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.

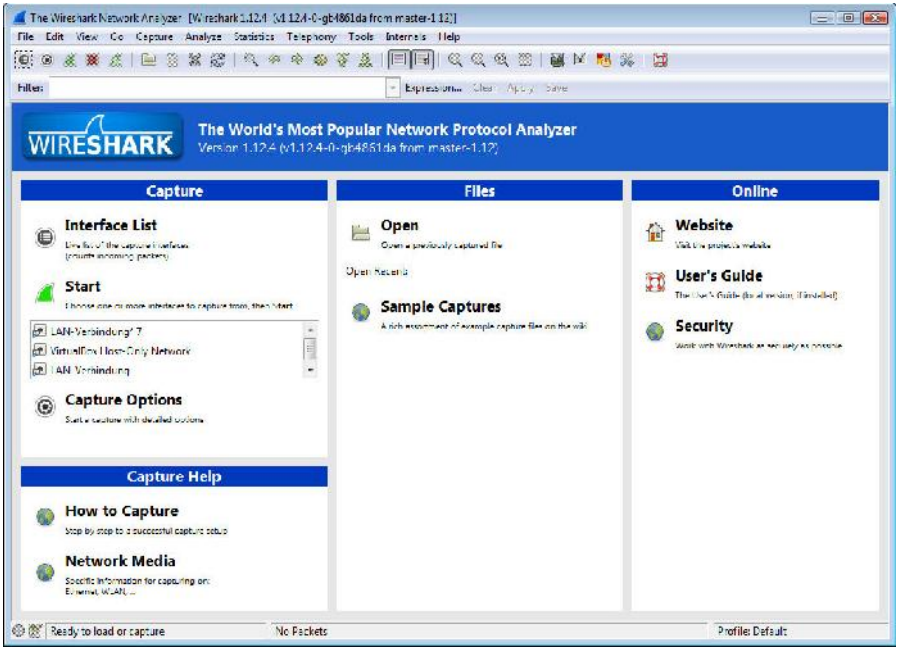
1.1 Wireshark kennenlernen

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
```

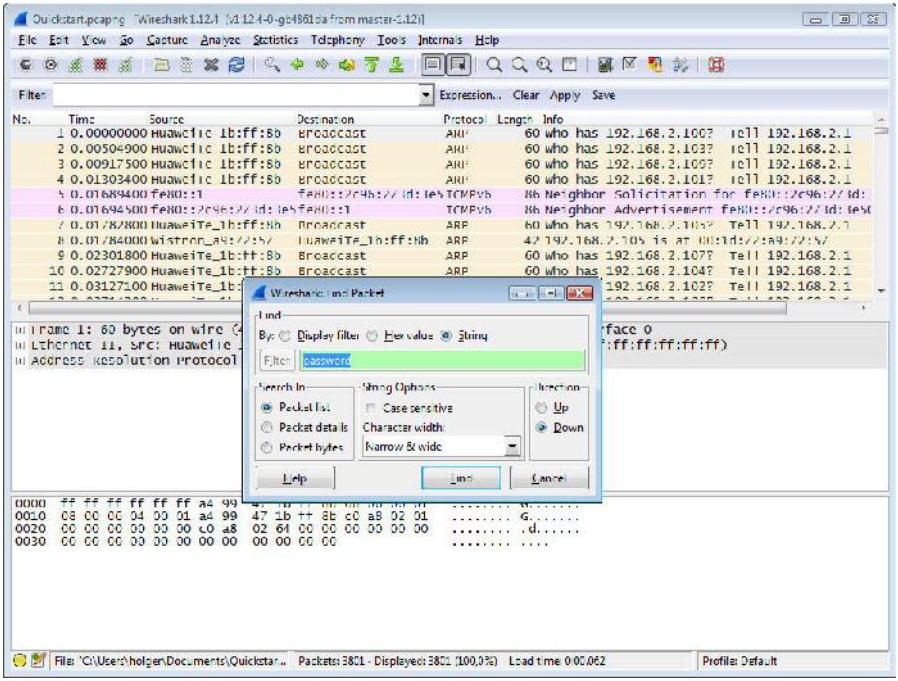
Die besagt, dass der Treiber für die Netzwerkschnittstellen nicht geladen werden konnte. Die Lösung ist einfach: Starten Sie Wireshark als Administrator. Dazu markieren Sie den Wireshark-Eintrag in der Schnellstart- oder Taskleiste mit der rechten Maustaste und führen den Befehl *Als Administrator ausführen*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

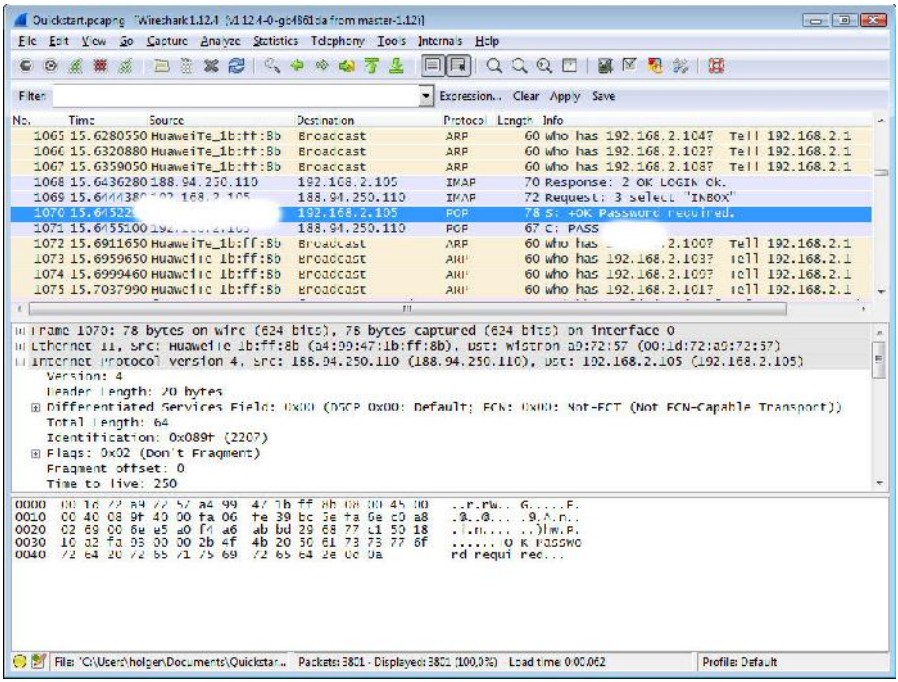
Um die Suche zu öffnen, führen Sie die Tastenkombination *Strg + N* aus. Wireshark präsentiert Ihnen den Suchdialog, der Ihnen verschiedene Suchoptionen und -parameter anbietet. Im Bereich *By* verwenden wir in diesem Quickstart die Option *String*, um eine bestimmte Zeichenfolge zu suchen.

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

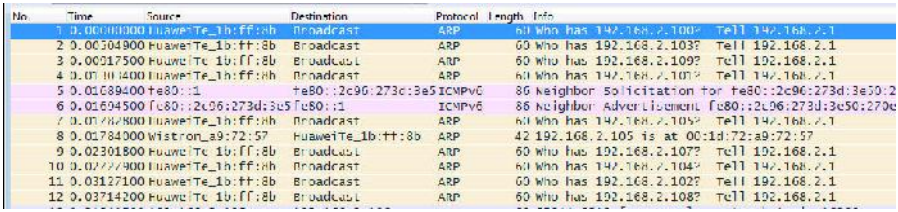
Bevor wir uns den weiteren Möglichkeiten widmen, die Wireshark bietet, möchte ich noch kurz auf die wesentlichen Bedienelemente der Benutzeroberfläche zu sprechen kommen.

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.

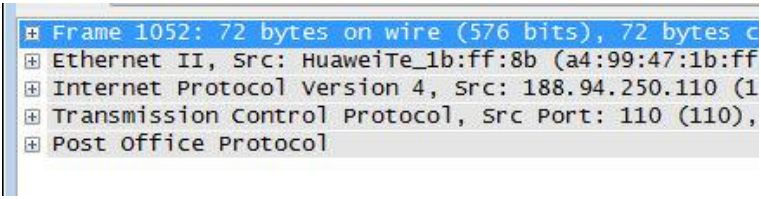
In der sogenannten Paketliste werden die aufgezeichneten Pakete aufgeführt. In der Liste werden die Pakete durchnummeriert und mit einem Zeitstempel versehen. Der Zeitstempel beginnt dabei mit dem Wert 0, der den Beginn der Aufzeichnung markiert. Die Paketliste führt folgende Spalten auf:

- Quelle
- Ziel
- Protokoll
- Länge

- Informationen

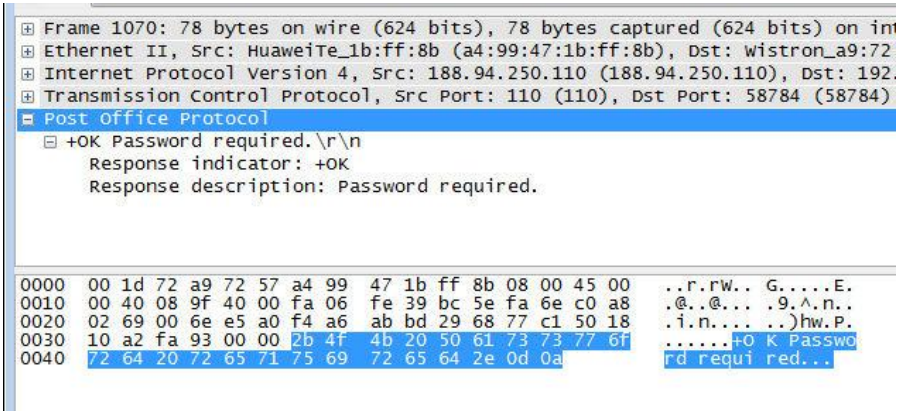
Über die Spaltenköpfe können Sie die Listeneinträge sortieren und somit beispielsweise die Darstellung nach den Zielsystemen sortieren.

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.

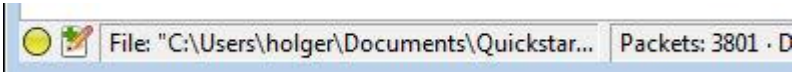
Es folgt die Byte- bzw. Rohdatenansicht. In dieser Ansicht können Sie die Informationen, die in den Paketen enthalten sind, in hexadezimaler und ASCII-Ansicht einsehen.



Die Paketdetails und die Rohdatenansicht.

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

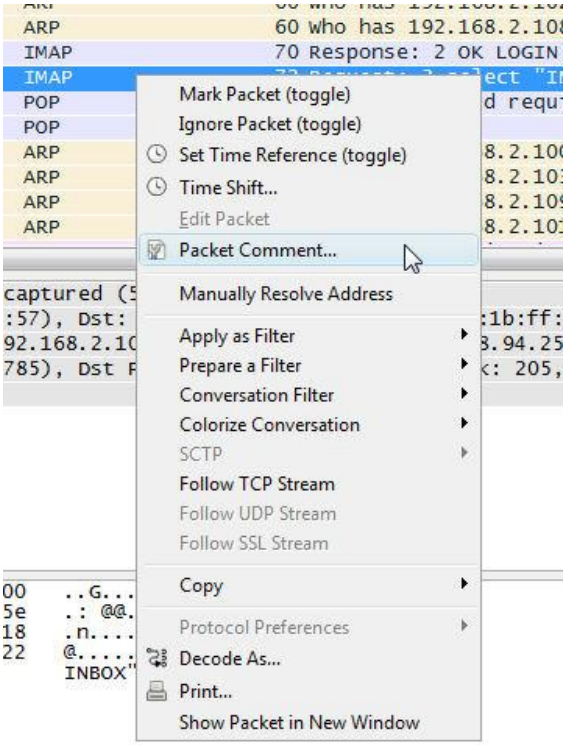
Insbesondere in der ASCII-Datendarstellung können Sie die übermittelten Informationen einsehen. Wie wir im weiteren Verlauf noch sehen werden, können Sie innerhalb der Programmoberfläche eine Fülle weiterer Funktionen ausführen.



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

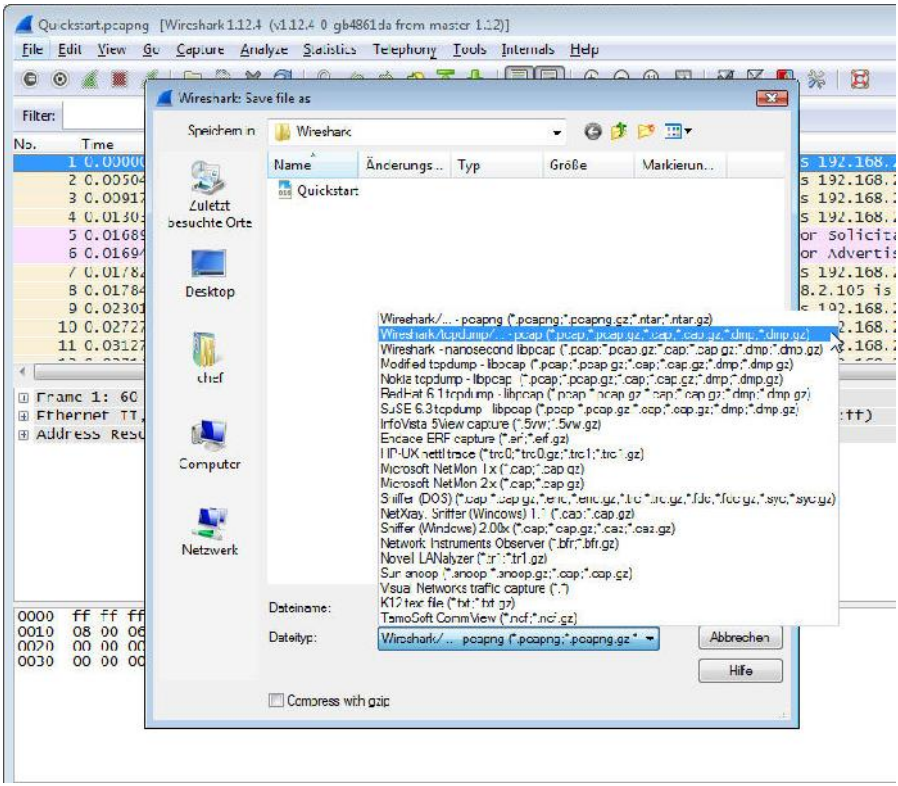
Wireshark ist laut der Website SecTools.org das beliebteste Sicherheitswerkzeug – noch weit vor anderen namhaften Tools. Laut Angaben der Entwickler wird der Sniffer Monat für Monat über 500.000 Mal von der Projekt-Site heruntergeladen. Dabei sind nicht die Downloads mitgezählt, bei denen Wireshark ein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

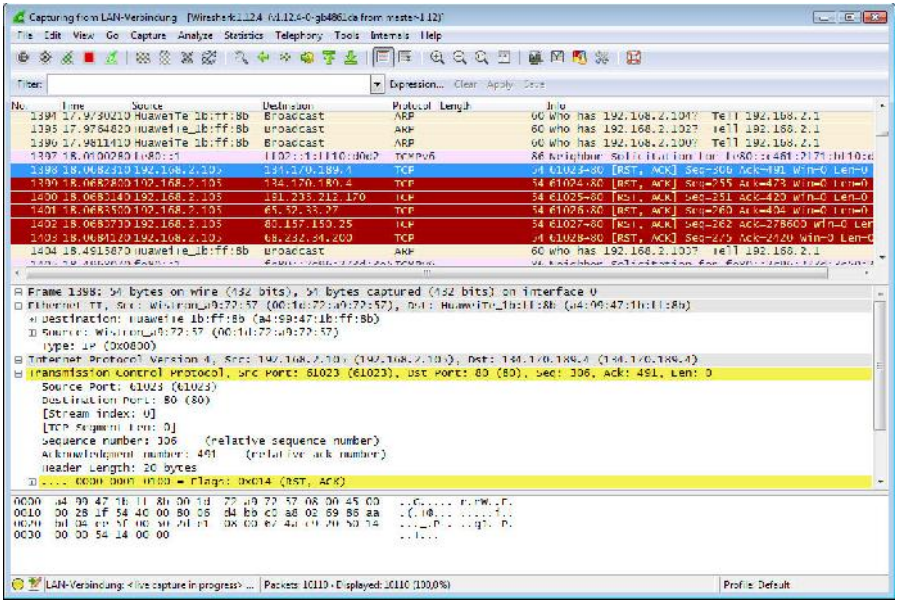
Da die drahtlose Kommunikation längst ein essentieller Bereich der Netzwerkkommunikation ist, müssen Sie wissen, welche Rechner sich Zugang zu Ihrem Netzwerk verschaffen wollen. Auch das kann Wireshark für Sie ermitteln.

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.

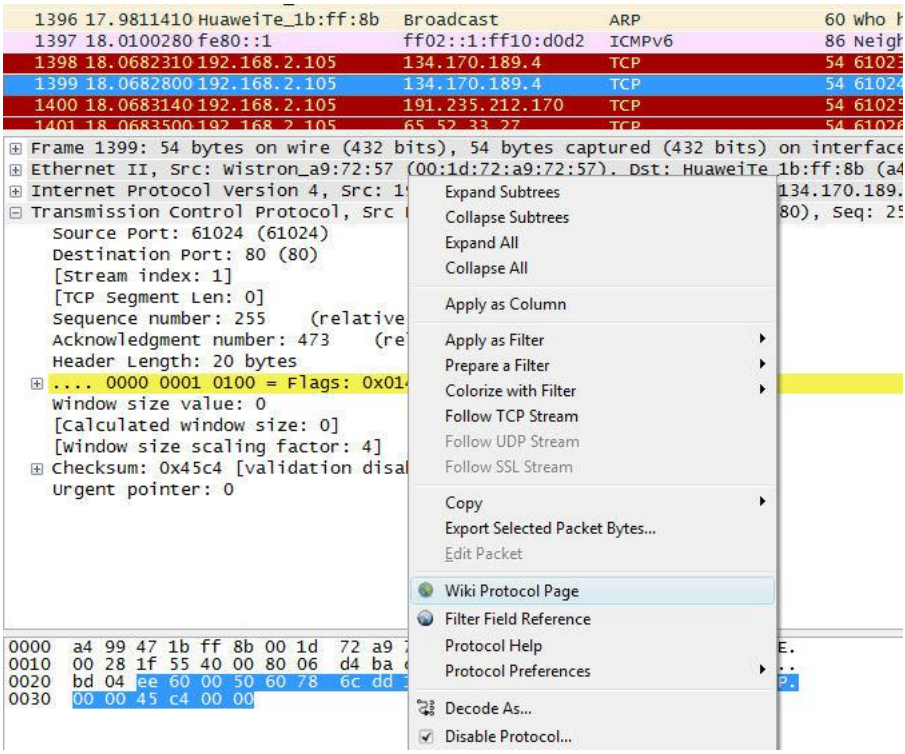
Eine der beliebtesten Aktionen für den Einstieg in Wireshark ist die Aufzeichnung des Traffics im eigenen Netzwerk in Ruhezustand, also dann, wenn keine Clients oder Server in irgendeiner Form aktiv sind. Sie werden nicht schlecht staunen, wie hoch dieses „Grundrauschen“ Ihres Netzwerks ist. Wir kommen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



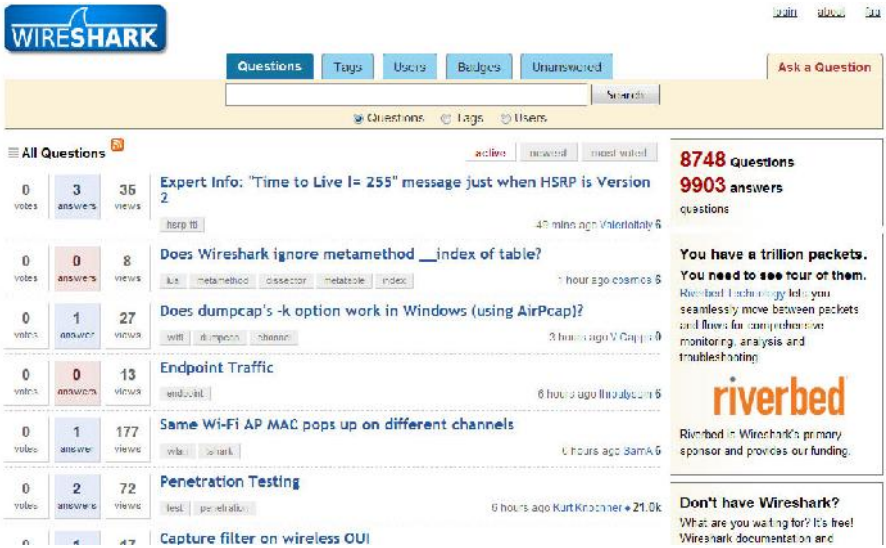
Wireshark unterstützt Einsteiger und Profis durch die Wiki-Integration gleichermaßen.

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.

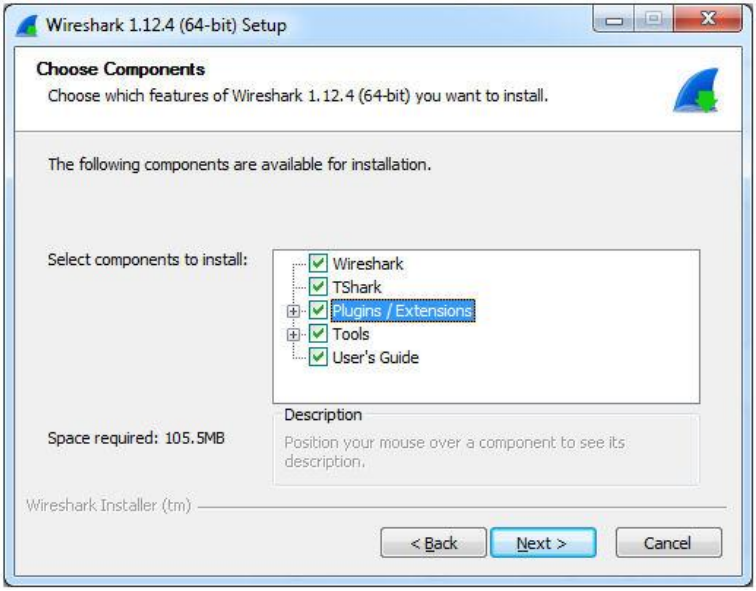
Auch die Darstellung, welche Benutzer welches Programm verwenden, beherrscht Wireshark. Last but not least können Sie mit Wireshark ausfindig machen, wie Programme beispielsweise die Transportprotokolle TCP und UDP verwenden.

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.

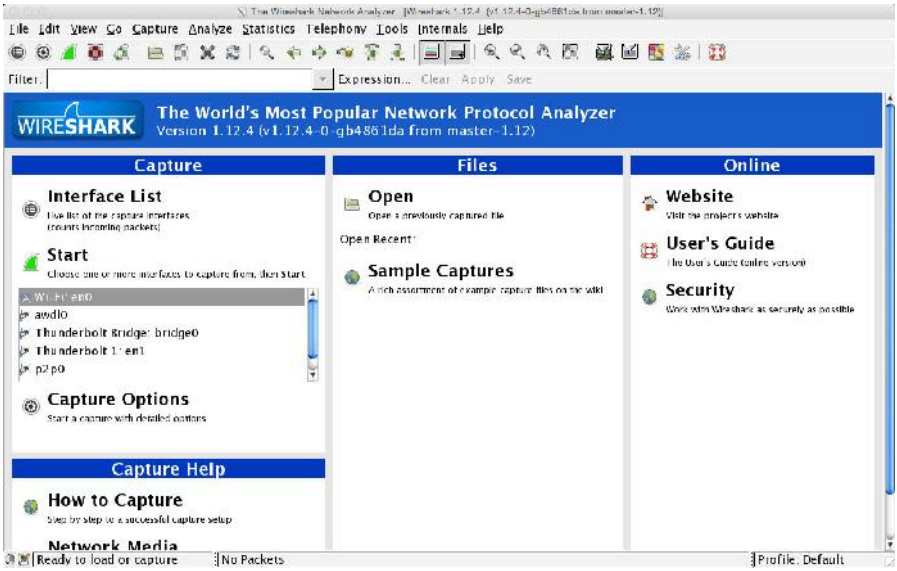
