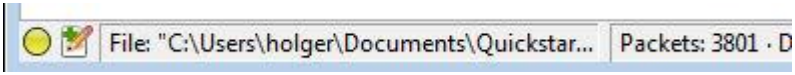
Es folgt die Byte- bzw. Rohdatenansicht. In dieser Ansicht können Sie die Informationen, die in den Paketen enthalten sind, in hexadezimaler und ASCII-Ansicht einsehen.



Die Paketdetails und die Rohdatenansicht.

Die verschiedenen Ansichten sind miteinander verknüpft und Sie können durch die Paketdetails zu den Rohdaten navigieren.

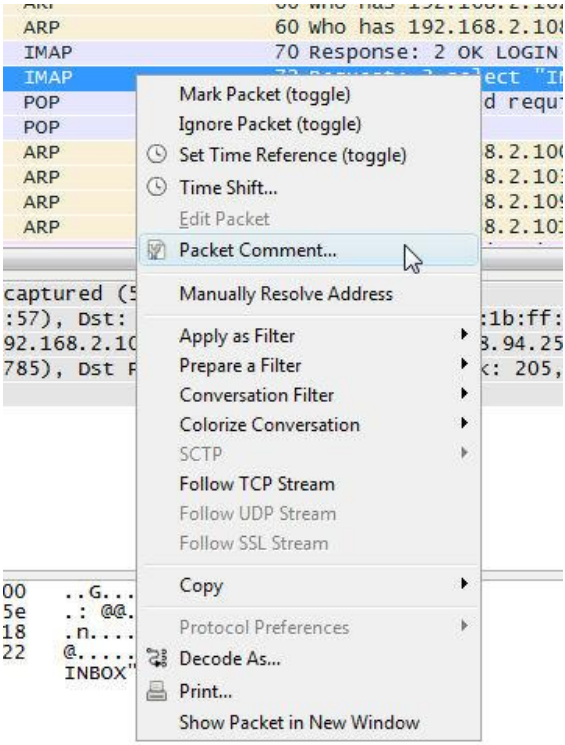
Insbesondere in der ASCII-Datendarstellung können Sie die übermittelten Informationen einsehen. Wie wir im weiteren Verlauf noch sehen werden, können Sie innerhalb der Programmoberfläche eine Fülle weiterer Funktionen ausführen.



Die Statusleiste von Wireshark.

Den Abschluss nach unten bildet die Statusleiste, die Ihnen verschiedene Funktionen und Informationen zur Verfügung stellt. Links finden Sie das Info-Symbol, das Ihnen den sogenannten Info-Status anzeigt.

Das Notiz-Symbol stellt Ihnen Platz für Ihre Anmerkungen zur aktuellen Aufzeichnung zur Verfügung. Haben Sie die Aufzeichnung als Capture-Datei gespeichert, verrät die Statuszeile Ihnen auch den Pfad. Der Statuszeile können Sie außerdem die Anzahl der Pakete und das gewählte Capture-Profil entnehmen.



Durch den Einsatz von Kontextmenüs ist Wireshark besonders benutzerfreundlich.

1.3 Was Wireshark so alles kann

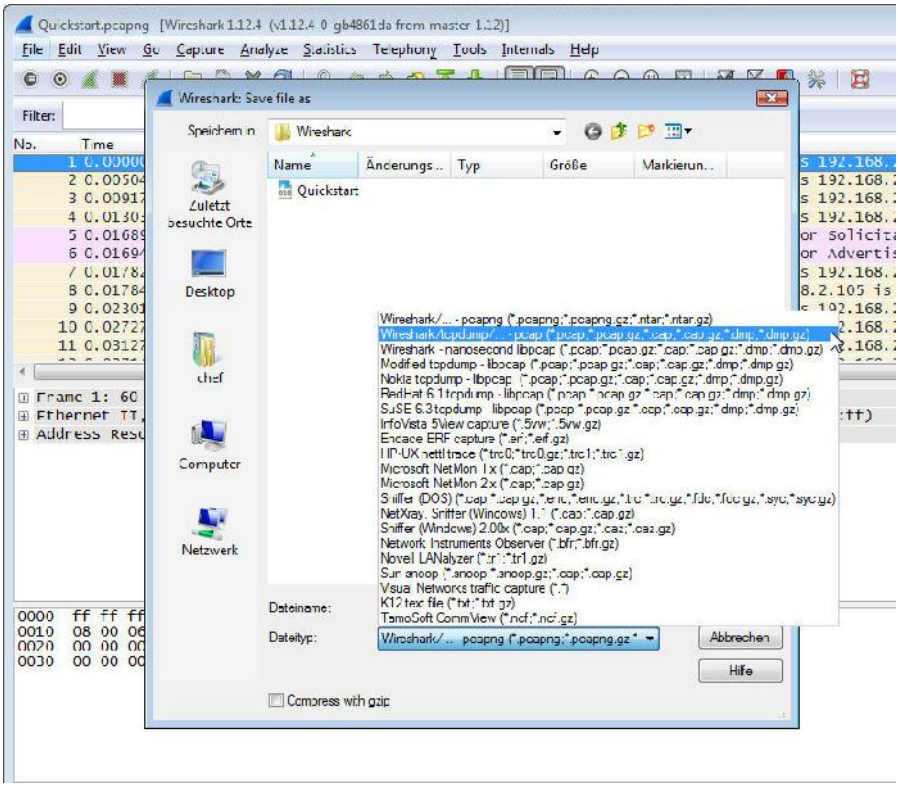
Wireshark ist laut der Website SecTools.org das beliebteste Sicherheitswerkzeug – noch weit vor anderen namhaften Tools. Laut Angaben der Entwickler wird der Sniffer Monat für Monat über 500.000 Mal von der Projekt-Site heruntergeladen. Dabei sind nicht die Downloads mitgezählt, bei denen Wireshark ein tragendes Element ist. Man denke beispielsweise an Kali Linux.

Wireshark verdankt seine Verbreitung sicherlich auch dem Umstand, dass das Programm für alle relevanten Betriebssystemplattformen verfügbar ist. Inzwischen gibt es sogar einen abgespeckten Android-Client und eine portable Version.

Auch wenn es auf den ersten Blick nicht unbedingt offensichtlich ist, zeichnet sich Wireshark durch eine hohe Benutzerfreundlichkeit aus – zumindest gilt das für ein

Programm dieser Art. Insbesondere durch den Einsatz von Kontextmenüs der rechten Maustaste ist Wireshark benutzerfreundlich. Die Menüs bieten unterschiedliche Funktionen, abhängig davon, welche Elemente Sie in Wireshark markieren.

Die Kernaufgaben von Wireshark sind die Fehlererkennung, die Sicherheitsanalyse und -prüfung sowie die Fehlerbehebung in Ihrem Netzwerk. Dabei wird üblicherweise zunächst der Datenverkehr aufgezeichnet und dann im nächsten Schritt analysiert.



Wireshark unterstützt vielfältige Formate.

Das Besondere dabei: Sie können Ihre Aufzeichnungen in unzähligen verschiedenen Formaten sichern und somit auch problemlos anderen Anwendern zur Verfügung stellen. Standardmäßig werden die Aufzeichnungen, auch Captures genannt, im PCAPNG-Format gesichert.

Wireshark verwendet für die Dekodierung der aufgezeichneten Daten sogenannte Dissektoren, die die Daten zerlegen und aus den übermittelten Datenpaketen die Datenfelder und Netzwerk-Frames identifizieren und anschließend darstellen.

Nicht immer, aber doch in vielen Fällen können diese Dissektoren auch die Inhalte der Frame interpretieren. Das wiederum kommt den Anwendern zugute, denn damit vereinfacht sich die Analyse und Interpretation der Informationen, die Ihnen der Sniffer präsentiert.

Da Wireshark ein klassisches Open Source-Projekt mit einer großen Community und Fangemeinde ist, wurden im Laufe der Jahre Tausende solcher Dissektoren entwickelt, die gängige Anwendungen und Protokolltypen analysieren können. Wireshark setzt dabei auf Lua für die Entwicklung von Dissektoren, aber auch von sogenannten Taps.

1.4 Die zentralen Aufgaben

Die wichtigsten Aufgabenbereiche von Wireshark sind die allgemeine Netzwerkanalyse, die Fehlersuche, die Sicherheitsprüfung und die Programmanalyse. Für jeden dieser Bereiche bietet Wireshark umfangreiche Funktionen.

Wenn Sie Ihr Netzwerk zunächst einer allgemeinen Analyse unterziehen wollen, so bietet Wireshark hierfür interessante Möglichkeiten. Sie können beispielsweise recht einfach herausfinden, welches die „geschwätzigsten“ Systeme sind. Sie können den typischen Datenverkehr als Klartext darstellen und die typischen Kommunikationsvorgänge ermitteln.

Sie können mit Hilfe von Wireshark herausfinden, ob die typischen Netzwerkfunktionen in Ihrem Netzwerk ordnungsgemäß funktionieren und auf welchen Hosts welche Dienste und Programme laufen.

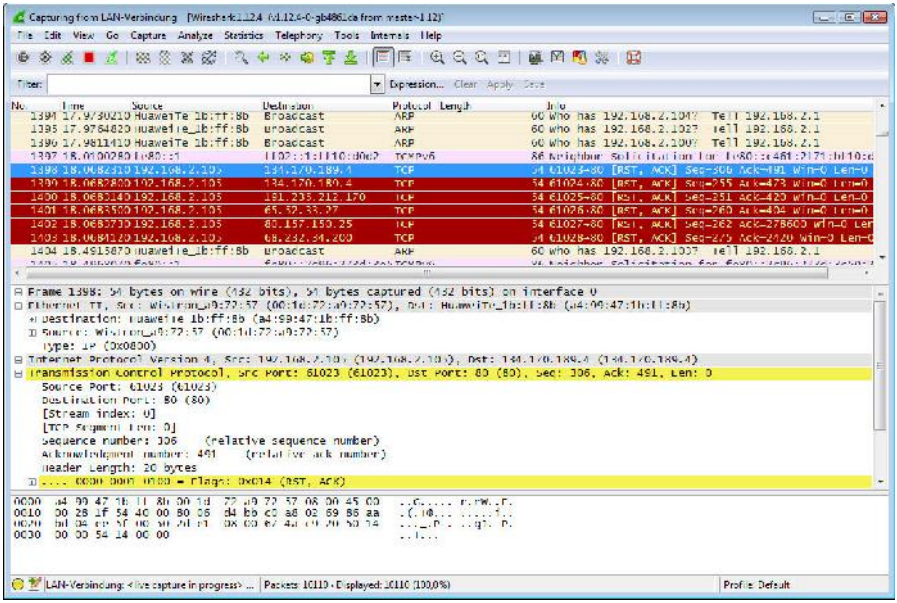
Da die drahtlose Kommunikation längst ein essentieller Bereich der Netzwerkkommunikation ist, müssen Sie wissen, welche Rechner sich Zugang zu Ihrem Netzwerk verschaffen wollen. Auch das kann Wireshark für Sie ermitteln.