Bestimmen Sie im nächsten Dialog, welche Systemverknüpfungen Sie anlegen wollen und mit welchen Dateierweiterungen Sie den Sniffer verknüpfen wollen.

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.

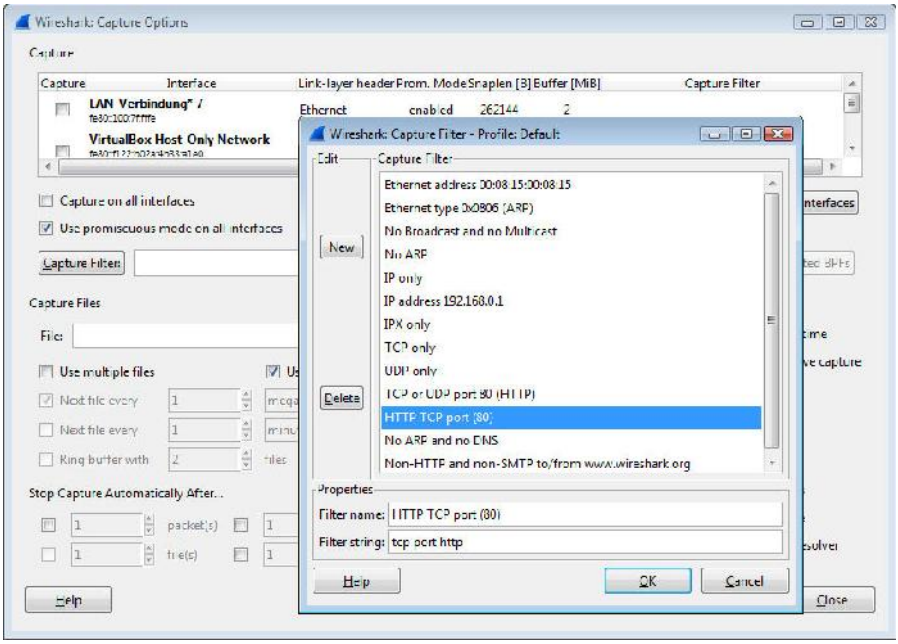
In der Praxis verwendet Wireshark für das Einlesen des Traffics die beiden Treiber WinPcap und libpcap. WinPcap ist die Windows-Variante des Pcap-Treibers, die Bibliothek libpcap kommt bei unixartigen Betriebssystemen zum Einsatz.

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

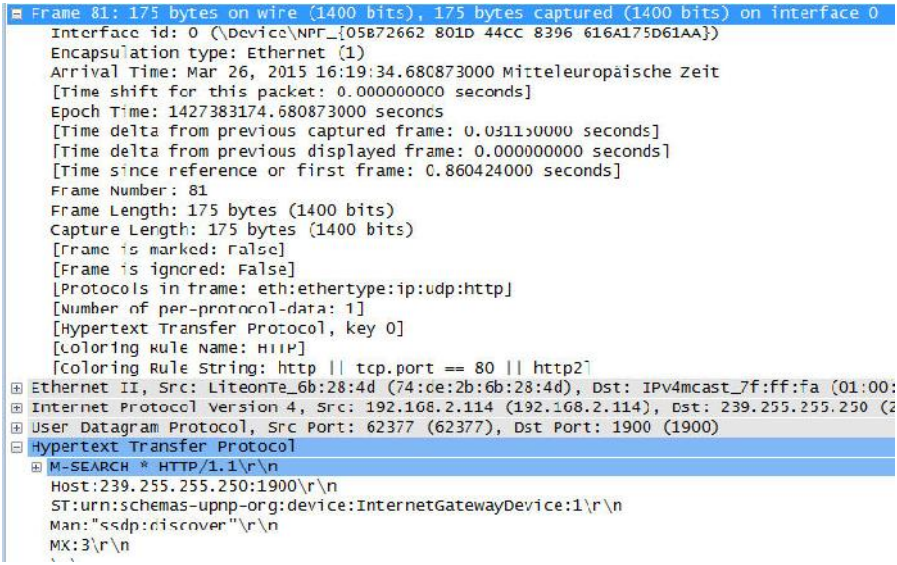
Die Capture Filter kommen auf der netzwerknahen Ebene zum Einsatz und erlauben es Ihnen, den aufzuzeichnenden Traffic frühzeitig einzuschränken. Sie können die Aufzeichnung beispielsweise auf diesem Weg auf IP- oder HTTP-Traffic begrenzen.



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.

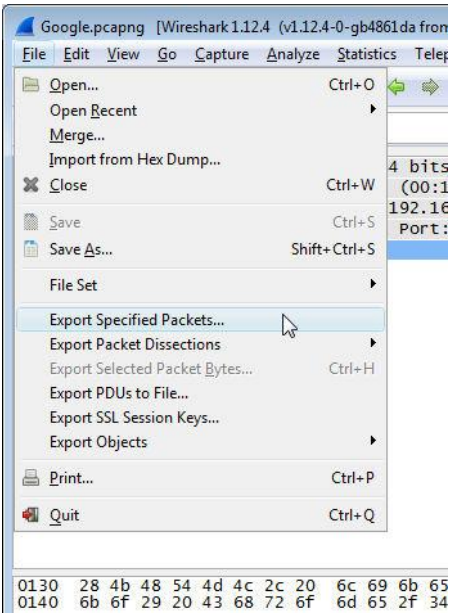
Der Frame, von dem wir hier sprechen, beginnt in obigem Beispiel erst mit dem zweiten Eintrag *Ethernet II*. Alle Informationen oberhalb dieses Elements sind Wireshark-eigene Metadaten. Unser Frame umfasst alle weiteren Inhalte bis einschließlich dem Hypertext Transfer Protocol-Knoten.

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.

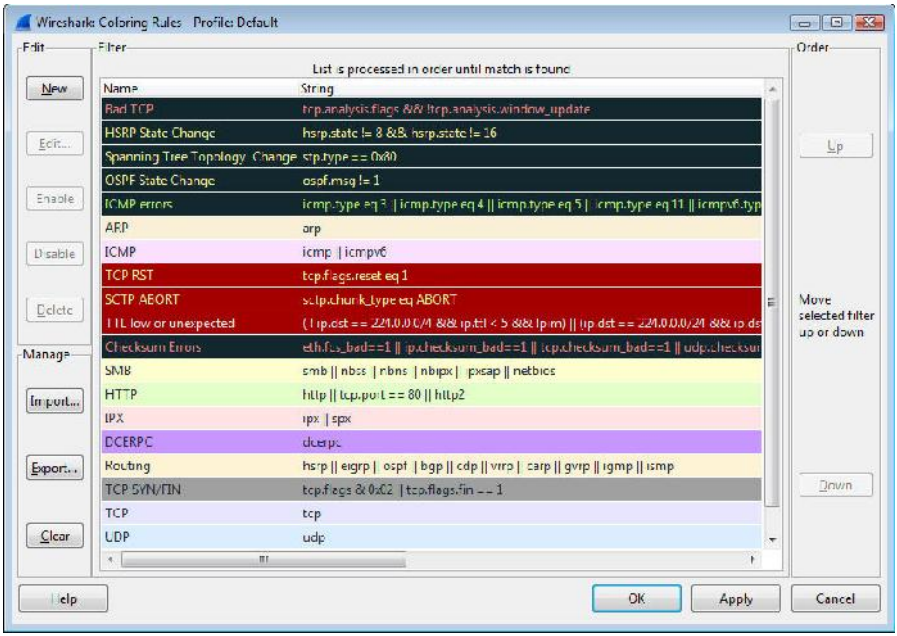
In diesem kleinen Workshop verwenden wir einen Browser, steuern Google an und führen eine Suche mit einem Suchbegriff durch. Dazu starten Sie in Wireshark eine neue Capture-Session, starten dann einen Browser und steuern damit Google an. Im Browserfenster geben Sie dann einen beliebigen Suchbegriff ein.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



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

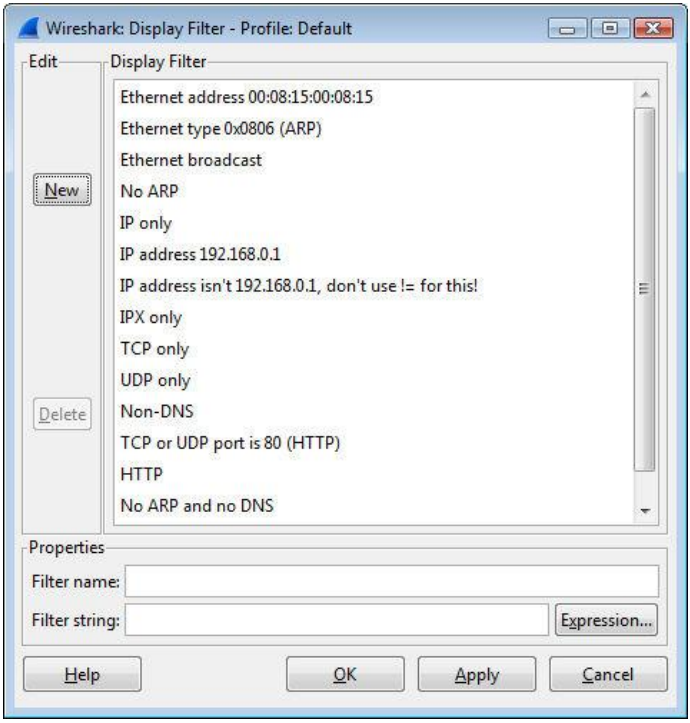
Diese Aktionen sind bislang nichts Neues für Sie, aber um ein Maximum aus dem Programm herausholen, sollten Sie insbesondere mit den wichtigsten Funktionen und Bedienelementen vertraut sein. Das Hauptmenü stellt Ihnen folgende Funktionen zur Verfügung:

- **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.

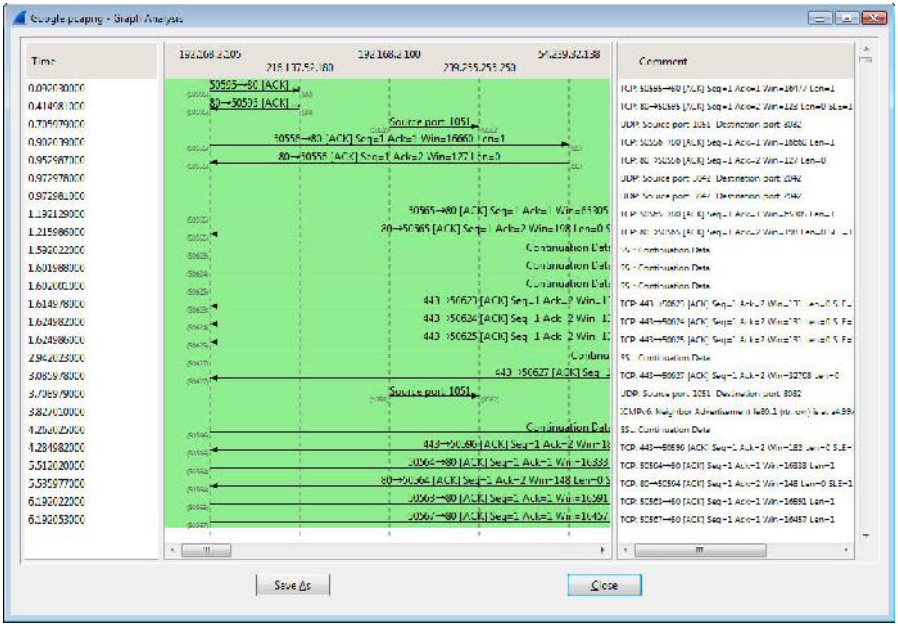
- **Go**: Dieses Menü dient der Navigation in den zu analysierenden Daten. Sie können dabei insbesondere von Paket zu Paket springen.
- **Capture**: Die Funktionen dieses Menüs dienen insbesondere der Auswahl und Konfiguration der zu überwachenden Schnittstellen. Sie können aber auch die Capture-Optionen 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.

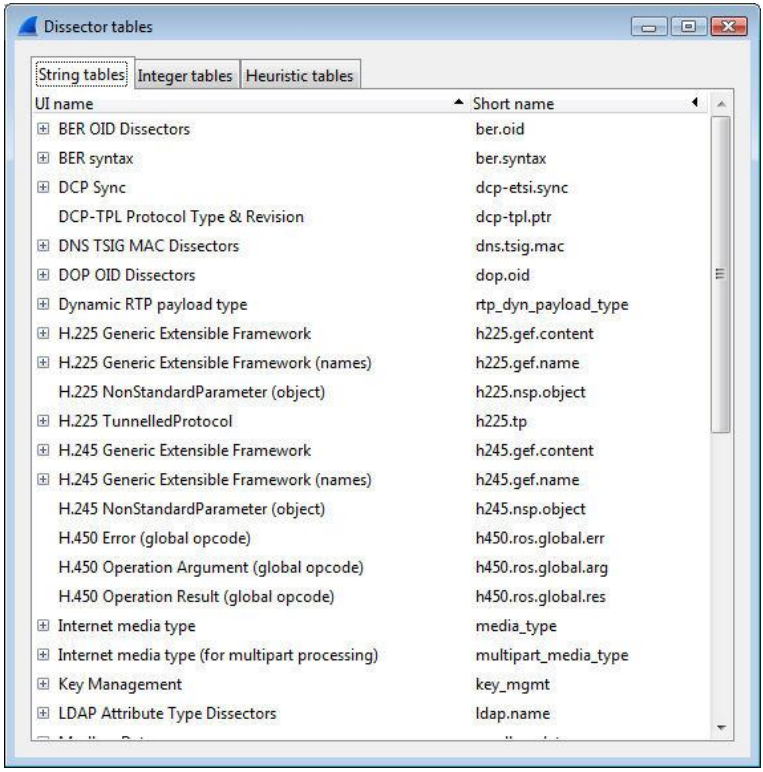


Abb. 22: Die Tabelle der Dissektoren.

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

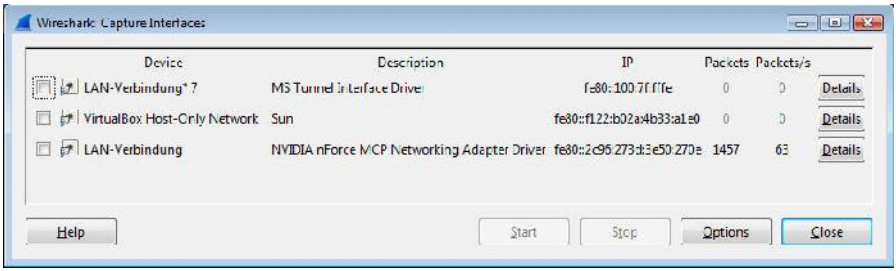
1.12 Werkzeugleiste

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:

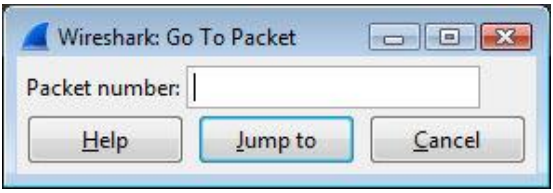
Die dateispezifischen Funktionen im Detail:

-  - 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:

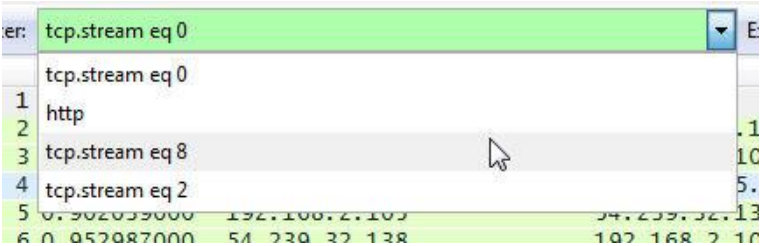
1.13 Filterfunktionen im Griff

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.

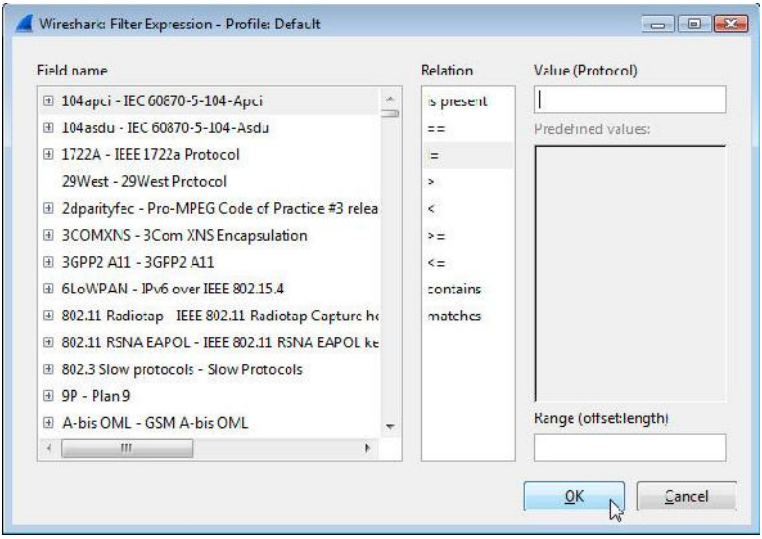
Damit Ihnen keine relevanten Informationen entgehen, müssen Sie die Filterfunktionen kennen und einzusetzen wissen. Wenn Sie beispielsweise entsprechend

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.



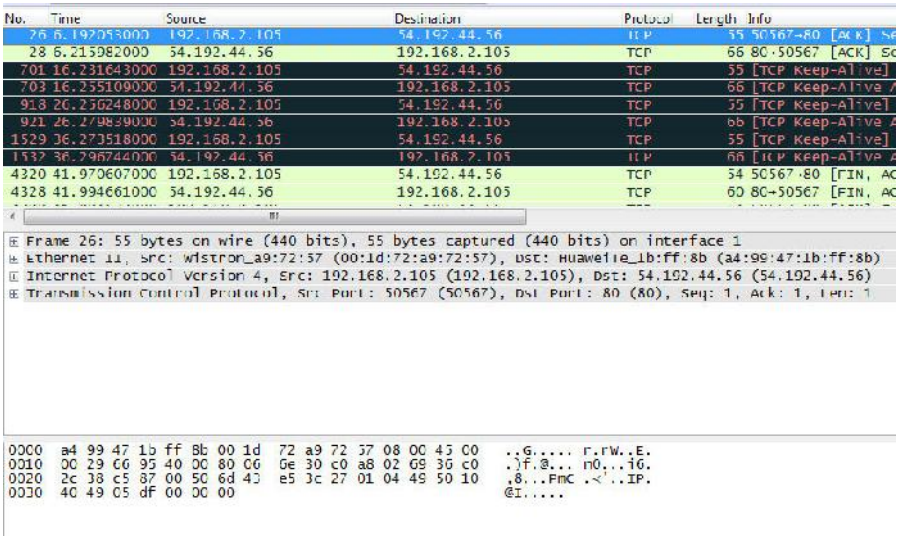
Das Anlegen von Filterausdrücken.

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.

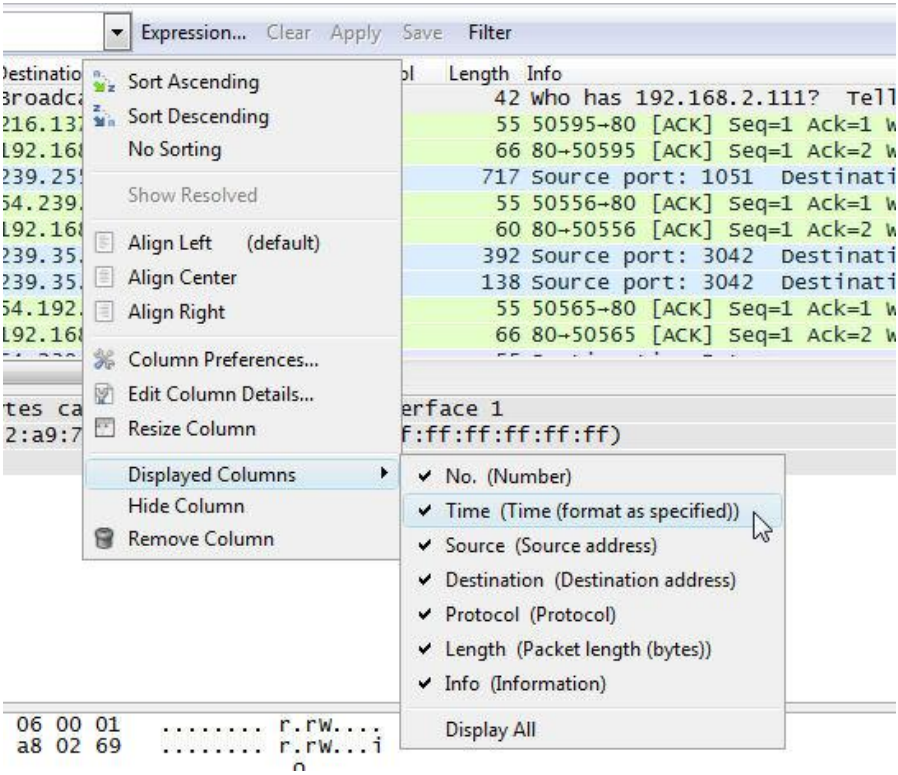
In der Paketansicht können Sie sich schnell und einfach durch die Paketliste bewegen und sich einen ersten Überblick verschaffen, welche Hosts miteinander kommuniziert haben. Sie können dieser Übersicht auch entnehmen, welche Programme dabei zum Einsatz kamen.

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.

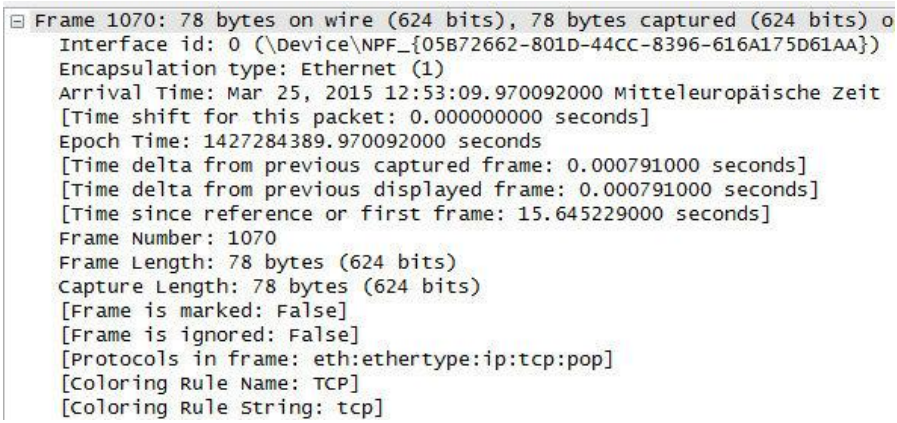


Das Ein- und Ausblenden von Spalten.

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.

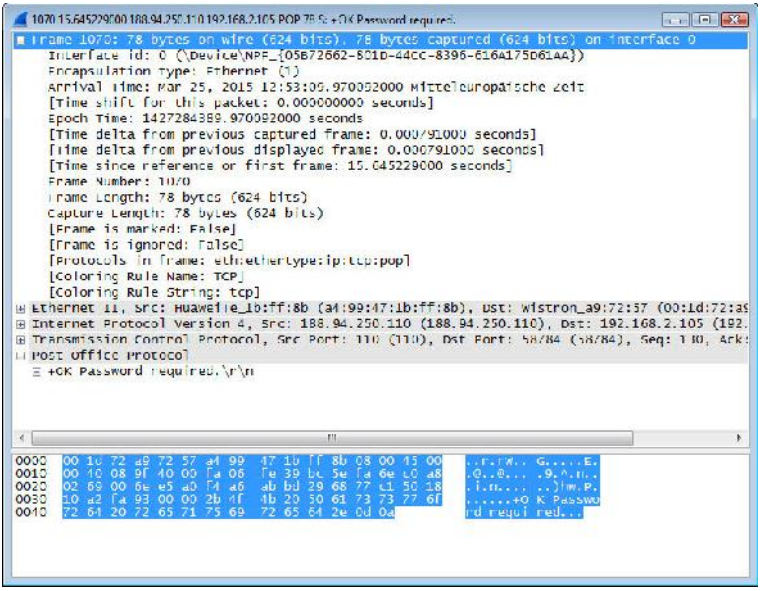


Die typischen Meta-Informationen eines Wireshark-Frames.

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.

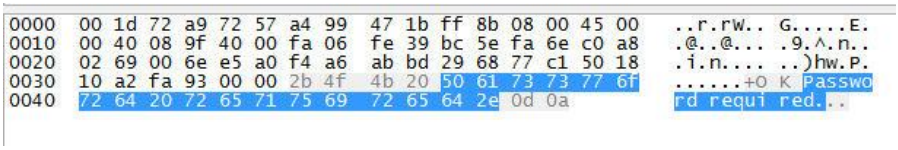