Sie können mit Wireshark allerdings nicht nur eine Schnittstelle oder ein lokales Netzwerk überwachen, sondern auch mehrere. Dabei ist das Aufzeichnen und Analysieren des ein- und ausgehenden Datenverkehrs eines bestimmten Hosts oder Subnetzes möglich. Sie können auch den HTTP- und FTP-Datentransfer aufzeichnen und gegebenenfalls rekonstruieren.

Ich hatte es oben angedeutet, dass Wireshark die Aufzeichnungen in verschiedenen Formaten sichern bzw. die Daten in verschiedene Formate exportieren kann. Aber auch der umgekehrte Weg ist möglich: Sie können die Daten anderer Sniffer in

Wireshark importieren und profitieren dann von den Analysefunktionen, die Ihnen Wireshark zur Verfügung stellt.

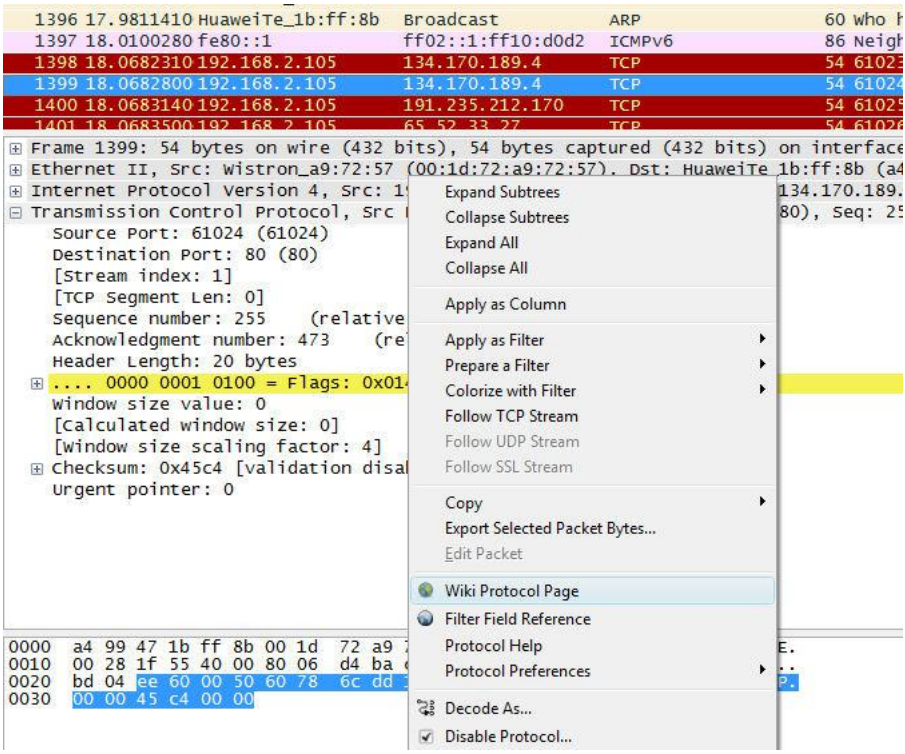
Eine der beliebtesten Aktionen für den Einstieg in Wireshark ist die Aufzeichnung des Traffics im eigenen Netzwerk in Ruhezustand, also dann, wenn keine Clients oder Server in irgendeiner Form aktiv sind. Sie werden nicht schlecht staunen, wie hoch dieses „Grundrauschen“ Ihres Netzwerks ist. Wir kommen weiter unten konkret darauf zu sprechen.



Das Grundrauschen eines Netzwerks ist beachtlich. Hier fallen untypische Netzwerkaktivitäten besonders schnell auf.

1.5 Fehlersuche

Neben der allgemeinen Netzwerkanalyse unterstützt Sie Wireshark insbesondere bei der Fehlersuche. Mit Hilfe des Sniffers können Sie beispielsweise Verzögerungen beim Datenverkehr zwischen Clients und Servern oder anderen relevanten Diensten ermitteln. Mit Wireshark kommen Sie TCP- und HTTP-Proxy-Problemen genauso auf die Spur, wie den Fehlermeldungen von bestimmten Applikationen.



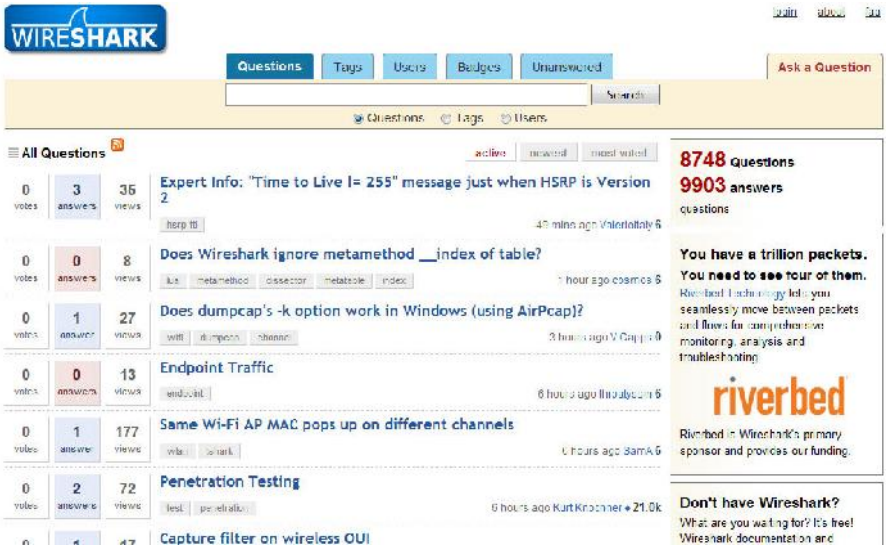
Wireshark unterstützt Einsteiger und Profis durch die Wiki-Integration gleichermaßen.

Kommen Ihnen bei der Traffic-Analyse bestimmte Einträge merkwürdig oder verdächtig vor, können Sie diese aber mangels Erfahrung nicht auf den ersten Blick interpretieren, hilft Ihnen die Wiki-Integration weiter. In der Detailansicht steht über das Kontextmenü der rechten Maustaste das Wireshark-Wiki mit den entsprechenden Einträgen zur Verfügung.

Mit Hilfe von Wireshark können Sie auch verminderte Datendurchsätze identifizieren, doppelte IP-Adressen ermitteln und überfüllte Datenpuffer identifizieren.

Sie können Wireshark auch dafür verwenden, um die Signalstärke in einem WLAN anzuzeigen und um deren Qualität zu prüfen. Sie kommen mit Wireshark wiederholten drahtlosen Verbindungsversuchen auf die Schliche.

Wireshark kann insbesondere gängige Fehlkonfigurationen im lokalen Netzwerk ermitteln und alle jene Anwendungen identifizieren, die einen unverhältnismäßig hohen Datendurchsatz und Traffic generieren.



Keine offene Fragen: Ask Wireshark liefert die Antworten auf all Ihre Fragen.

Wireshark-Anwender profitieren beim Einsatz des Sniffers von der langen Tradition und der riesigen Community, die das Tool pflegt und dokumentiert. Wenn Sie mit dem Wiki nicht weiterkommen, steht Ihnen mit Ask Wireshark (*http://ask.wireshark.org*) eine tolle Plattform zur Verfügung, in der Sie Ihre Fragen und Probleme loswerden können. Dort bleibt keine Frage unbeantwortet – im Gegenteil. Im Mai 2015 gab es zu 8748 bisher gestellten Fragen sage und schreibe 9903 Antworten.

1.6 Sicherheitschecks

Den dritten wichtigen Bereich, den Wireshark abdeckt, sind die Sicherheitsprüfungen. Sie können den Sniffer sogar als forensisches Werkzeug einsetzen.

Sie können mit Wireshark recht einfach all die Applikationen in Ihrem Netzwerk identifizieren, die keine Standard-Ports verwenden. Der Sicherheitsspezialist taugt auch dazu, ein- und ausgehenden Traffic von verdächtigen Hosts zu erkennen.

Trojaner, Backdoors und andere unerwünschte Prozesse haben häufig die Eigenschaft, den Angreifer über den aktuellen Status und neue Informationen zu informieren. Derartige Muster kann Wireshark genauso ermitteln, wie den ein- und ausgehenden Datenverkehr von verdächtigen Hosts.

Mit seinen Prüffunktionen kann Wireshark sogar Prozesse identifizieren, die versuchen, das eigene Netzwerk auszukundschaften. Nicht minder interessant ist die Möglichkeit, die Zieladressen dieses Traffics zu lokalisieren und zu kartographieren.

Wireshark kann auch fragwürdige Umleitungen und verdächtige Frames entdecken. Der Sniffer kennt außerdem die bekannten Signaturen von Kennwortattacken.

1.7 Programmanalyse

Den letzten Funktionsbereich, den Wireshark noch zu bieten hat, ist die Programmanalyse. Sie können sich mit dem Sniffer über die Funktionsweise von aktivierten Netzwerkprogrammen und -diensten informieren. Der Sicherheitsspezialist erlaubt die Auswertung und grafische Aufbereitung der Bandbreitennutzung. Sie können mit Wireshark auch Fehlermeldungen von Programmen und den damit bereitgestellten Diensten nachgehen.