Mit Hilfe des Kontextmenüs der rechten Maustaste können Sie verschiedene weitere Aktionen ausführen. Mit *Expand All* können Sie beispielsweise alle eingeklappten Informationen ausklappen. Mit *Collapse All* können Sie die Baumansicht wieder zusammenfalten. Mit den beiden Befehlen *Expand Subtrees* und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

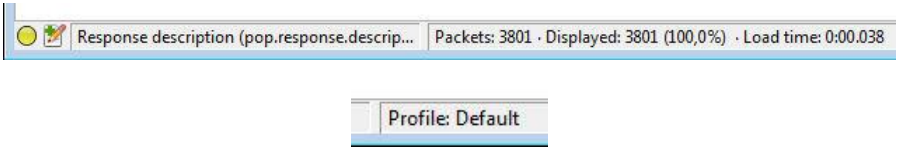


Die Byte-Ansicht erlaubt tiefe Einblick in den Datentransfer.

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

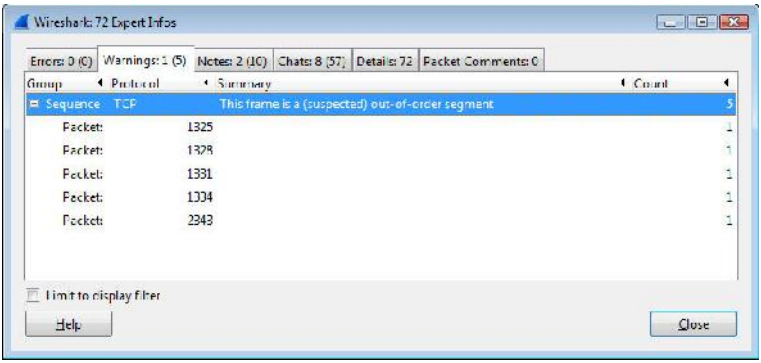
Den Abschluss nach unten hin bildet die Statusleiste, der Sie verschiedene Statusinformationen entnehmen können. Die Statusleiste umfasst mehrere Infobereiche und auch zwei Schaltflächen.



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.

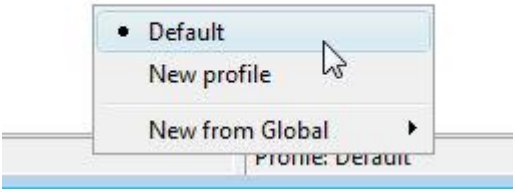
Das Hinzufügen von Kommentaren.

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.

2 Wireshark in Aktion – live

Wireshark kennt zwei zentrale Einsatzszenarien: Das eine bezeichnet man als Live Capturing und überwacht den Netzwerktraffic in Echtzeit, das andere zeichnet den Traffic auf und speichert ihn in einer Capture-Datei, die dann zu einem späteren Zeitpunkt analysiert wird. In der Praxis kombiniert man diese beiden Szenarien meist. Doch da für jedes spezifische Dinge zu beachten sind, widmen wir uns zunächst dem einen und im nächsten Kapitel der Analyse von Aufzeichnungen.

Das Einlesen von Live-Netzwerkdaten ist eine der wichtigsten Funktionen von Wireshark. Sie können dabei unterschiedlichsten Traffic aufzeichnen und die Aufzeichnung mit unterschiedlichen Kriterien auch wieder anhalten, beispielsweise nach einer bestimmten aufgezeichneten Datenmenge oder einer Paketanzahl. Sie können den Traffic in Echtzeit analysieren, während im Hintergrund weiter aufgezeichnet wird.

Auch bei Live-Aufzeichnungen können Sie Filter für die gezielte Beschränkung der Ausgaben verwenden. Besonders flexibel sind Sie bei der Sicherung der Aufzeichnungen. Diese können in mehrere Dateien geschrieben werden. Sie können dabei beispielsweise die Größe der Sicherungen und die Anzahl der letzten Sicherungsdateien bestimmen. Live Capturing erlaubt auch die simultane Aufzeichnung verschiedener Netzwerkschnittstellen.

Die Capturing Engine unterliegt allerdings auch gewissen Einschränkungen. Sie können beispielsweise nur bedingt Aufzeichnungen beim Erfüllen bestimmter Kriterien beenden.

2.1 Vorbereitungen

Bevor Sie mit der Aufzeichnung der Netzwerkaktivitäten beginnen, sind einige Vorbereitungen zu treffen. Das Einrichten der Aufzeichnung ist bisweilen ein wenig tricky – zumindest, wenn Sie erst in die Netzwerkanalyse mit Wireshark einsteigen.

Bevor Sie sich an die eigentliche Capture-Konfiguration machen, sollten Sie einige Dinge beachten. Zunächst benötigen Sie Root- oder Administratorrechte, um Live Capturing durchzuführen. Als Nächstes müssen Sie entscheiden, welche Netzwerkschnittstellen überwacht werden sollen.

Ihr Einstieg in die Welt von Wireshark und ihre ersten Aufzeichnungsversuche können die gesamte Bandbreite abdecken: „Wow, das ist ja mal einfach“ bis hin zu „Wireshark gibt aber merkwürdige Infos aus“. Gerade Neulinge tun sich schwer, die Capture-Einstellungen praktikabel zu nutzen. Wenn Sie diese ersten Hürden genommen haben, geht alles andere später einfacher.

Das Aufzeichnen umfasst mehrere Schritte. Noch bevor Sie Wireshark in Betrieb nehmen, sollten Sie sicherstellen, dass Sie den gewünschten Traffic aufzeichnen und analysieren dürfen. Mit Wireshark können Sie auch den Traffic von entfernten Schnittstellen aufzeichnen. Gerade beim Remote Capturing muss vor einer Aufzeichnung sorgsam geprüft werden, ob aufgrund von rechtlichen Rahmenbedingungen, den Datenschutzbestimmungen oder anderen Vorschriften und Vorgaben eine Aufzeichnung überhaupt zulässig ist.

Sollten für die Aufzeichnung Änderungen an der Verkabelung erforderlich sein, müssen Sie auch hier zunächst prüfen, ob derlei Eingriffe in die Netzwerkumgebung zulässig sind.

Dann können Sie sich dem zweiten Schritt zuwenden: der allgemeinen Einrichtung der Umgebung. Hierzu gehört, dass Sie sicherstellen bzw. dafür sorgen, dass Sie über ausreichende Berechtigungen für die Aufzeichnung verfügen. Hiermit sind technische Berechtigungen des verwendeten Betriebssystems gemeint.