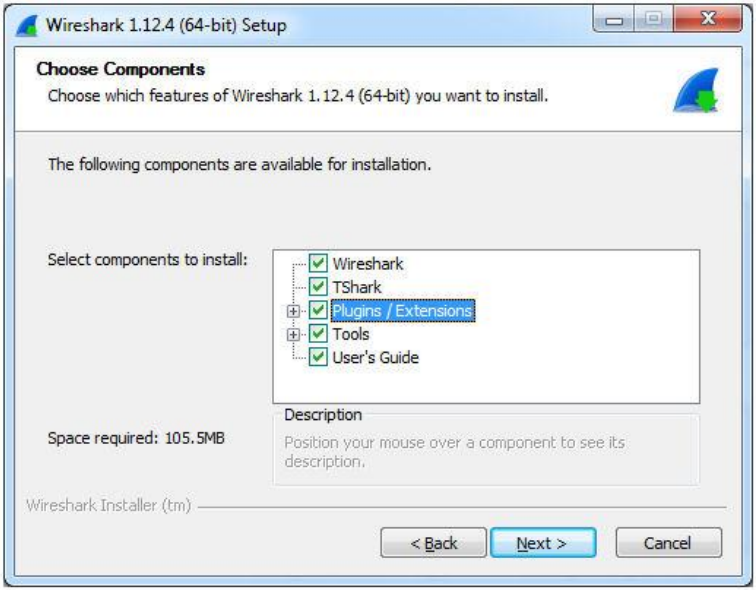
Auch die Darstellung, welche Benutzer welches Programm verwenden, beherrscht Wireshark. Last but not least können Sie mit Wireshark ausfindig machen, wie Programme beispielsweise die Transportprotokolle TCP und UDP verwenden.

1.8 Wireshark in Betrieb nehmen

Sind Sie von den Möglichkeiten und der Funktionalität von Wireshark überzeugt, können Sie sich im nächsten Schritt der Installation des Sniffers zuwenden und Wireshark in Betrieb nehmen.

Laden Sie sich dazu zunächst die aktuelle Wireshark-Version herunter. Die trägt im Mai 2015 die Programmbezeichnung 1.12.x. Unter Windows ist die Installation wirklich ein Kinderspiel. Starten Sie mit einem Doppelklick auf die Installationsdatei die Installationsroutine.

Sie müssen zunächst den Lizenzbedingungen zustimmen. Im zweiten Schritt erfolgt die Auswahl der zu installierenden Komponenten. Hier sind in der Regel keine weiteren Anpassungen erforderlich.



Die Auswahl der zu installierenden Wireshark-Komponenten.

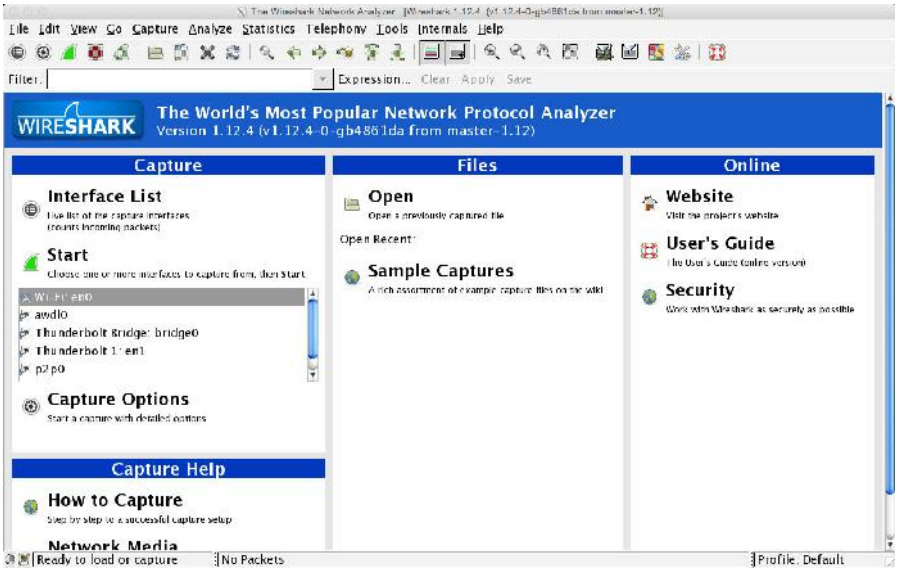
Bestimmen Sie im nächsten Dialog, welche Systemverknüpfungen Sie anlegen wollen und mit welchen Dateierweiterungen Sie den Sniffer verknüpfen wollen.

Der nächste Schritt dient der Konfiguration des Zielverzeichnisses. Stimmen Sie im Folgedialog der Installation von WinPcap zu. Das ist ein Treiber, der durch den Hardware-nahen Zugriff auf die Netzwerkkarte das Sammeln der übertragenen Daten erlaubt.

Mit einem abschließenden Klick auf *Install* starten Sie dann die Installation. Sie können den Installationsvorgang in einer Fortschrittsanzeige verfolgen. Während

der Installation müssen Sie auch der WinPcap-Installation und der zugehörigen Lizenz zustimmen. Zum Abschluss können Sie Wireshark das erste Mal starten.

Unter alternativen Betriebssystemen ist die Installation von Wireshark ebenfalls einfach durchzuführen. Bei den meisten Linux-Distributionen lässt sich Wireshark einfach mit Hilfe des jeweiligen Paketmanagers installieren. Wenn Sie Wireshark unter Mac OS X verwenden wollen, müssen Sie zunächst die X11-Komponenten installieren. Anschließend steht einer Installation auf einem Apple-Rechner nichts im Weg.



Wireshark unter Mac OS X.

1.9 Die Aufzeichnung des Datenverkehrs

Grundlegende Netzwerkkenntnisse sind für die Verwendung von Wireshark unerlässlich. Wenn Sie dann auch noch wissen, wie Wireshark die Daten aufzeichnet, steht einer erfolgreichen Netzwerk- und Traffic-Analyse nichts mehr im Wege.

Die Aufzeichnungen von Wireshark basieren auf einer flexiblen Architektur, die erst durch spezielle Treiber möglich wird. Ein Computer, der eine Netzwerkverbindung per Ethernet oder einen WLAN-Adapter herstellt, verwendet hierfür zu-

nächst einen spezifischen Netzwerkadapter und einen sogenannten Link Layer-Treiber.

Wireshark kann über diese beiden Komponenten direkt auf den Netzwerkverkehr zugreifen und diesen aufzeichnen und für die anschließende Analyse bereitstellen.

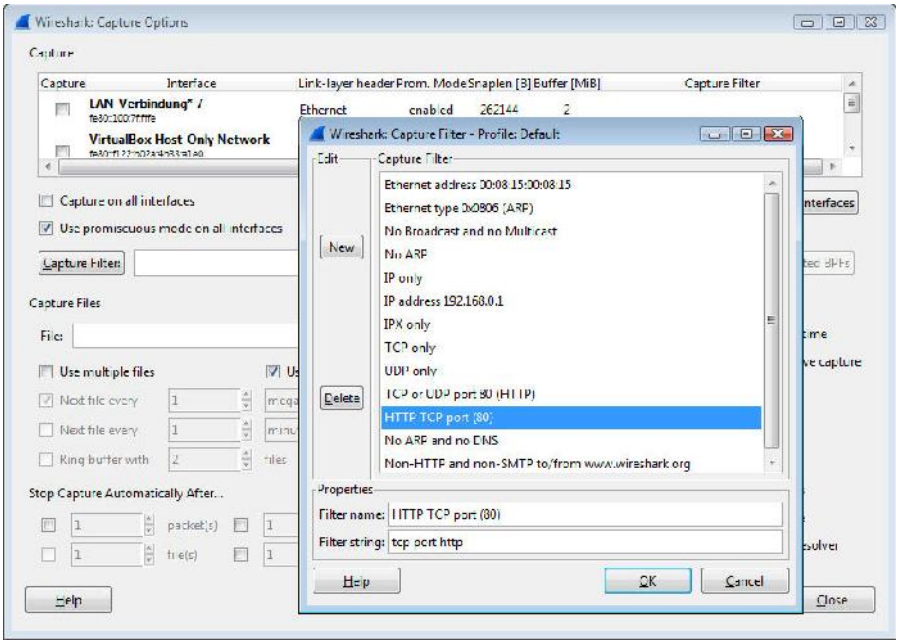
In der Praxis verwendet Wireshark für das Einlesen des Traffics die beiden Treiber WinPcap und libpcap. WinPcap ist die Windows-Variante des Pcap-Treibers, die Bibliothek libpcap kommt bei unixartigen Betriebssystemen zum Einsatz.

Sowie Sie die Datenaufzeichnung beginnen, startet Wireshark eine kleines Hilfsprogramm: dumpcap. Dieses Hilfsprogramm ist für die eigentliche Aufzeichnung zuständig. Konkret reicht das Utility die Frames mit Hilfe eines speziellen Link Layer-Treibers an das Aufzeichnungsmodul von Wireshark, die so genannte Capture Engine, weiter.

Wireshark stellt Ihnen nun zwei Filter für die gezielte Einschränkung der Ausgangsdaten zur Verfügung:

- Capture Filter
- Display Filter

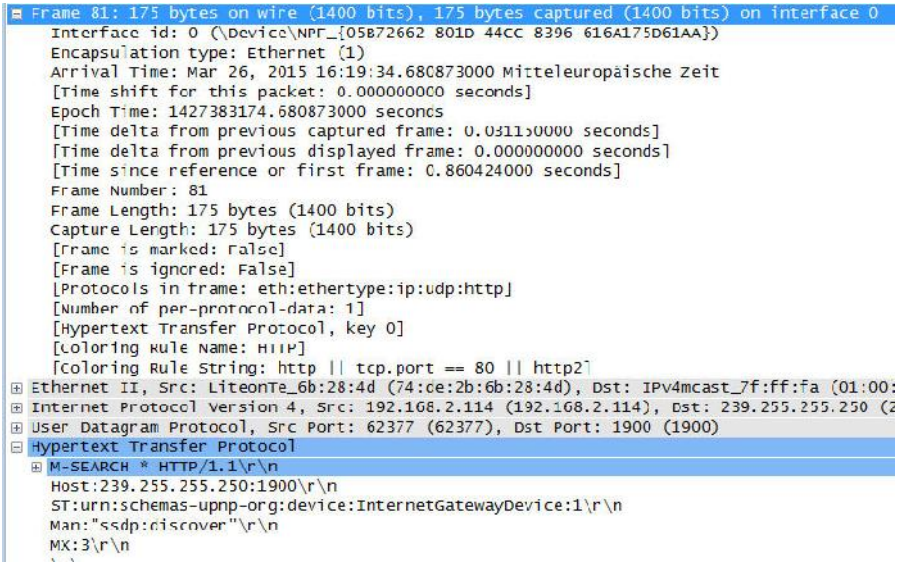
Die Capture Filter kommen auf der netzwerknahen Ebene zum Einsatz und erlauben es Ihnen, den aufzuzeichnenden Traffic frühzeitig einzuschränken. Sie können die Aufzeichnung beispielsweise auf diesem Weg auf IP- oder HTTP-Traffic begrenzen.



Die Konfiguration der Capture-Filter.

Die Display-Filter dienen nach der Aufzeichnung dazu, die bereits gesammelten Informationen zu bündeln und dann zu filtern. Über die Capture-Optionen kann man genau bestimmen, welche Pakete von dumpcap aufgezeichnet werden.

Nachdem dumpcap die Daten an die Capture Engine übergeben hat, werden die dort von der Core Engine und den verfügbaren Dissektoren, Plug-ins und schließlich den Display-Filtern verarbeitet. Die Dissektoren splitten die Daten-Frames in die verschiedenen Datenfelder auf und Sie können häufig bereits eine Analyse der Datenfelder bzw. der Inhalte in diesen Feldern durchführen.



Frames und Pakete.

1.10 Datenpaket versus Frame

Wir sind im bisherigen Verlauf dieses Einstiegs in die Netzwerkanalyse mit Wireshark immer wieder den beiden Begriffen Datenpakete, oder kurz Paket, und Frames begegnet. Damit Sie immer genau wissen, wovon hier die Rede ist, sollten Sie die Merkmale der beiden und deren Unterschiede kennen.

Im Zusammenhang mit Wireshark beschreibt ein Frame einen Kommunikationsvorgang auf der MAC-Ebene inklusive dem MAC-Header und Trailer. Die Kommunikation zwischen zwei Geräten bzw. Diensten erfolgt dabei auf Frame-Basis.

Nun bezeichnet Wireshark in der Paketliste die verschiedenen Einträge in chronologischer Abfolge als Frame 1, Frame 2 etc. Diese Kennzeichnung ist allerdings ein wenig irreführend, denn der erste Abschnitt enthält lediglich einen Header, den Wireshark anlegt.

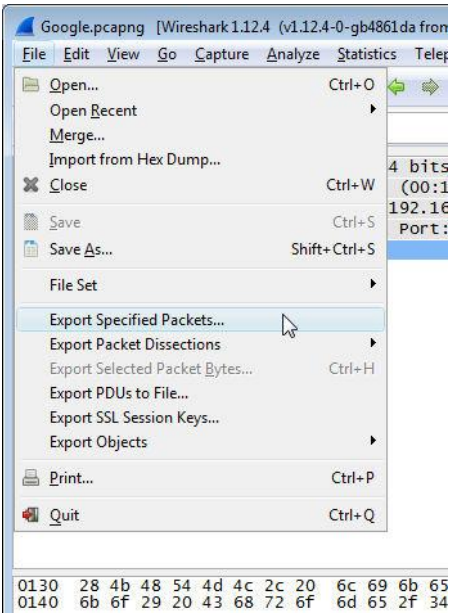
Der Frame, von dem wir hier sprechen, beginnt in obigem Beispiel erst mit dem zweiten Eintrag *Ethernet II*. Alle Informationen oberhalb dieses Elements sind Wireshark-eigene Metadaten. Unser Frame umfasst alle weiteren Inhalte bis einschließlich dem Hypertext Transfer Protocol-Knoten.

Beim einem Paket handelt es sich um den Inhalt eines MAC-Frames. In unserem Beispiel beginnt das Paket mit den IP-Kopfzeilen und endet unmittelbar vor der MAC-Fußzeile.

1.11 Einstieg in die praktische Analyse des Datenverkehrs

Anhand eines zweiten Workshops möchte ich Ihnen als Nächstes zeigen, wie Sie die wichtigsten Funktionen von Wireshark in der Praxis einsetzen und welche weiteren Funktionen Sie kennenlernen sollten, um effektiv mit dem Sniffer arbeiten zu können.

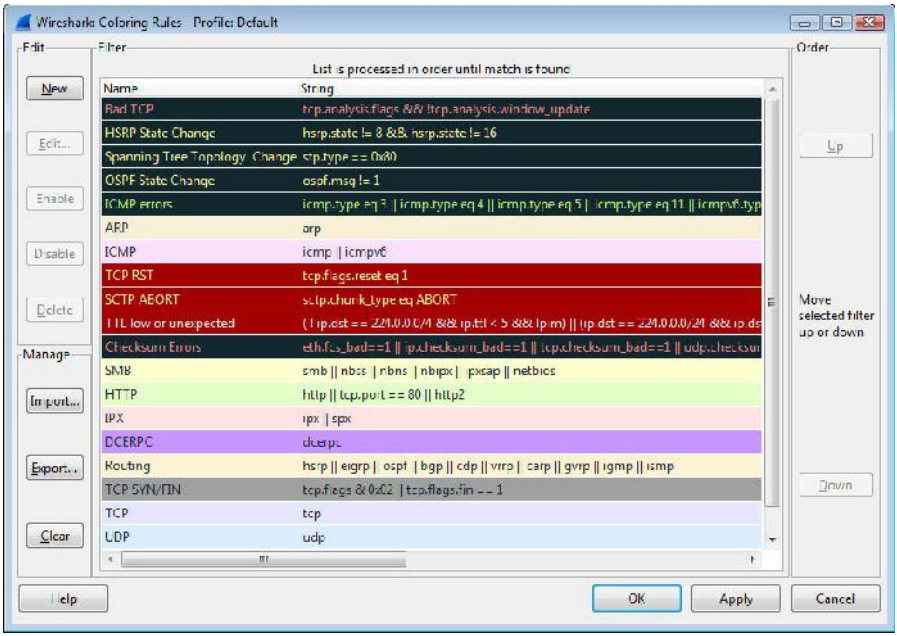
In diesem kleinen Workshop verwenden wir einen Browser, steuern Google an und führen eine Suche mit einem Suchbegriff durch. Dazu starten Sie in Wireshark eine neue Capture-Session, starten dann einen Browser und steuern damit Google an. Im Browserfenster geben Sie dann einen beliebigen Suchbegriff ein. Nachdem im Browser das Suchergebnis ausgegeben wird, beenden Sie die Aufzeichnung.



Das *File*-Menü stellt Ihnen die wichtigsten dateispezifischen Funktionen zur Verfügung.

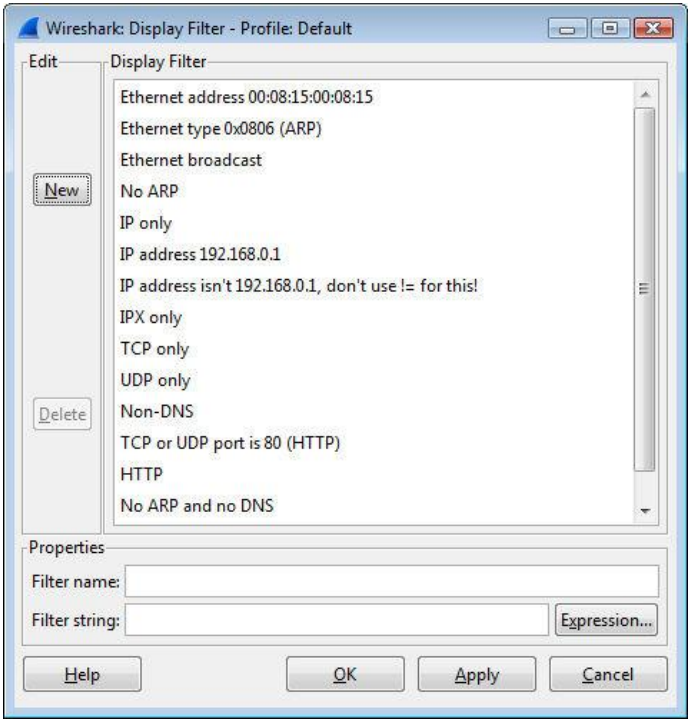
Diese Aktionen sind bislang nichts Neues für Sie, aber um ein Maximum aus dem Programm herausholen, sollten Sie insbesondere mit den wichtigsten Funktionen und Bedienelementen vertraut sein. Das Hauptmenü stellt Ihnen folgende Funktionen zur Verfügung:

- **File**: Das Dateimenü erlaubt Ihnen das Öffnen von einer oder mehreren Capture-Dateien. Hier finden Sie auch verschiedene Exportmöglichkeiten.
- **Edit**: Im Bearbeiten-Menü finden Sie umfangreiche Such- und Markierungsmöglichkeiten. Auch die Programmeinstellungen sind über dieses Menü verfügbar.
- **View**: Das Ansichten-Menü erlaubt Ihnen die Anpassung der Ansicht, die Ihnen Wireshark präsentiert. Sie können beispielsweise die Paketliste und -details ein- und ausschalten. Sollte Ihnen die Farbzuordnung nicht zusagen, die Wireshark den verschiedenen Elementen und Inhalten zuweist, können Sie diese mit dem Untermenü *Coloring Rules* ändern.



Die Einstellungen für die farbige Kennzeichnung der aufgezeichneten Daten.