Unter Windows sollten Sie Wireshark beispielsweise als Administrator ausführen. Dazu klicken Sie auf das Wireshark-Icon und führen aus dem Kontextmenü der rechten Maustaste den Befehl *Als Administrator ausführen* aus.

Linux-Anwender profitieren von einer Besonderheit: Wireshark implementiert eine Trennung der Privilegien. Während die GUI von einem Standardanwender ausgeführt wird, wird das dumpcap-Utility, das für die Aufzeichnung zuständig ist, mit Root-Rechen ausgeführt.

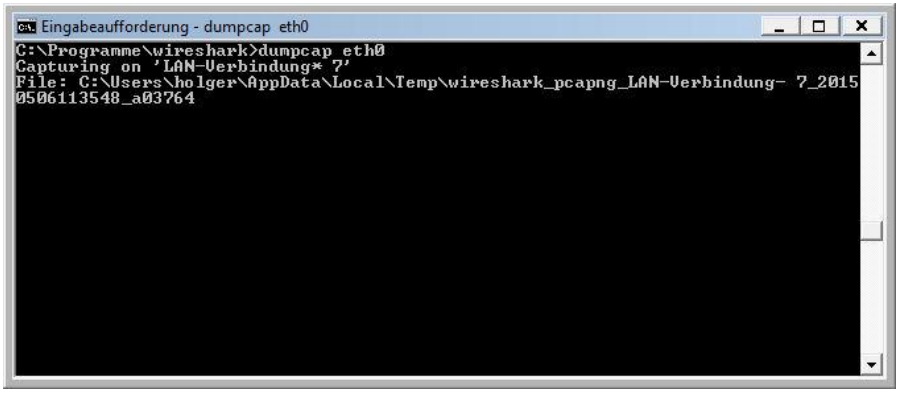
Dann gilt es zu prüfen, dass das verwendete Betriebssystem auch die notwendigen Treiber für die Aufzeichnung besitzt und dass diese aktiviert sind. Die Zeiteinstellungen müssen korrekt vorgenommen sein.

Der dritte Schritt dient der eigentlichen Aufzeichnung der Netzwerkdaten – und zwar der des ein- und ausgehenden Traffics. Es ist offensichtlich, dass der Traffic, unabhängig von der Netzwerk-Topologie, von und zu Ihrer Sniffer-Installation läuft.

Sie müssen außerdem das entsprechende Interface bestimmen und dann die Aufzeichnung starten. Für den Einstieg sollten Sie keinerlei Filter verwenden. Nun können Sie die Aufzeichnung starten. Nehmen Sie den ein- und ausgehenden Traffic unter die Lupe.

Sollten bei den ersten Aufzeichnungen Probleme zu Tage treten, kann das folgende Ursachen haben:

- **Netzwerkschnittstellen**: Stellen Sie sicher, dass Sie die geeigneten Schnittstellen ausgewählt haben.
- **Netzwerkmedien**: Prüfen Sie, ob es medienspezifische Einschränkungen der Netzwerkumgebung gibt.
- **Promiscuous Modus**: Schalten Sie diesen Modus ein bzw. aus und prüfen Sie, mit welchem die Aufzeichnung bzw. das Mitschneiden funktioniert.
- **Überschneidende Software**: Netzwerksoftware wie VPN- oder persönlichen Firewall-Software auf unteren Netzwerkebenen können Probleme bei der Aufzeichnung verursachen.
- **Offloading**: Auch der NIC kann die Aufzeichnung behindern.
- **Kein Traffic:** Stellen Sie sicher, dass es in Ihrem Netzwerk auch tatsächlich produktiven Traffic gibt.
- **Performance**: Eine mangelhafte Netzwerk-Performance kann eine Aufzeichnung erschweren bzw. sogar verhindern.



Das Konsolenprogramm Dumpcap in Aktion.

Sollten Sie dennoch keinen nennenswerten Traffic aufzeichnen können, so liegt das mit hoher Wahrscheinlichkeit an dem verwendeten Treiber. Ob die verwendeten Treiber tcpdump und WinDump korrekt arbeiten, können Sie auf der Konsole

herausfinden. Auch Probleme mit libpcap bzw. WinPcap können eine Aufzeichnung verhindern.

Nachdem Sie in Schritt 3 alle etwaigen Probleme gelöst und die Vorbereitung für die Aufzeichnung von ein- und ausgehendem getroffen haben, steht als Nächstes die Frage zur Debatte, was mit dem Traffic passieren soll, der an andere als den Wireshark-Rechner gerichtet ist.

Sie müssen dazu insbesondere die richtige Positionierung des Sniffers in der Netzwerktopologie bestimmen. Auch hier kann es medienspezifische Einschränkungen und das Ein- bzw. Ausschalten des Promiscuous Modus geben. Im Zweifel gilt: Probieren geht über studieren.

Eine der Besonderheiten von Wireshark ist die Fähigkeit, dass Sie mit dem Sniffer auch den Traffic von entfernten Systemen aufzeichnen können. Hierzu bedient sich Wireshark verschiedener Tools und Techniken. So kann beispielsweise WinPcap-Remote, das Remote-Feature von WinPcap verwendet werden. Auch die Ausführung von Wireshark auf dem Remote-System und die Fernsteuerung mit einer VNC-Lösung wäre denkbar. Wireshark unterstützt außerdem spezifische Capture-Filtereinstellungen für das Remote Capturing. Wir kommen weiter unten noch darauf zu sprechen.

2.2 Aufzeichnung starten

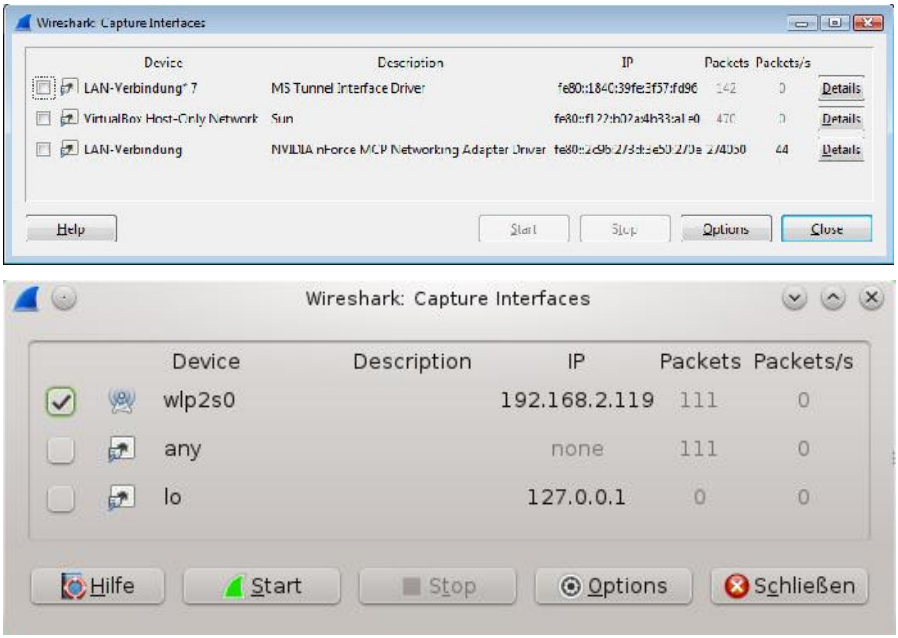
Haben Sie notwendige Vorüberlegungen für die Aufzeichnung des Netzwerk-Traffics mit Wireshark angestellt, können Sie sich der tatsächlichen Aufzeichnung zuwenden.

Bevor Sie eine Aufzeichnung starten können, müssen Sie zunächst die Schnittstellen und Aufzeichnungsoptionen bestimmen. Wenn Sie bereits den Namen der Capture-Schnittstelle kennen, können Sie die Aufzeichnung mit Wireshark auch auf der Konsole mit folgendem Kommando starten:

```
wireshark -i eth0 -k
```

Dieser Befehl startet das Wireshark-Capturing auf Schnittstelle *eth0*.

Zunächst müssen Sie also die Schnittstellen auswählen und dann im nächsten Schritt die Capture-Optionen einsehen bzw. gegebenenfalls bearbeiten. Um die Auswahl der Schnittstellen zu treffen, klicken Sie in der Symbolleiste auf das Symbol *Capture Interfaces*.



Die Konfiguration und Auswahl der Schnittstellen (oben unter Windows, unten unter Linux)

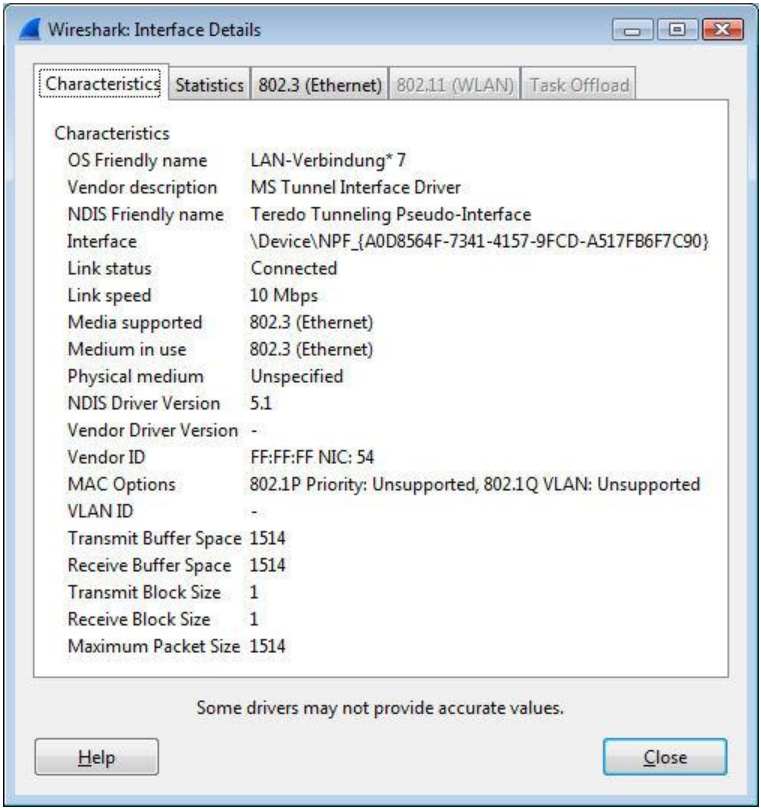
Voranstehende Abbildung zeigt die beiden Dialoge *Captures Interfaces* unter Linux und Windows. Laut Angaben der Entwickler beansprucht dieser Dialog sehr viele Systemressourcen. Sie sollten ihn daher nach der Interface-Auswahl schließen. Sollten in dem Dialog ein oder mehrere Schnittstellen nicht auftauchen, so liegt das mit hoher Wahrscheinlichkeit daran, dass sie in den Systemeinstellungen nicht aktiviert ist.

Die meisten Rechner stellen mehrere Netzwerkschnittstellen zur Verfügung. Die können Sie alle für die Netzwerkaufzeichnung verwenden. Dazu aktivieren Sie die gewünschten Schnittstellen der Reihe nach.

Der Dialog *Capture Interfaces* stellt Ihnen folgende Funktionen, Informationen und Einstellungen zur Verfügung:

- **Device**: In dieser Spalte wird die Bezeichnung der Schnittstelle angezeigt. Diese Informationen entnimmt Wireshark dem verwendeten Betriebssystem. Links neben der Device-Spalte zeigt ein kleines Symbol den Typ der Schnittstelle an.

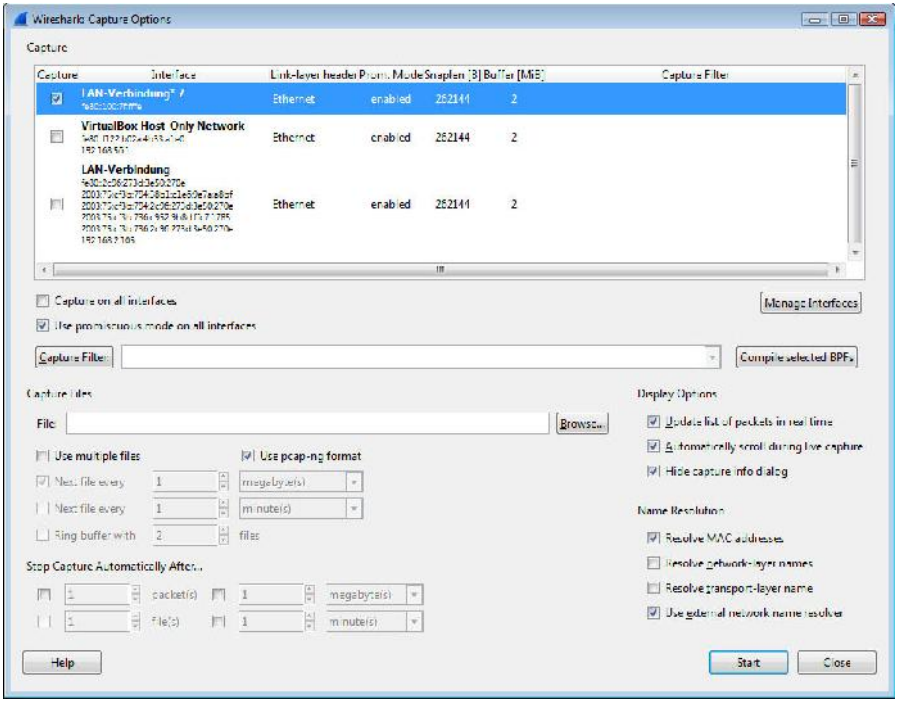
- **Description**: Hier finden Sie die Beschreibung der Netzwerkschnittstelle. Auch diese Information bezieht Wireshark vom Betriebssystem. Sie können allerdings auch eigene Kommentare über die Schnittstellenoptionen hinzufügen.
- **IP**: In dieser Spalte wird die erste IP-Adresse aufgeführt, die Wireshark für eine Schnittstelle identifizieren kann. Mit einem Klick auf die Angabe können Sie zu anderen gefundenen Adressen switchen – sofern solche vorhanden sind. Anstelle von IP- werden häufig auch MAC-Adressen aufgeführt.
- **Packets**: In dieser Spalte führt Wireshark die Anzahl der Pakete aus, die das Interface aufgezeichnet hat. Ist die Anzeige grau, wurden in der letzten Sekunde keine Daten aufgezeichnet.
- **Packets/s**: Diese Spalte führt die Zahl der Pakete auf, die in der letzten Sekunde aufgezeichnet wurden. Auch hier gilt: Wurden keine Daten aufgezeichnet, ist die Anzeige grau.
- **Details**: Führen Sie Wireshark auf einem Windows-System aus, können Sie mit einem Klick auf die *Details*-Schaltfläche jede Menge weitere Informationen über die Schnittstelle abrufen. Die Schnittstellendetails sind derart umfangreich, dass sie auf verschiedene Registerkarten verteilt sind.
- **Start**: Unterhalb der Interface-Liste finden Sie vier Schaltflächen zur Steuerung der Auszeichnung. Mit einem Klick auf die *Start*-Fläche beginnen Sie die Aufzeichnung entsprechend Ihren Voreinstellungen.
- **Stop**: Mit einem Klick auf diese Schaltfläche beenden Sie den Capture-Vorgang.
- **Options**: Mit einem Klick auf diese Schaltflächen öffnen Sie die Capture-Optionen.
- **Close**: Um die Schnittstellenauswahl zu schließen, klicken Sie auf diese Schaltfläche.
- **Help**: Schließlich können Sie mit einem Klick auf *Help* die Hilfe des Programms starten.



Die Details der Schnittstelle.

2.3 Die Capture-Optionen

Nach der Auswahl der zu verwendeten Netzwerkschnittstelle können Sie als Nächstes die sogenannten Capture-Optionen anpassen. Die öffnen Sie im Dialog *Capture Interface* mit einem Klick auf *Options*. Alternativ klicken Sie in der Symbolleiste auf das zugehörige Symbol.



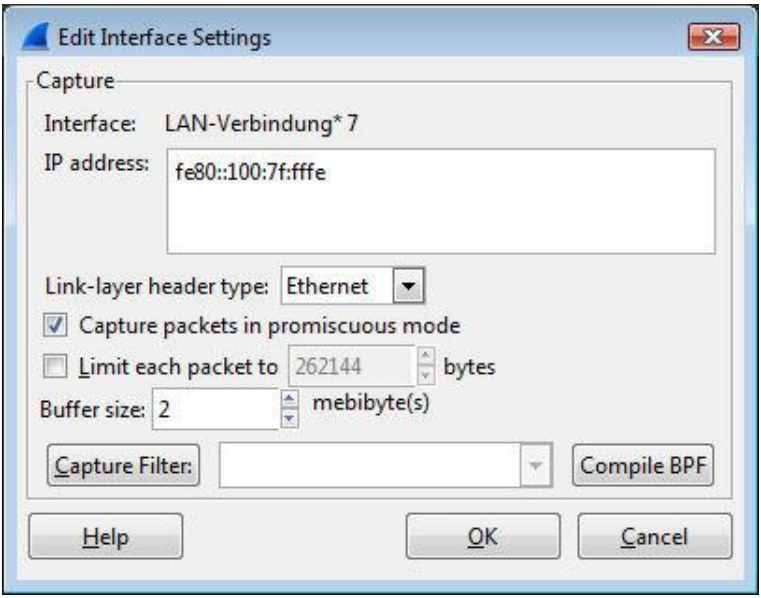
Die Capture-Optionen.

Im oberen Bereich des Dialogs finden Sie eine Tabelle, in der die von Wireshark erkannten Netzwerkschnittstellen aufgeführt werden. Die Tabelle führt folgende Informationen auf:

- **Capture**: In dieser Spalte erfahren Sie, ob die Schnittstelle für die Aufzeichnung aktiviert wurde oder nicht. Sie können diese aktivieren, wieder deaktivieren und neue hinzuschalten.

- **Interface**: Hier werden die von Wireshark erkannten Netzwerkstellen aufgeführt. Neben der Adapterbezeichnung werden hier die IP- und die MAC-Adresse angezeigt. Kann Wireshark keine Adresse auflösen, so finden Sie hier den Hinweis *None*. Beachten Sie, dass bei Windows-Systemen keine Loopback-Adresse aufgeführt wird, bei Linux-Systemen hingegen schon.
- **Link-layer Header**: Dieser Spalte können Sie den Link Layer-Header-Typ entnehmen. Der kann beispielsweise *Ethernet* lauten.
- **Promicuous Mode**: Der Promicuous Mode bezeichnet einen bestimmten Empfangsmodus von Netzwerkkomponenten, bei dem das Gerät den gesamten ankommenden Datenverkehr an die in diesen Modus geschaltete Netzwerkschnittstelle liest (anstatt nur den für das Gerät bestimmten Datenverkehr) und die Daten zur Verarbeitung an das Betriebssystem weitergibt. Hier erfahren Sie, ob dieser Modus für die jeweilige Schnittstelle aktiviert (enabled) oder deaktiviert (disabled) ist.
- **Snaplen**: Dieser Spalte können Sie entnehmen, wie die maximale Datenmenge ist, die von jedem Paket aufgezeichnet wird. Der Standartwert *Default* entspricht 65535 Byte.
- **Buffer**: Wireshark verwendet einen Zwischenspeicher, um die Daten während der Aufzeichnung zu puffern und für eine reibungslose Aufzeichnung zu sorgen. Dessen Größe kann für jede Schnittstelle anders konfiguriert sein. Dieser Spalte entnehmen Sie die Größe in MByte.
- **Mon. Mode**: Diese Funktion ist nur bei unixartigen Systemen verfügbar. Diese Spalte verrät Ihnen, ob der Monitormodus aktiviert ist oder nicht.
- **Capture Filter**: Der letzten Tabellenspalte können Sie schließlich entnehmen ob, und wenn ja welche, Aufzeichnungsfilter gesetzt wurden.

Sie können die Einstellungen für jede Netzwerkschnittstelle ändern, indem Sie einen Doppelklick auf einen Eintrag ausführen. Wireshark öffnet den Dialog *Edit Interface Settings*, in dem Sie verschiedene Änderungen vornehmen können. Sie können beispielsweise die Paket- und Puffergröße ändern. Mit einem Klick auf die Schaltfläche *Capture Filter* können Sie außerdem die Filterkonfiguration ändern.

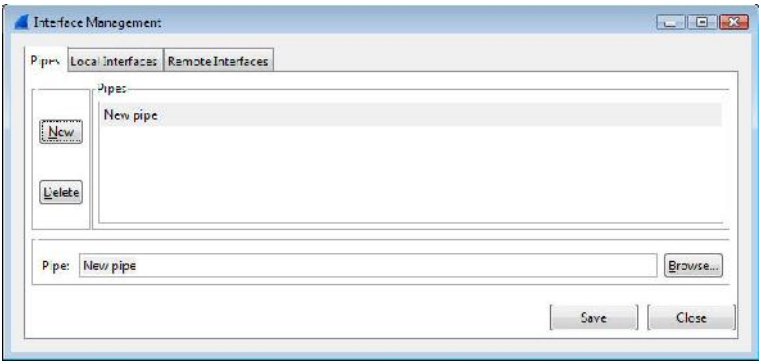


Die Schnittstelleneinstellungen.

Die Capture-Optionen bieten unterhalb der tabellarischen Übersicht weitere Anpassungsmöglichkeiten. Unmittelbar im Anschluss folgen verschiedene Optionen und Auswahlmöglichkeiten:

- **Capture on all interfaces**: Wenn Sie den Traffic auf allen Schnittstellen mitschneiden wollen, müssen Sie nicht in der Tabelle jedes Häkchen manuell setzen, sondern können durch Aktivieren dieser Option alle Schnittstellen aktivieren.
- **Use promiscuous mode on all interfaces**: Durch das Aktivieren dieser Option setzt Wireshark alle Netzwerkadapter in den Promiscuous Modus bei der Aufzeichnung.
- **Capture Filter**: Mit dieser Funktion wählen Sie die Aufzeichnungsfilter im Dialog *Capture Filter* aus, die auf alle auswählten Schnittstellen angewendet werden. Sie können auch neue Filter anlegen. Später hinzugefügte Interfaces „erben“ die hier getroffenen Einstellungen. Standardmäßig erfolgt keine Filterung. Wir kommen weiter unten noch detailliert auf die Verwendung von Filtern zu sprechen.

- **Compile selected BPFs**: Mit einem Klick auf diese Schaltfläche kompilieren Sie die Filterkonfiguration. Dabei wird ein Pop-up-Dialog ausgegeben, der den resultierenden Pseudo-Code anzeigt. Die Ausgabe kann Ihnen helfen, die Filterung besser zu verstehen.