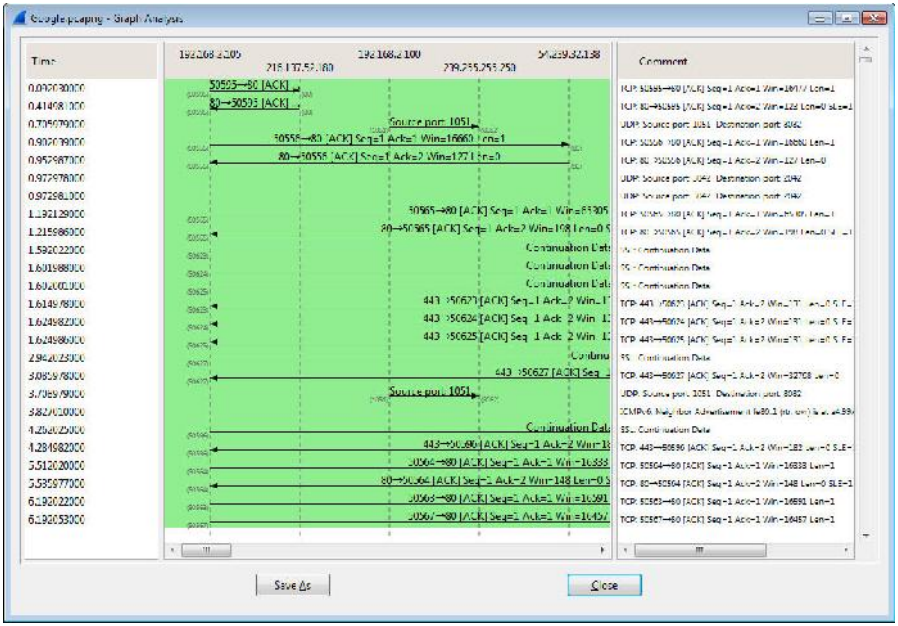
- **Go**: Dieses Menü dient der Navigation in den zu analysierenden Daten. Sie können dabei insbesondere von Paket zu Paket springen.
- **Capture**: Die Funktionen dieses Menüs dienen insbesondere der Auswahl und Konfiguration der zu überwachenden Schnittstellen. Sie können aber auch die Capture-Optionen und die Capture-Filter anpassen.
- **Analyze**: Dieses Menü dient in erster Linie der Auswahl der Darstellungsfilter. Sie können damit beispielsweise die dem Standardprofil zugeordneten Filter bearbeiten. Ihnen stehen aber auch Dekodierfunktionen zur Verfügung. Sie können außerdem verschiedenen Streams folgen.



Die Filter des Standardprofils.

- **Statistics**: An Daten und Informationen wird es Ihnen bei der Verwendung von Wireshark nie mangeln. Das zeigt ein erster Blick in der Menü *Statistics*. Sie können allgemeine statistische Zahlen über dieses Menü ab-

rufen, aber auch jede Menge Details bis hin zu aufwändigen grafischen Aufbereitungen des Datenverkehrs. Ein Bespiel hierfür ist die grafische Analyse, wie Sie in nachstehender Abbildung dargestellt ist.



Alle Achtung: Die grafische Traffic-Auswertung zeigt Ihnen genau, wie und wo welche Daten transferiert wurden.

- **Telephony**: Das Telefonie-Menü stellt Ihnen umfangreiche Analyse- und Auswertungsfunktionen für den Telefonverkehr zur Verfügung. Insbesondere VoIP- und SIP-Verbindungen können mit Wireshark untersucht werden.

- **Tools**: Mit den Funktionen dieses Untermenüs können Sie die Firewall-Regeln für eine geöffnete Capture-Konfiguration anpassen und auf die LUA-Funktionen zugreifen.

- **Internals**: Das Interna-Untermenü bietet Ihnen die Möglichkeit, die Dissektoren-Tabellen des Sniffers einzusehen. Die Tabellen sind in dem zugehörigen Dialog auf drei Registerkarten verteilt:

- String
- Integer
- Heuristisch

Wenn Sie exakt wissen wollen, welche Protokolle Wireshark tatsächlich unterstützt, so können Sie das dem Untermenü *Supported Protocols* entnehmen.

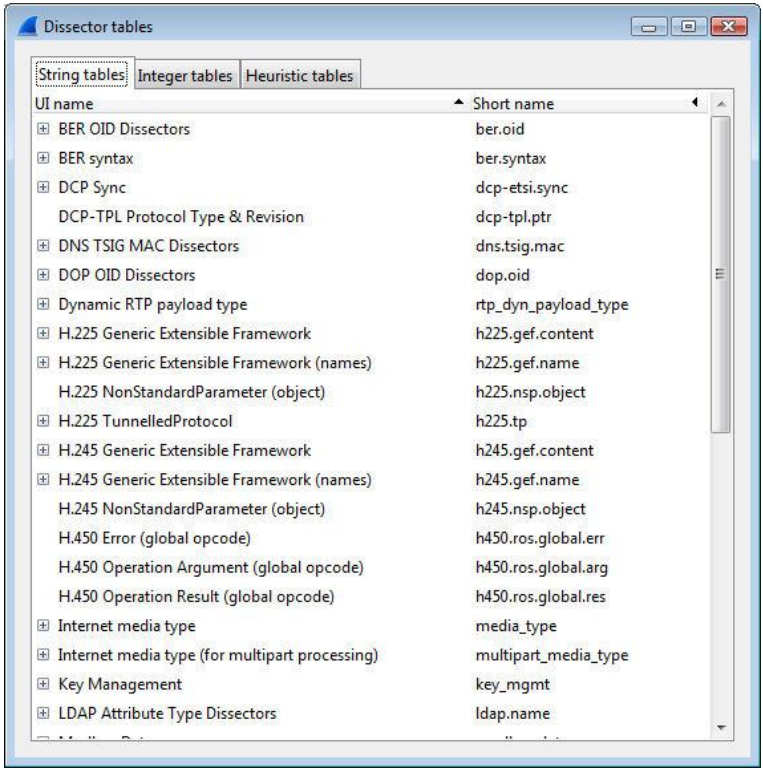


Abb. 22: Die Tabelle der Dissektoren.

- **Help**: Im letzten Menü finden Sie verschiedene Hilfen und weiterführende Informationen.

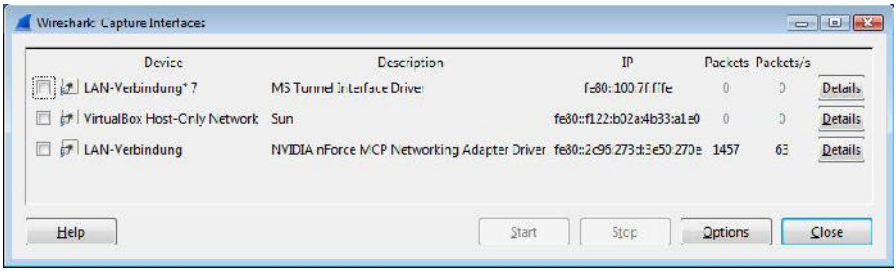
1.12 Werkzeugleiste

Während über die Menüleiste fast alle Funktionen von Wireshark zur Verfügung stehen, sind die wichtigsten Funktionen über die Symbolleiste verfügbar. Diese sind in Gruppen zusammengefasst, die ähnliche Funktionen bieten. Der erste Teil der Symbolleiste sieht wie folgt aus:

Ein Teil der Wireshark-Symbolleiste.

Mit Hilfe der Symbolleiste vereinfacht sich die Nutzung und Steuerung von Wireshark deutlich, denn Sie können schnell und einfach auf die wichtigsten Funktionen zugreifen. Die erste Funktionsgruppe bezieht sich auf das Aufzeichnen der Netzwerkaktivitäten. Die Belegung der Symbole sieht wie folgt aus:

-  - Zeigt die Schnittstellenliste an. Dabei muss es sich nicht nur um Netzwerkschnittstellen handeln. Auch Bluetooth-Schnittstellen werden angezeigt. Der Dialog erlaubt auch das Öffnen der Capture-Optionen.



Die Auswahl der Schnittstelle.

-  - Zeigt die Capture-Optionen, also die Aufzeichnungsoptionen an, über die Sie beispielsweise die Schnittstellen verwalten und die Capture-Filter bestimmen.
-  - Beginnt die Aufzeichnung entsprechend der Capture-Einstellungen.

-  - Stoppt die laufende Aufzeichnung.
-  - Startet die aktuelle Capture-Konfiguration erneut.

Es folgt als Nächstes die Funktionsgruppe mit den dateispezifischen Aktionen. Diese Funktionen erlauben insbesondere das Speichern und Öffnen von Aufzeichnungen:

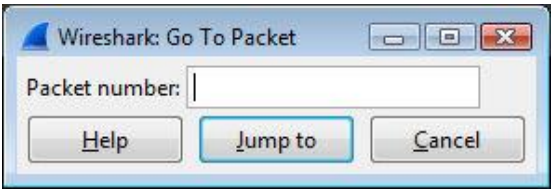
Die dateispezifischen Funktionen im Detail:

-  - Öffnet eine gespeicherte Aufzeichnung. Am Einfachsten erfolgt das Öffnen allerdings über die Startseite von Wireshark.
-  - Sichert die Aufzeichnung. Sie können dabei das Zielverzeichnis bestimmen.
-  - Schließt die aktuelle Capture-Datei. Sie können in Wireshark mehrere Aufzeichnungen gleichzeitig öffnen und ausführen.
-  - Führt einen Reload der Capture-Datei aus.

Die Navigationsfunktionen innerhalb vom Wireshark.

Die nächste Befehlsgruppe fasst die verschiedenen Funktionen für die Suche und Navigation in Ihren Aufzeichnungen zusammen. Dabei stehen Ihnen insgesamt sechs Funktionen zu Verfügung:

-  - Mit einem Klick auf dieses Symbol öffnen Sie die Suche, mit der Sie Ihre Aufzeichnungen nach Zeichenfolgen durchforsten können. Die Suche bietet Ihnen verschiedene Beschränkungsmöglichkeiten.
-  - Klicken Sie auf diese Schaltfläche, um in der History einen Eintrag zurück zu springen.
-  - Hiermit springen Sie im Verlauf einen Eintrag nach vorne.
-  - Mit einem Klick auf diese Schaltfläche öffnen Sie den Dialog *Go To Packet* und geben dann in dem Eingabefeld *Packet number* den Zahlenwert an.



Die Sprungfunktion.

-  - Um zum ersten Paket zurückzuspringen, klicken Sie auf diese Schaltfläche.
-  - Klicken Sie auf diese Schaltfläche, um zum letzten Paket in der Paketliste zu springen.

Die nächste Gruppe umfasst zwei Schaltflächen, deren Funktionen sich auf die Paketliste beziehen:

Die Funktionen für die Paketliste.

Die beiden Funktionen sind aktiviert. Die linke Funktion sorgt für die farbige Kennzeichnung der Einträge in der Paketliste. Hinter der rechten Funktion verbirgt sich die AutoScroll-Funktion, die dafür sorgt, dass die Paketliste bei der Aufzeichnung neuer Pakete automatisch nach unten scrollt.

Die vorletzte Gruppe stellt Ihnen Funktionen für die Begutachtung der Daten zur Verfügung. Sie können den aufgezeichneten Traffic, genauer die Darstellung vergrößern und verkleinern sowie die Ansicht wieder auf die Standardgröße reduzieren.

Die Vergrößerungs- und Verkleinerungsfunktion.

Mit Hilfe der beiden links befindlichen Symbole können Sie die Ansicht Ihrer Aufzeichnungen verkleinern und vergrößern. Mit der 1:1-Ansicht kehren Sie zur Ausgangsansicht zurück. Mit einem Klick auf das rechte Symbol passen Sie die Spaltenbreite an.

Es folgt die vorletzte Symbolgruppe, die Ihnen insbesondere Filter- und Capture-Einstellungen zur Verfügung stellt:

Die vorletzte Funktionsgruppe.

In dieser Gruppe stehen Ihnen folgende Funktionen zur Verfügung:

-  - Öffnet die Capture-Filtereinstellungen, über die Sie genau festlegen können, welche Filter zum Einsatz kommen sollen und welche nicht.
-  - In diesem Dialog legen Sie entsprechend fest, welche Display-Filter zum Einsatz kommen sollen.
-  - Auch diesen Dialog kennen Sie bereits: Hier bestimmen Sie die Farben, die zur Kennzeichnung der Inhalte verwendet werden.
-  - Hier finden Sie die Programmeinstellungen von Wireshark, über die Sie insbesondere die Bedieneroberfläche anpassen können.

Das letzte Symbol der Wireshark-Symbolleiste ist Ihr digitaler Rettungsanker, der die Gestaltung eines Rettungsrings besitzt. Ein Klick auf folgendes Symbol öffnet die englischsprachige Hilfe von Wireshark:

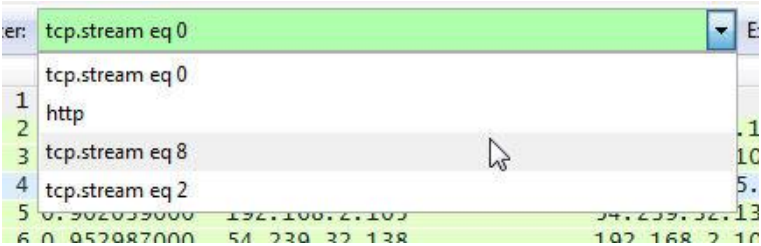
1.13 Filterfunktionen im Griff

Unterhalb der Symbolleiste finden Sie die Filterfunktionen, über die Sie die von Wireshark aufgezeichneten Informationen gezielt nach unterschiedlichen Kriterien filtern können. Damit steht Ihnen eine der wichtigsten Funktionen für das Aufspüren der gesuchten Informationen zur Verfügung. Die Filter unterstützen Sie bei der sprichwörtlichen Suche nach der Stecknadel im Heuhaufen. Wireshark sammelt nicht selten Tausende oder gar Zehn- oder Hunderttausende Datenpakete. Diese manuell zu sichten und zu analysieren ist nahezu unmöglich.

Die Filterleiste.

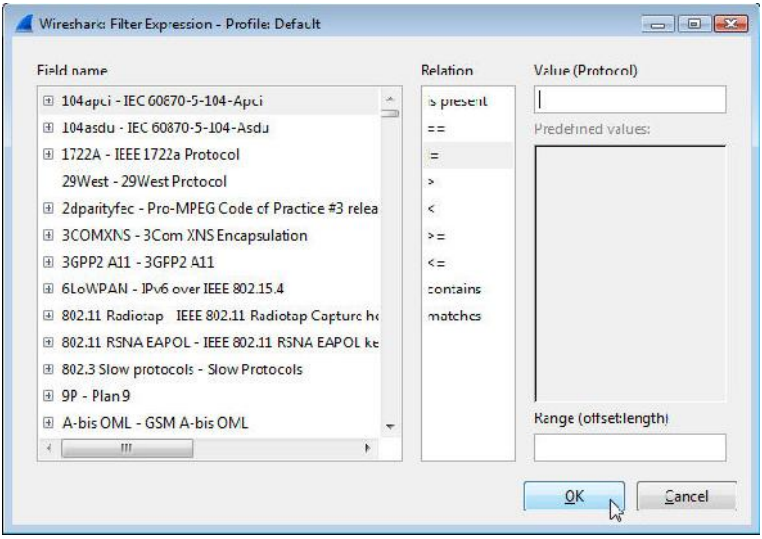
Damit Ihnen keine relevanten Informationen entgehen, müssen Sie die Filterfunktionen kennen und einzusetzen wissen. Wenn Sie beispielsweise entsprechend

obigem Beispiel den Datenverkehr analysieren wollen, können Sie einfach anderen Datenverkehr ausblenden.



Die Auswahl einer gespeicherten Filterkonfiguration.

Mit einem Klick auf *Filter* öffnen Sie den oben kurz vorgestellten Dialog der Display-Filter. Über das Auswahlmenü greifen Sie auf die gespeicherten Filter zu.



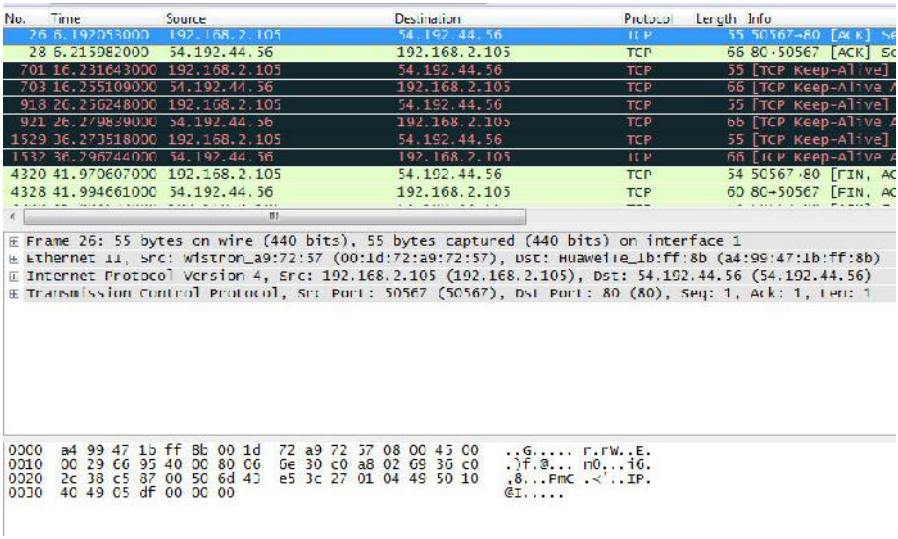
Das Anlegen von Filterausdrücken.

Rechts neben dem Auswahlmenü finden Sie weitere wichtige Filterfunktionen. Mit einem Klick auf *Expression* öffnen Sie den gleichnamigen Dialog, in den Sie Ihre

eigenen Filterausdrücke bauen können. Dabei stehen Ihnen umfangreiche Protokollauswahlmöglichkeiten zur Verfügung, die Sie mit logischen Operatoren und eigenen Wertangaben kombinieren können.

Die Filterleiste umfasst vier weitere Funktionen: Mit einem Klick auf *Clear* leeren Sie das Filterfeld und die Anzeige wird auf den Ausgangspunkt zurück versetzt. Mit *Apply* wenden Sie einen Filter an und die Darstellung wird entsprechend der Filterkonfiguration eingeschränkt.

Sie können auch sehr bequem eine neue Filterkonfiguration zur späteren Wiederverwendung sichern. Dazu klicken Sie auf *Save*. Schließlich wenden Sie den letzten Eintrag aus dem Auswahlmenü mit einem Klick auf *Filter* an.



Die drei Infobereiche Paketliste, Detailansicht und Byte-Ansicht.

1.14 Die Ansichten im Detail

Unterhalb der Symbol- und Filterleiste finden Sie die eigentlichen Daten, die Wireshark aufgezeichnet hat und die Sie dann analysieren können. Von oben nach unten präsentiert Ihnen Wireshark die Paketliste, gefolgt von der Detailansicht und der Byte-Ansicht. Auch diese Ansichten und die darin verfügbaren Funktionen sollten Sie kennen und soweit es sinnvoll und notwendig ist, sich darin zielgerichtet bewegen können.

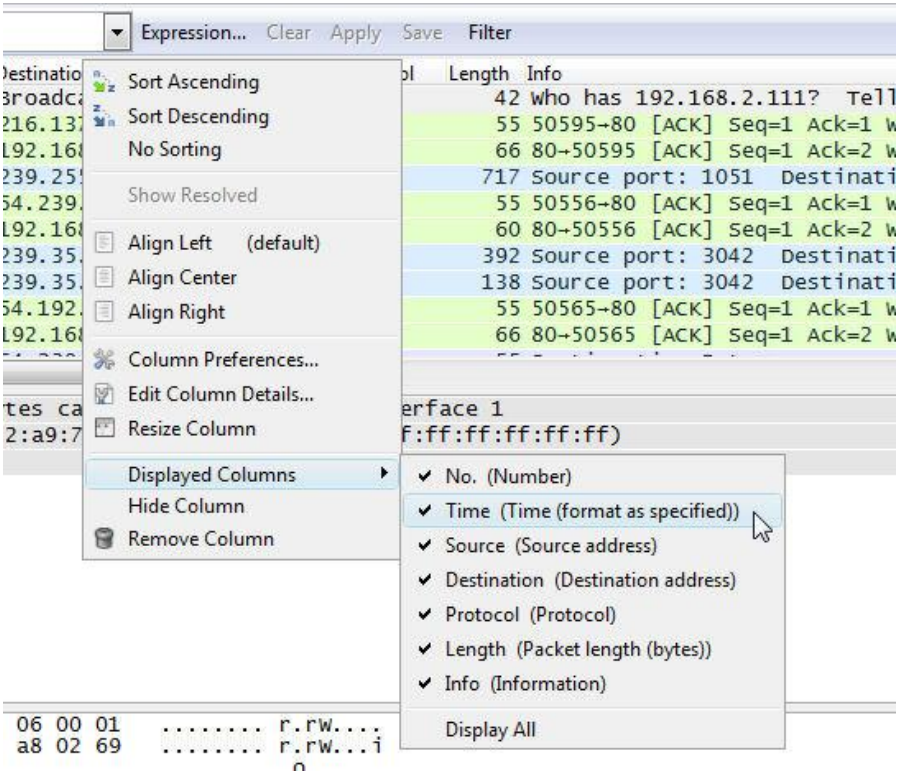
In der Paketansicht können Sie sich schnell und einfach durch die Paketliste bewegen und sich einen ersten Überblick verschaffen, welche Hosts miteinander kommuniziert haben. Sie können dieser Übersicht auch entnehmen, welche Programme dabei zum Einsatz kamen.