- **Manage Interfaces**: Sollte in der Interface-Liste eine gewünschte Schnittstelle nicht ausgeführt werden, können Sie diese mit einem Klick auf diese Schaltfläche öffnen. In dem gleichnamigen Dialog können Sie bestehenden Schnittstellen verwalten und neue anlegen. Diesen Dialog verwenden Sie auch für das Anlegen von Remote-Schnittstellen.



Das Interface-Management mit Wireshark.

Als Nächstes können Sie im Bereich *Capture Files* verschiedene dateispezifische Einstellungen vornehmen:

- **File**: In diesem Eingabefeld können Sie den Dateinamen für die Aufzeichnungsdatei bestimmen. Das Feld ist standardmäßig leer. Wenn Sie es leer lassen, werden die Daten temporär gespeichert. Über die *Browse*-Schaltfläche können Sie im Dateisystem navigieren und den Speicherplatz bestimmen.
- **Use multiple files**: Wireshark schreibt die Aufzeichnungen standardmäßig in einer Datei. Die wird schnell mehrere GByte groß. Um das zu verhindern, können Sie die Aufzeichnungen in mehrere Dateien schreiben. Dazu aktivieren Sie diese Option und bestimmen dann die Größe oder die Dauer, ab der in eine neue Datei geschrieben wird. Sie können die Aufzeichnung auch nach x Dateien abbrechen. Dazu aktivieren Sie die Option *Stop capture after x files* und geben die Dateizahl an.

- **Use pcap-ng format**: Durch Aktivieren dieses Kontrollkästchens verwenden Sie das neue PCAPNG-Format, das sich aktuell allerdings noch in der Entwicklung befindet. Wenn Sie mehrere Schnittstellen überwachen, wird automatisch dieses Format verwendet.

Die Capture-Optionen stellen Ihnen verschiedene Möglichkeiten zur Verfügung, mit denen Sie die Aufzeichnung automatisch beim Erreichen definierbarer Kriterien beenden können. Die dazu verfügbaren Einstellungen sind im Bereich *Stop Capture Automatically After* zu finden:

- Anzahl der Pakete
- MByte-Grenzwert
- Dauer in Minuten
- Anzahl an Dateien

Im rechten Dialogbereich finden Sie zwei weitere Konfigurationsbereiche: *Display Options* und *Name Resolution*. Der Bereich *Display* bietet folgende Optionen:

- **Update list of packets in real time**: Diese Option ist standardmäßig aktiviert und sorgt für eine kontinuierliche Aktualisierung der Paketliste in Echtzeit. Wenn Sie diese Option deaktivieren, wird die Ansicht während der Aufzeichnung nicht aktualisiert.
- **Automatically scroll during live capture**: Wenn Sie diese Option aktivieren, scrollt die Anzeige automatisch während der Anzeige mit.
- **Hide capture info dialog**: Ist diese Option aktiviert, wird der *Capture info*-Dialog im Hintergrund platziert.

Unter *Name Resolution* können Sie vier Einstellungen vornehmen:

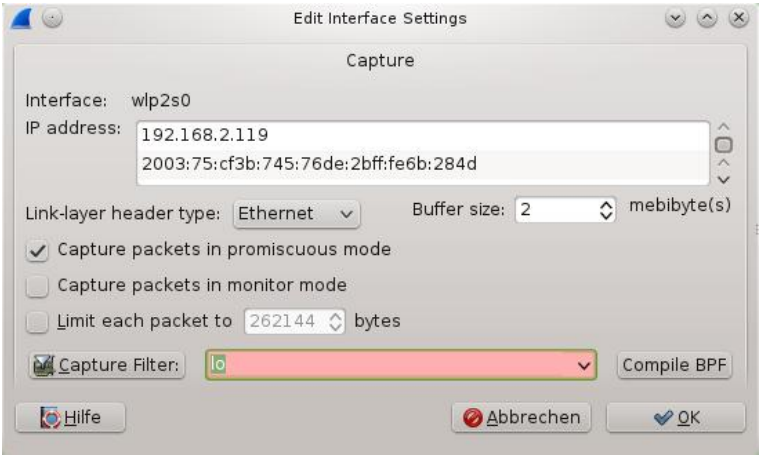
- **Resolve MAC addresses**: Diese Option ist standardmäßig aktiviert und löst die MAC-Adressen auf.
- **Resolve network-layer names**: Sorgt für die Auflösung der Netzwerk-Layer-Namen.
- **Resolve transport-layer name**: Löst den Namen der Transportschicht auf.

- **Use external network name resolver**: Auch externe Netzwerknamen können aufgelöst werden.

Wir kommen in Kapitel 6.3 noch einmal auf die Namesauflösung zurück. Den Abschluss des Dialogs bilden die *Help*-, *Start*- und *Close*-Tasten am unteren Ende des Dialogs.

2.4 Interface-Einstellungen

Wir sind bereits oben der Interface-Konfiguration begegnet, die Sie mit einem Doppelklick auf den betreffenden Interface-Eintrag öffnen. Hier können Sie verschiedene Einstellungen einsehen und bearbeiten. Dem Dialog entnehmen Sie im Kopfbereich zunächst die Interface-Bezeichnung.



Die Interface-Konfiguration unter Linux.

Die weiteren Einstellungen und Informationen im Überblick:

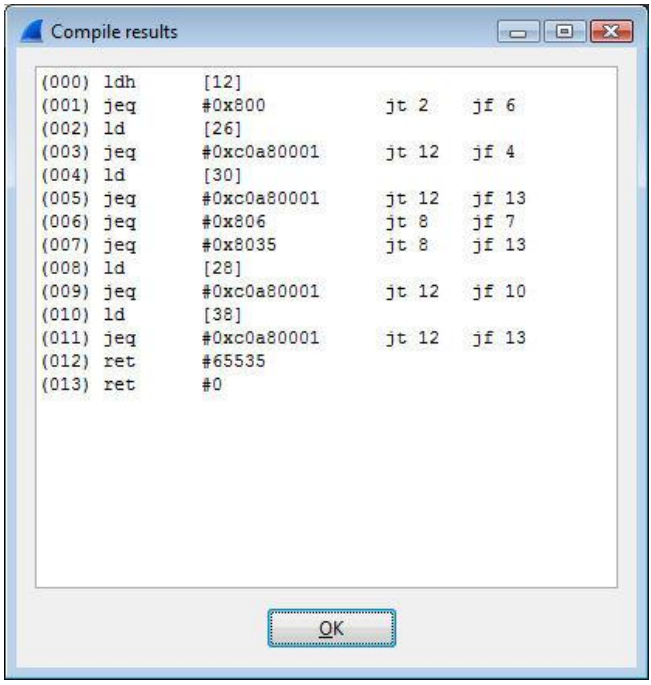
- **IP address**: Hier werden die der Netzwerkkarte zugehordneten Adressen aufgeführt. In der Regel handelt es sich um die IP- und die MAC-Adressen der Schnittstelle.
- **Link-layer header type**: Wenn Sie Traffic von einer Ethernet-Schnittstelle aufzeichnen, behalten Sie die Konfiguration *Ethernet* bei. Wenn Sie

Traffic von einem Cisco Cable Modem Termination System aufzeichnen, das DOCSIS-Traffic über der Ethernet legt, wählen Sie die Option *DOCSIS*.

- **Wireless settings**: Wenn Sie für das Aufzeichnen des Traffics einen AirPcap-Adapter verwenden, können Sie hier die drahtlose Aufzeichnung konfigurieren. Diese Einstellung ist nur unter Windows verfügbar.
- **Remote settings**: Unter Windows können Sie einer weiteren Einstellungen begegnen, die für das Remote Capturing relevant ist. Wir kommen weiter untenr darauf zu sprechen.
- **Capture packets in promiscuous mode**: Aktivieren Sie dieses Kontrollkästchen, um den Netzwerkadapter in den Promiscuous Mode zu versetzen. Wenn Sie diese Option deaktivieren, werden nur die Pakete aufgezeichnet, die von und zu dieser Schnittstelle übermittelt werden, nicht aber alle anderen Datenpakete in dem Netzwerksegment. Allerdings bedeutet das Aktivieren dieses Modus nicht notwendigerweise, dass sie auch alle Pakete zu sehen bekommen.
- **Limit each packet to n bytes**: Hiermit bestimmen Sie die maximale Datenmenge, die Wireshark von jedem Paket aufzeichnet. Dieser Wert wird gelegentlich auch als Snaplen bezeichnet. Wenn Sie diese Option deaktivieren, ist der Wert standardmäßig auf 65.535 gesetzt – ein ausreichend hoher Wert für die meisten Protokolle. Wenn Sie unschlüssig sind, ob für Ihre Anwendungszwecke der Wert geeignet ist, behalten Sie einfach den Standardwert bei. Sollten Sie nicht alle Daten der Pakete benötigen, können Sie mit diesem Schalter steuern, wie viel an Informationen tatsächlich aufgezeichnet wird.
- **Buffer size: n megabytes**: Hier legen Sie die Größe des Zwischenspeichers fest, den Wireshark beim Aufzeichnen verwendet. Der ist meist 2 MByte groß, kann aber bei einer ausreichenden Systemausstattung erhöht werden. Es handelt sich hierbei um den Kernel-Puffer.
- **Capture packets in monitor mode**: Wenn Sie einen WLAN-Adapter verwenden, können Sie mit dieser Option den Monitormodus aktivieren. Wie bereits erwähnt, ist dieser Modus nur bei unixartigen Systemen verfügbar. Das Aktivieren dieser Option ist auch für das Mitschneiden von IEEE 802.11-Headern relevant. Beachten Sie, dass sich der Adapter bei der Verwendung des Monitor-Modus womöglich von dem Netzwerk löst, weil er für die Überwachung benötigt wird.
- **Capture Filter**: Mit einem Klick auf diese Schaltfläche öffnen Sie die Ihnen bereits bekannte Filterauswahl. Wenn Sie mit dem Setzen von Filtern

vertraut sind, können Sie die Filterkonfiguration auch manuell in das Eingabefeld eingeben. Standardmäßig kommt kein Filter zum Einsatz. Wir kommen in Kapitel 5 detailliert auf die Verwendung von Filtern zu sprechen; auch darauf, wie Sie eigene Filterkonfigurationen definieren, sichern und anwenden.

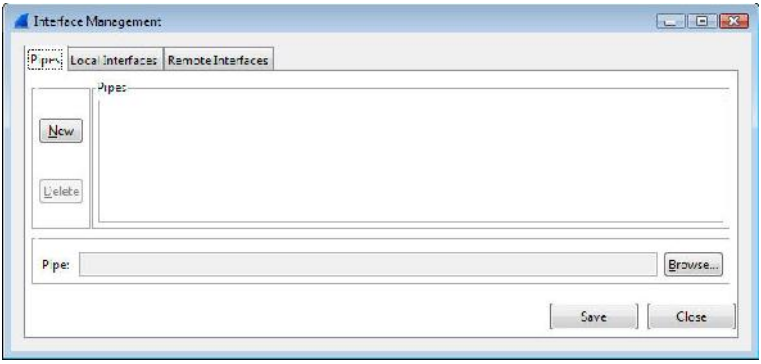
- **Compile BPF**: Nach der Auswahl eines Filters können Sie die Filterkonfiguration in BPF-Code kompilieren. Wireshark gibt das Ergebnis der Kompilierung in einem neuen Pop-up-Dialog aus. Nachstehende Abbildung zeigt ein Beispiel. Diese Ausgabe ist insbesondere für Anwender interessant, die tief in die Netzwerkanalyse mit Wireshark eintauchen wollen.



Die Ausgabe der Kompilierung.

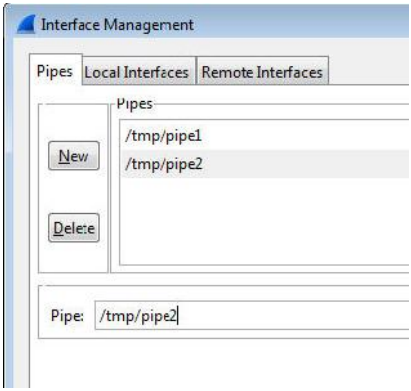
2.5 Neues Interface hinzufügen

Wireshark liest anhand der Systemkonfiguration die bestehenden Netzwerkschnittstellen ein und stellt sie Ihnen über die Capture-Optionen zur Verfügung. Sie können diese Konfiguration allerdings auch anpassen und beispielsweise neue Schnittstellen anlegen.



Das Schnittstellenmanagement.

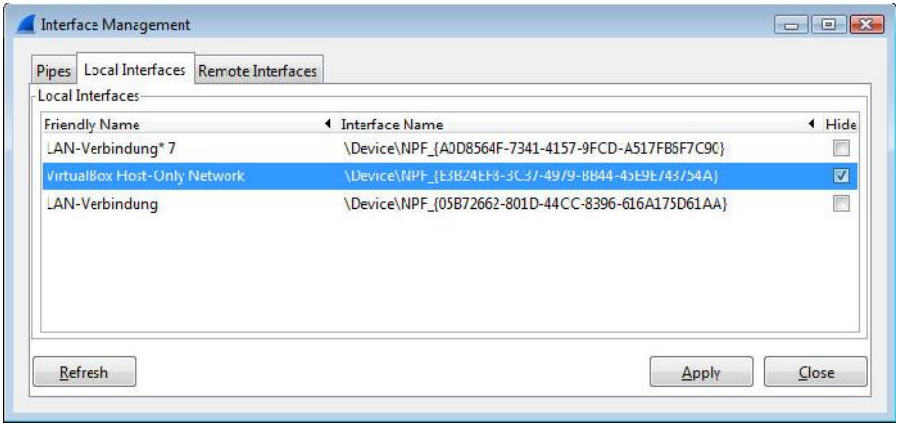
Das Schnittstellenmanagement von Wireshark erlaubt Ihnen das Hinzufügen von Pipes und Remote-Schnittstellen. Pipes, lokale und entfernte Schnittstellen sind auf drei Registerkarten verteilt.