In der Paketliste werden standardmäßig sieben Spalten mit Informationen angezeigt. Standardmäßig sind alle sieben Spalten aktiviert, können aber auch gezielt ein- und ausgeblendet werden. In der Paketliste finden Sie die folgenden Spalten:

- **Spaltennummer**: Wireshark nummeriert die Frames der Reihe nach durch. Die Frames werden standardmäßig in der durchnummerierten Abfolge aufgelistet. Sie können die Reihenfolge leicht ändern, indem Sie in die Spaltenüberschrift klicken.
- **Zeit**: Die zweite Spalte trägt die Bezeichnung *Time* und führt die Frames in chronologischer Reihenfolge der Aufzeichnung auf. Dabei wird nicht der aktuelle Zeitpunkt verwendet, sondern die Reihenfolge beginnt beim Wert 0.0. Zu allen nachfolgenden Frames wird dann das Zeitintervall seit Beginn der Aufzeichnung aufgeführt. Auch in dieser Spalte können Sie die Reihenfolge mit einem Klick auf den Spaltenkopf umkehren.
- **Quelle**: Dieser Spalte können Sie die Adresse der höchsten verfügbaren Netzwerkschicht eines Frames entnehmen, das von der Quelle aus versendet wurde. Meist handelt es sich dabei um die IP-Adresse, aber manchmal kann auch nur die MAC-Adresse identifiziert werden.
- **Ziel**: Zu jeder Quelle gehört auch ein Ziel. Dieser Spalte entnehmen Sie die Zieladressen der übermittelten Frames. Auch hier werden entweder IP- oder MAC-Adressen eingeblendet. Wie Sie obiger Abbildung entnehmen können, werden bei dieser Beispielaufzeichnung immer IP-Adressen angezeigt.
- **Protokoll**: In der vierten Spalte wird das verwendete Protokoll aufgeführt, das für die Übermittlung der Daten-Frames verwendet wurde. Dabei werden die oben erwähnten Dissektoren verwendet. Diese Spalte ist hilfreich, um die Ansicht nach bestimmten Daten-Traffics zu sortieren.
- **Länge**: In der Spalte *Length* wird die Gesamtlänge der Daten-Frames aufgeführt. So erkennen Sie schnell, ob bestimmte Anwendungen kleine oder eher größere Datenpakete transferieren.
- **Info**: In der siebten und letzten Spalte werden ergänzende Informationen zu den Frames aufgeführt. Dort können Sie beispielsweise schnell und einfach erkennen, ob es sich um DNS-Abfragen oder HTTP-Requests handelt.

Wie bereits erwähnt, können Sie die Spalten mit einem Klick auf den Spaltentitel neu sortieren. Haben Sie die Sortierung mit einem Klick geändert, können Sie sie mit einem erneuten Klick wieder rückgängig machen.

Sie können auch die Spaltenreihenfolge ändern. Dazu klicken Sie auf einen Spaltenkopf und ziehen diesen mit gedrückter linker Maustaste an die neue Position. Sie können auch einzelne oder auch mehrere Spalten ausblenden.

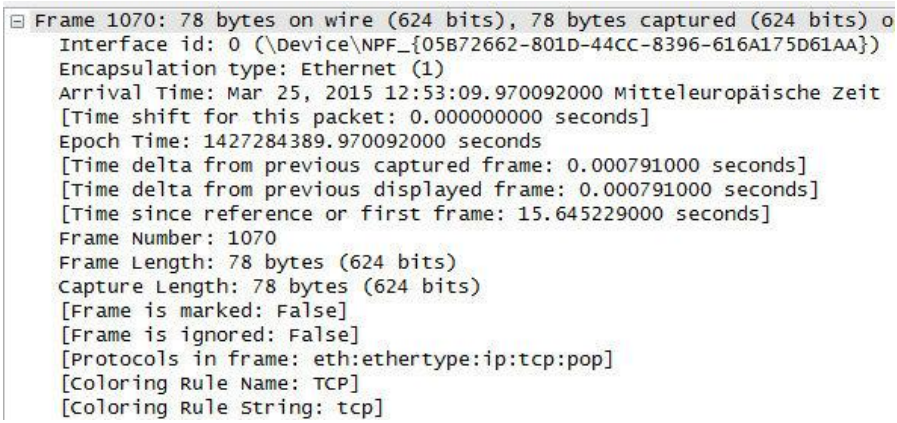


Das Ein- und Ausblenden von Spalten.

Sie können eine einzelne Spalte einfach ausblenden, indem Sie den Spaltenkopf mit der rechten Maustaste markieren und dann aus dem Kontextmenü den Befehl *Hide Column* ausführen. Mit Hilfe des Untermenüs *Displayed Column* können Sie gezielt weitere Spalten aus- und wieder einblenden. Ich hatte es oben bereits angedeutet: Sie können mit Hilfe der rechten Maustaste und den zugehörigen Pop-up-

Menüs viele interessante und nützliche Funktionen ausführen. Wir kommen im weiteren Verlauf immer wieder auf diese Möglichkeiten zu sprechen.

Die verschiedenen Ansichten und Listen sind in Wireshark interaktiv miteinander verknüpft. Wenn Sie in der Paketliste einen Eintrag markieren, werden in der darunter befindlichen Detailansicht die Feinheiten eines Frames bzw. Pakets angezeigt. Sie sollten sich bei der Navigation in den Aufzeichnungen immer wieder in Erinnerung rufen, dass es sich bei der Frame-Sektion um Wireshark-spezifische Daten handelt, und diese nicht Teil des Datenpakets sind, die Sie aufgezeichnet haben. Mit der Frame-Sektion fügt der Sniffer Informationen über einen Frame hinzu, die für eine spätere Datenanalyse hilfreich sein können.

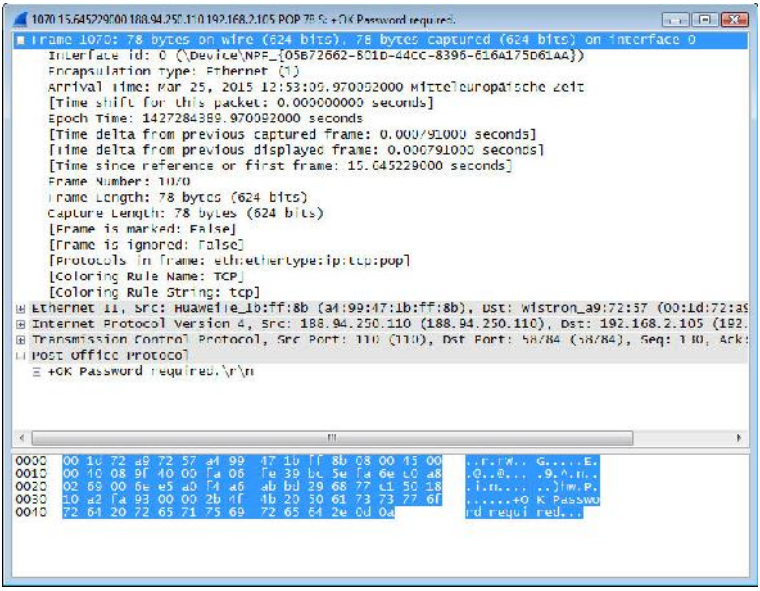


Die typischen Meta-Informationen eines Wireshark-Frames.

Mit einem Klick auf ein Pluszeichen öffnen Sie in der Detailansicht beispielsweise die Daten des Frame-Knotens. Voranstehende Abbildung zeigt die typischen Daten und Informationen, die Sie in einem Frame-Eintrag finden. Es handelt sich bei diesen Daten um Meta-Informationen, die die Aufzeichnungen erweitern.

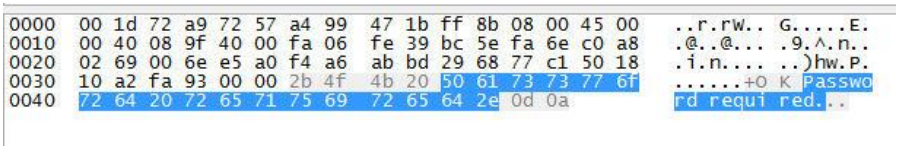
Mit Hilfe des Kontextmenüs der rechten Maustaste können Sie verschiedene weitere Aktionen ausführen. Mit *Expand All* können Sie beispielsweise alle eingeklappten Informationen ausklappen. Mit *Collapse All* können Sie die Baumansicht wieder zusammenfalten. Mit den beiden Befehlen *Expand Subtrees* und *Collapse Subtrees* können Sie die markierten Äste auf- und einklappen.

Sie vereinfachen sich die Analyse, indem Sie mit einem Doppelklick auf einen Eintrag in der Paketliste klicken und diesen so in einem eigenen Fenster öffnen. Somit können Sie ein Paket einfacher unter die Lupe nehmen.



Ein Datenpaket wurde in einem eigenen Fenster geöffnet.

Am unteren Ende des Dialogs finden Sie die sogenannte Byte-Ansicht, die Ihnen die Inhalte der Datenpakete als Hexadezimalcode oder als ACSII-Zeichen anzeigt. Mit einem Rechtsklick in die Ansicht können Sie zwischen den beiden Ansichten wechseln.

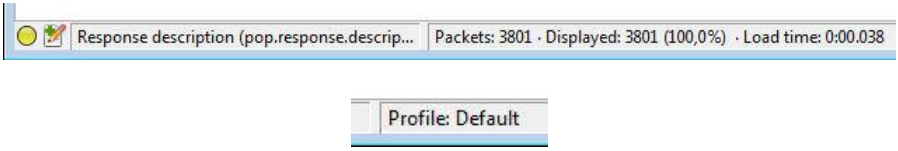


Die Byte-Ansicht erlaubt tiefe Einblick in den Datentransfer.

Durch Markieren von Inhalten kennzeichnet Wireshark die zugehörigen Daten. Sie können die Byte-Ansicht prinzipiell auch über die Programmeinstellungen deaktivieren, doch macht das in der Regel wenig Sinn.

1.15 Die Statusleiste

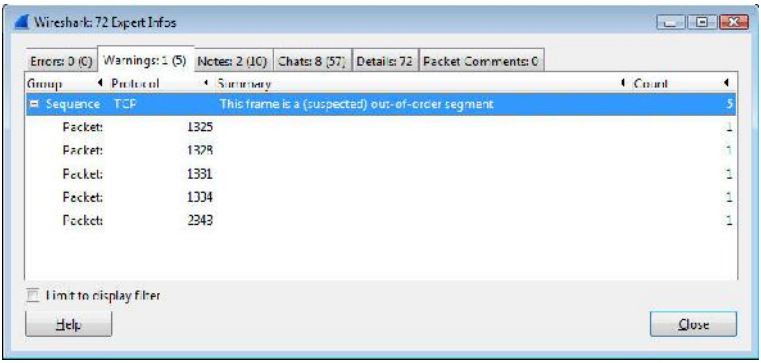
Den Abschluss nach unten hin bildet die Statusleiste, der Sie verschiedene Statusinformationen entnehmen können. Die Statusleiste umfasst mehrere Infobereiche und auch zwei Schaltflächen.



Die Funktionen der Statusleiste.

Hinter dem Kreis links verbergen sich die Experteninfos. Mit einem Klick öffnen Sie den Dialog *Expert Infos*, der eine Art Protokoll von Anomalien führt, die Wireshark bei der Aufzeichnung identifiziert hat. Der Gedanke dahinter: Dem Anwender sollen Auffälligkeiten einfach zugänglich gemacht werden. Durch die gebündelte Zusammenfassung von möglichen Netzwerkproblemen ist es für Netzwerkadministratoren einfacher, diesen auf den Grund zu gehen.

Sie sollten dabei beachten, dass es sich hierbei um eine Zusatzinfo handelt. Aber der Umkehrschluss gilt nicht: Gibt die Experteninfo keine Hinweise aus, bedeutet das noch lange nicht, dass es nicht doch welche gibt.



Die Experteninfos weisen Sie auf Anomalien hin.

Wir kommen später noch einmal auf diese Funktion zu sprechen. Anhand des voranstehenden Beispiels können Sie sehr schön erkennen, dass dieses Paket eine Warnung aufweist. Derlei Warnungen gilt es zu untersuchen und ihnen nachzugehen.

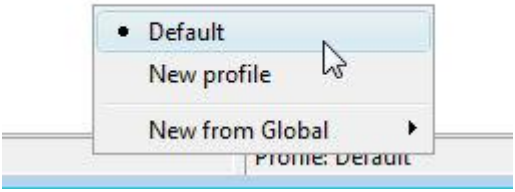
Das Hinzufügen von Kommentaren.

Wenn Sie Ihre Aufzeichnung im PCAPNG-Format speichern, können Sie diese immer auch um Notizen erweitern. Dazu klicken Sie auf das zweite Symbol in der Statusleiste. In einem einfachen Editor-Fenster können Sie Ihre Anmerkungen zu einer Aufzeichnung hinterlegen.

In der Statusleiste folgen zwei Infobereiche, die Ihnen Informationen über die Datenfelder und die Anzahl der Pakete liefern. Wenn Sie eine Aufzeichnung gespeichert haben, können Sie diesem Bereich den Speicherort der Datei entnehmen. Die Trennlinie zwischen diesen beiden Bereichen können Sie verschieben. Wenn Sie die Trennung verschieben, können Sie dem linken Bereich außerdem die Größe der Aufzeichnungen und die Länge entnehmen.

Im rechten Bereich können Sie die Anzahl der Pakete ersehen, die in der geöffneten Capture-Datei enthalten sind. Sollten Sie die Ansicht über Filter eingeschränkt haben, finden Sie auch die Zahl der dargestellten Pakete. Außerdem können Sie diesem Bereich die Ladezeit entnehmen.

Rechts finden Sie dann noch die Profilauswahl. In Profilen sind die Voreinstellungen und Sniffer-Konfigurationen hinterlegt, die Sie beispielsweise für verschiedene Analyseaufgaben anwenden können. Ihre Wireshark-Installation verfügt über ein Standardprofil. Wie wir später noch sehen werden, stellt Ihnen Wireshark eine Profilverwaltung zur Verfügung, mit der Sie weitere Profile anlegen können.



Die Profilauswahl von Wireshark.

Index

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

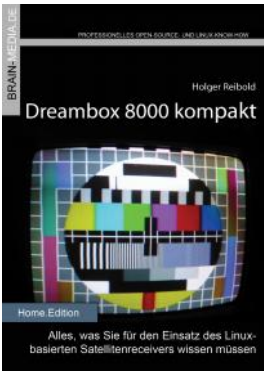
V

W

X

Z

Weitere Brain-Media.de-Bücher



Dreambox 8000 kompakt

Die Dreambox 8000 stellt ihre Vorgänger allesamt in den Schatten. Was Sie alles mit der Dreambox 8000 anfangen können, verrät Ihnen die Neuauflage unseres Dreambox-Klassikers. Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

Umfang: 450 Seiten plus CD
ISBN: 978-3-939316-90-9
Preis: 29,80 EUR

Scribus 1.4 kompakt

Scribus ist längst ein ebenbürtiger Gegenspieler von InDesign & Co. In unserem Handbuch erfahren Sie alles, was Sie für den erfolgreichen Einstieg wissen müssen. Auf über 450 Seiten lernen Sie nahezu jede Programmfunktion kennen. Praxisbezogene Beispiele zeigen, wie Sie mit Scribus schnell ans Ziel gelangen.

Umfang: 465 Seiten plus DVD
ISBN: 978-3-939316-91-6
Preis: 29,80 EUR

X-Plane 10 kompakt

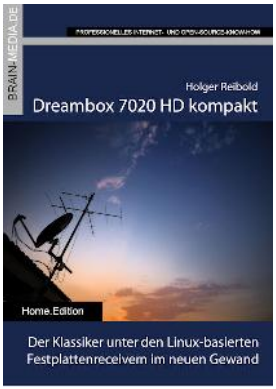
Der Klassiker unter den Flugsimulatoren geht in die zehnte Runde. Viele neue Funktionen und verbessertes Handling warten auf die Anwender. Kein Wunder also, dass die Fangemeinde wächst und wächst. Unser Handbuch beschreibt alles, was Sie für das Fliegen mit X-Plane wissen sollten.

Umfang: 430 Seiten
ISBN: 978-3-939316-96-1
Preis: 24,80 EUR

Audacity 2.0 kompakt

Audacity ist zweifelsohne das beliebteste freie Audioprogramm. Vom anfänglichen Geheimtipp hat sich der Editor zum Standard für die Aufzeichnung und Bearbeitung von Audiodaten gemausert. Das Vorwort steuert der ehemalige Core-Entwickler Markus Meyer bei.

Umfang: 306 Seiten
ISBN: 978-3-95444-027-6
Preis: 24,80 EUR



Dreambox 7020 HD kompakt

Der Klassiker im neuen Gewand: Die Dreambox 7020 HD besticht durch das OLED-Display an der Front sowie ihr flexibles Tuner-Konzept. In diesem Handbuch lernen Sie die vielfältigen Einsatzmöglichkeiten der Box kennen. Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

Umfang: 430 Seiten
ISBN: 978-3-939316-99-2
Preis: 24,80 EUR

Evernote kompakt

Bei der alltäglichen Informationsflut wird es immer schwieriger, Wichtiges von Unwichtigem zu trennen, Termine und Kontakte zu verwalten. Mit Evernote können Sie diese Flut bändigen und Ihren Alltag optimieren. "Evernote kompakt" vermittelt das notwendige Know-how für den Einsatz von Evernote auf Ihrem Desktop, Smartphone und online.

Umfang: 320 Seiten
ISBN: 978-3-95444-098-6
Preis: 22,80 EUR

Fire TV kompakt

Mit Fire TV hat Amazon eine tolle kleine Box für das Online-Entertainment auf den Markt gebracht, die für wenig Geld die gesamte Palette der Internet-basierten Unterhaltung abdeckt. In diesem Handbuch erfahren Sie, was Sie alles mit der kleinen Box anstellen können.

Umfang: 182 Seiten
ISBN: 978-3-95444-172-3
Preis: 16,80 EUR

Magento SEO kompakt

Magento ist die Standardumgebung für den Aufbau eines Online-Shops. Doch damit Sie mit Ihren Shop-Angebot auch im Internet wahrgenommen werden, müssen Sie ein wenig die Werbetrommel rühren und den Shop für Google & Co. optimieren. Mit wenigen Handgriffen machen Sie Ihren Online-Shop SEO-fest und maximieren Ihre Verkäufe.

Umfang: 100 Seiten
ISBN: 978-3-95444-098-6
Preis: 14,80 EUR

Weitere Titel in Vorbereitung

Wir bauen unser Programm kontinuierlich aus. Aktuell befinden sich folgende Titel in Vorbereitung:

- Android Forensik
- Android Security
- Papierloses Büro
- Alfresco kompakt

Plus+

Plus+ − unser neues Angebot für Sie ... alle E-Books im Abo. Sie können 1 Jahr lang alle Brain-Media-Bücher als E-Book herunterladen und diese auf Ihrem PC, Tablet, iPad und Kindle verwenden − und das ohne irgendwelche Einschränkungen. Das Beste: Plus+ schließt auch alle jene Bücher ein, die in diesem Jahr noch erscheinen.

Und das zum Sonderpreis von 29 Euro! Ein unschlagbares Angebot!

Auf unserer Website steht ein detaillierter Überblick aller Titel im PDF-Format zum Download bereit (ca. 6,2 MB), der bereits zu Plus+ gehörende Titel aufführt und die in naher Zukunft hinzukommen.