Zwei neue Pipes sind entstanden.

Um eine neue Pipe anzulegen, klicken Sie auf der Registerkarte *Pipes* auf die Schaltfläche *New* und geben unter *Pipe* den Pfad ein. Mit einem Klick auf *Save* sichern Sie die Schnittstelle.

Der Registerkarte *Local Interfaces* können Sie die von Wireshark erkannten Schnittstellen entnehmen. Hier können Sie Schnittstellen gezielt verbergen, damit Sie nicht in anderen Dialogen auftauchen. Wenn Sie dem Wireshark-System eine neue Schnittstelle hinzugefügt haben, beispielsweise einen USB-WLAN-Adapter, wird der nicht automatisch der Wireshark-Konfiguration hinzugefügt. Der Grund hierfür: Das konsistente Scanning könnte negativ beeinflusst werden. Um eine geänderte oder neue Netzwerkschnittstelle in Wireshark einzulesen, führen Sie einen Refresh durch. Dazu klicken Sie auf die Schaltfläche *Refresh*.



Die Verwaltung der lokalen Schnittstellen.

Um eine nicht für Wireshark relevante Schnittstelle zu verbergen, aktivieren Sie das Kontrollkästchen in der *Hide*-Spalte. Mit einem Klick auf *Apply* setzen Sie etwaige Änderungen um.

Um eine entfernte Schnittstelle in Wireshark zu verwenden, wechseln Sie zur Registerkarte *Remote Interfaces* und legen mit *Add* eine neue Schnittstelle an. Sie müssen als Nächstes den Host, Port und gegebenenfalls die Zugangsdaten angeben. Im nächsten Abschnitt erfahren Sie, wie Sie konkret dabei vorgehen.

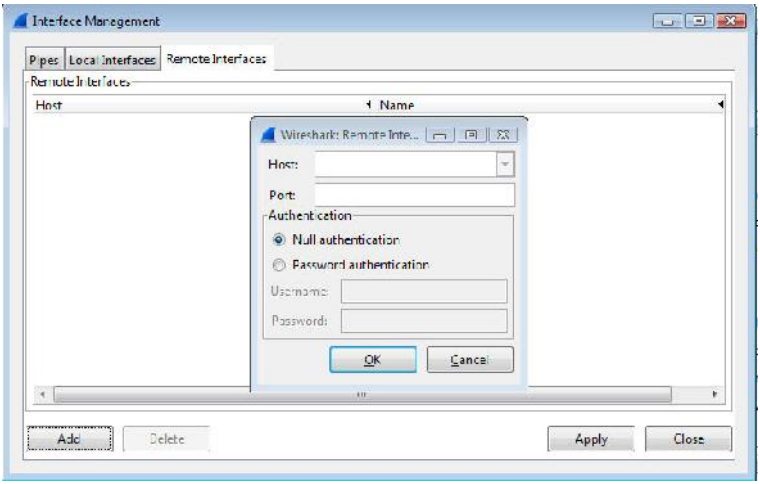
2.6 Remote-Schnittstelle einrichten

Die Kernaufgabe von Wireshark ist das Mitschneiden von Traffic auf lokalen Schnittstellen. Doch dazu benötigen Sie immer unmittelbaren Zugang zu dem System, das die Netzwerkfunktionalität bereitstellt. Nun ist es nicht immer möglich oder praktikabel, dass man direkten Zugriff auf eine oder mehrere relevante Netzwerkschnittstellen hat, über die der Traffic geleitet wird, der für Sie von Interesse ist.

Wenn Sie Wireshark auf einem Windows-System ausführen, bietet Ihnen der Sniffer die Möglichkeit des Remote Capturing. Wenn Sie Linux als Plattform verwenden, ist eine Traffic-Aufzeichnung beispielsweise per SSH möglich.

Bevor Sie allerdings mit Ihrer lokalen Wireshark-Installation auf eine entfernte Schnittstelle zugreifen können, müssen Sie auf dem Remote-System den Remote Packet Capture Protocol Service installieren. Der einfachste Weg: Handelt es sich um ein Windows-System, installieren Sie WinPcap (*http://www.winpcap.org/install/default.htm*) auf dem Ziel-System. Nachdem Sie WinPcap auf dem Ziel installiert haben, öffnen Sie in der Windows-Systemsteuerung die Service-Einstellungen. Dort finden Sie den Eintrag *Remote Packet Capture Protocol*. Starten Sie diesen.

Sie müssen auf dem Zielsystem außerdem sicherstellen, dass dort Port 2002 offen ist, denn der Remote Packet Capture Protocol-Service ist standardmäßig über diesen Port erreichbar.



Das Anlegen eines neuen Remote-Interfaces.

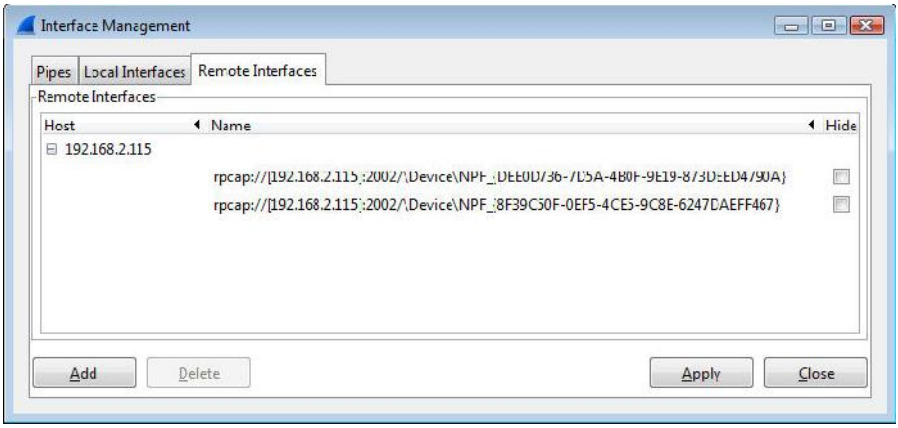
Um eine neue Remote-Schnittstelle für die Traffic-Aufzeichnung anzulegen, öffnen Sie die Interface-Verwaltung und wechseln zur Registerkarte *Remote Interfaces*. Dort klicken Sie auf *Add*, um den Dialog für die Konfiguration der Remote-Schnittstelle zu öffnen.

Die Einstellungen für das Remote-System:

- **Host**: Geben Sie in diesem Eingabefeld die IP-Adresse oder den Hostnamen des Remote-Systems an. Sollten Sie bereits erfolgreich Hosts für das Remote Capturing eingerichtet haben, können Sie diese über das Auswahlmenü wählen.
- **Port**: In diesem Eingabefeld geben Sie den Port für den Remote Packet Capture Protocol-Service an. Der lautet standardmäßig 2002.
- **Null authentification**: Wählen Sie diese Option, wenn für das Remote-System keine Zugangskennung erforderlich ist.
- **Password authentification**: Üblicherweise ist der Zugang zum Remote-System passwortgeschützt. Sollte das in Ihrem Fall auch so sein, wählen Sie diese Option und geben den Benutzernamen und das Passwort an.

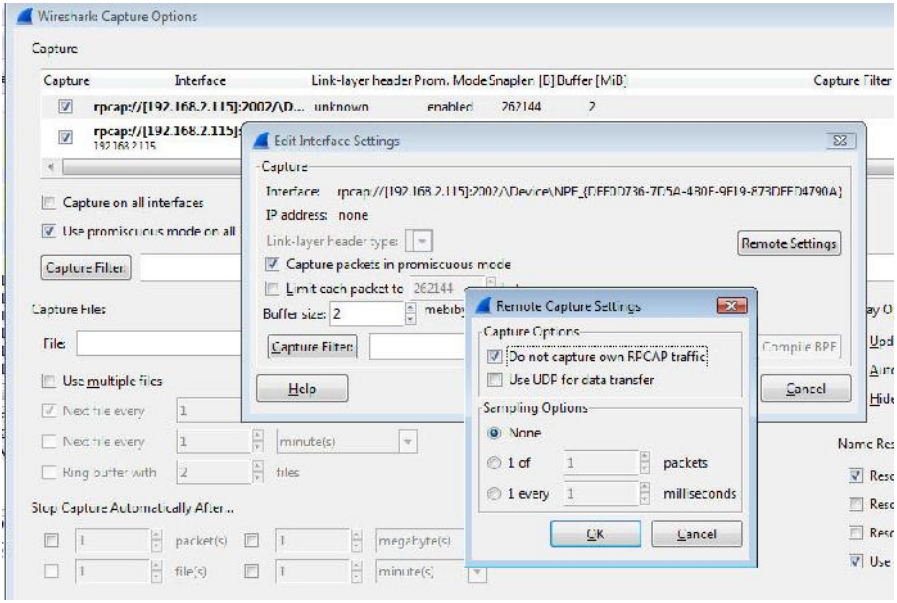
Die Liste der Schnittstellen konnte auf dem Remote-System nicht abgerufen werden.

Nach der Installation des WinPcap-Moduls müssen Sie auf Seiten des Remote-Systems dafür sorgen, dass dieses Modul ausgeführt wird. Sie müssen die Firewall-Einstellungen gegebenenfalls anpassen. Auch wenn ein Zugriff auf das Remote-System möglich ist, ist in den meisten Fällen auch die Angabe der Benutzerdaten erforderlich. Gelingt der Verbindungsaufbau nicht, gibt Wireshark eine entsprechende Meldung aus, dass die Authentifizierung fehlgeschlagen ist.



Ein erstes Remote Interface wurde erfolgreich eingerichtet.

Ist die Konfiguration des Remote Interface erfolgreich, finden Sie die entsprechende Konfiguration auf der Registerkarte *Remote Interface*.



Die Konfiguration der Remote-Schnittstelle.

Da es sich bei der Schnittstelle um eine „neue“ bzw. weitere Schnittstelle für Wireshark handelt, finden Sie den Eintrag nun auch in der Interface-Liste. Dort können Sie den Interface-Eintrag, wie oben beschrieben, mit einem Doppelklick öffnen und dann weitere Remote-spezifische Einstellungen einsehen und bearbeiten.

Wireshark präsentiert Ihnen den Dialog *Edit Interface Settings*, dessen wesentlichen Funktionen und Einstellungen Sie bereits kennen. Neu ist hier die Funktion *Remote Capture Settings*. Der zugehörige Dialog stellt Ihnen folgende Optionen zur Verfügung:

- **Do not capture own RPCAP traffic**: Diese Option ist standardmäßig aktiviert und sorgt dafür, dass kein RPCAP-Traffic zwischen dem Remote-Service und Wireshark aufgezeichnet wird. Sie sollten diese Option nur dann ausschalten, wenn die Aufzeichnung auf einem anderen als dem Interface erfolgt, mit dem die Verbindung zu Wireshark erfolgt.
- **Use UDP for data transfer**: Das Remote Capturing und der Datenfluss zwischen Wireshark und dem Remote-Dienst erfolgen in der Regel über eine TCP-Verbindung. Durch Aktivieren dieser Option können Sie auch einen UDP-Stream für den Datentransfer verwenden.
- **Sampling Options**: Diese Einstellungen sind für die optimale Anpassung des Remote Capturing an die verfügbaren Bandbreiten wichtig. Wireshark geht standardmäßig davon aus, dass genügend Bandbreite für die Übermittlung der Daten zur Verfügung steht, insbesondere für die Übermittlung der aufgezeichneten Informationen von Remote- zum Wireshark-System, die die Capture-Filter durchlaufen haben. Steht ausreichend Bandbreite zur Verfügung, behalten Sie die Voreinstellung *None* bei. Sie haben die Wahl zwischen zwei weiteren Einstellungen:
    - 1 of x packets: Hier sendet der Remote Packet Capture Protocol-Service lediglich eines von x Paketen. Diese Option ist bei geringer Bandbreite sinnvoll.
    - 1 every x milliseconds: Hier werden die Daten zeitlich eingeschränkt. Auch diese Einschränkung ist ebenfalls bei geringeren Bandbreiten sinnvoll einsetzbar.

Alternativ können Sie übrigens auch auf dem Remote-System eine Wireshark-Installation aufsetzen und diese dann von dem Steuersystem nutzen – zumindest den Aufzeichnungstreiber.

2.7 Erste Filter bei der Aufzeichnung

Wireshark verwendet die Libcap-Filtersprache für die Filterung der Aufzeichnungen. Diese bietet Ihnen vielfältige Filtermöglichkeiten, allerdings ist die Filterung nicht immer einfach zu verstehen. Für den Moment genügt eine kurze Einführung in der Filterung. Wie werden diese in Kapitel 5 weiter vertiefen.

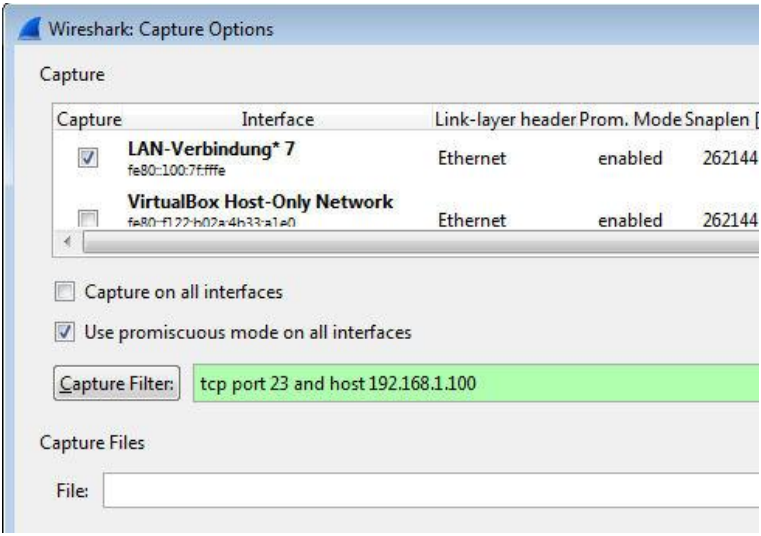
Ein Capture-Filter besteht aus einer Reihe von primitiven Ausdrücken, die durch Verarbeitungsanweisungen und optionale Schalter miteinander verbunden sind. Ein Filter sieht üblicherweise wie folgt aus:

```
[not] Ausdruck [and|or [not] Ausdruck ...]
```

Um beispielsweise den Telnet-Traffic zu einem Host *192.168.1.100* zu filtern, verwenden Sie folgende Konfiguration:

```
tcp port 23 and host 192.168.1.100
```

Diese Filterkonfiguration geben Sie in das Eingabefeld *Capture Filter* der Capture-Optionen ein.



Die Verwendung einer eigenen Filterkonfiguration.

Wenn Sie nun mit dem Capture-Filter die Ansicht auf den Telnet-Traffic beschränken wollen, der nicht vom Host *192.168.1.100* kommt, so erzielen Sie das einfach mit folgender Konfiguration:

```
tcp port 23 and not src host 192.168.1.100
```

Schauen wir uns einige typische Operatoren an, mit denen Sie Live-Traffic filtern können. Um den Traffic auf Basis des Hostnamens oder der IP-Adresse zu filtern, verwenden Sie folgende Filterkonfiguration:

```
[Quelle|Ziel] host <host>
```

Dieses Konstrukt erlaubt die Filterung auf Basis der Hostnamen oder der IP-Adressen. Vor den Filter können Sie die beiden Schüsselwörter *src*|*dst* für die Quellen- bzw. Zielangabe setzen, wenn Sie nur an Traffic in eine bestimmte Richtung interessiert sind. Ist keine Quelle- oder Zielabgabe vorgesehen, wird der Traffic in beide Richtungen aufgezeichnet.

Wenn Sie die laufende Aufzeichnung auf Ethernet-Hostadressen beschränken wollen, so verwenden Sie hierfür folgende Konfiguration:

```
ether [src|dst] host <ehost>
```

Auch hier können Sie wieder mit den Operatoren *src* und *dst* arbeiten.

Interessieren Sie sich für die Pakete, die einen Host als Gateway nutzen, verwenden Sie hierfür folgenden Filter:

```
gateway host <host>
```

In diesem Fall ist der angegebene Host weder die Quelle, noch das Ziel des Traffic, sondern dient einzig der Weiterleitung.

Sie können auch nach Netzwerknummern suchen. Auch hierfür verwenden Sie die folgende Konfiguration:

```
[src|dst] net <net> [{mask <mask>}|{len <len>}]
```

Auch bei dieser Konfiguration können Sie wieder die Parameter *src*|*dst* verwenden. Sie können für die Filterung auch die Netzmaske oder das CIDR-Präfix angeben.

Wenn Sie den Traffic auf bestimmte TCP- oder UDP-Port beschränken wollen, so ist das ebenfalls einfach in den Capture-Optionen möglich:

```
[tcp|udp] [src|dst] port <port>
```

Wenn Sie eine Filterung auf Protokoll und Quelle- bzw. Zielbasis durchführen wollen, muss *tcp*|*udp* vor *src*|*dst* stehen.

Für die Capture-Filterung können Sie auch die Paketlänge heranziehen. Um Pakete mit einer Länge größer oder kleiner einem bestimmten Wert zu identifizieren, verwenden Sie folgenden Filter:

```
less|greater <länge>
```

Wireshark bietet Ihnen auch die Möglichkeit, auf der Ethernet- oder IP-Layer zu filtern:

```
ip|ether proto <protokoll>
```

Entsprechend ist auch ein Filtern nach Ethernet-, IP-Broadcasts oder Multicasts möglich:

```
ether|ip broadcast|multicast
```

Und wenn Ihnen all diese Möglichkeiten noch nicht genügen, so können Sie für die Capture-Filterung auch komplexe Filter erstellen. Das lässt sich insbesondere mit logischen Ausdrücken realisieren. Die folgende Filterkonfiguration sucht nach Bytes oder einem Bereich:

```
<expr> relop <expr>
```

Wie wir oben gesehen haben, erlaubt Wireshark das Remote Capturing. Hierfür stehen Ihnen auch spezielle Filterfunktionen zur Verfügung. Wenn Sie eine Wireshark-Installation aus der Ferne steuern, beispielsweise per SSH, ein exportiertes X11-Fenster, einen Terminalsserver oder eine vergleichbare Lösung, so wird der Remote Content über das Netzwerk transportiert und dabei werden Unmengen an zusätzlichen Daten hinzugefügt. Das wiederum führt zu einer Verfälschung der Aufzeichnungen.

Um dieses Problem zu umgehen, versucht der Sniffer zunächst herauszufinden, ob eine Remote-Verbindung besteht. Dazu werden spezifische Umgebungsvariablen

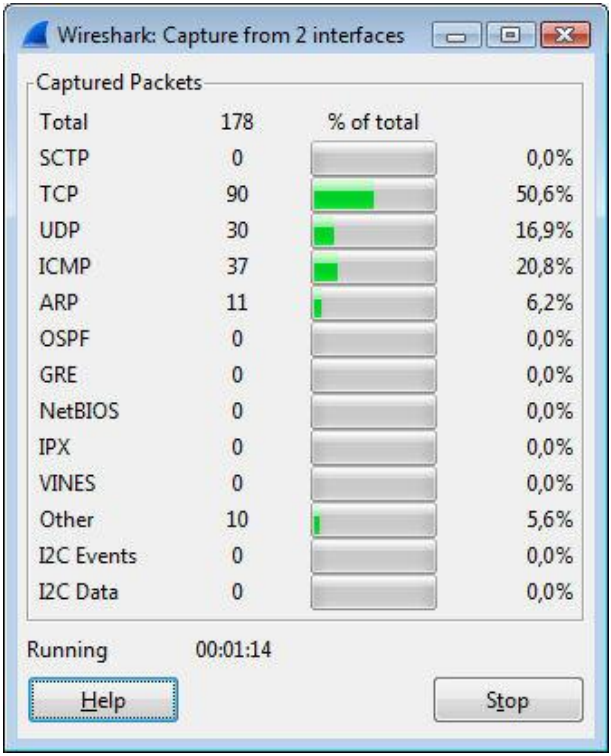
überprüft. Dann wird automatisch ein Capture-Filter erzeugt, der die spezifischen Verbindungseigenheiten abbildet und diese Informationen herausfiltert. Dabei werden die folgenden Umgebungsvariablen analysiert:

```
SSH_CONNECTION (ssh)
<Remote IP> <remote port> <local IP> <local port>

SSH_CLIENT (ssh)
<Remote IP> <remote port> <local port>

REMOTEHOST (tcsh oder andere)
<Remote-Name>

DISPLAY (x11)
[Remote Name]:<display num>

SESSIONNAME (Terminal Server)
<Remote Name>
```

Bei einem Windows-System stellt Wireshark fest, ob der Sniffer in einer Remote Desktop Services-Umgebung (Windows Terminal) läuft.

2.8 Capture-Vorgang in Aktion

Wireshark stellt Ihnen mit dem *Capture Info*-Dialog eine weitere interessante Funktion zur Verfügung, die Ihnen während einer laufenden Aufzeichnung die Gesamtzahl der bereits aufgezeichneten Pakete anzeigt.



Die *Capture Info*-Box.

Die Pakete werden nach den verschiedenen Protokollen aufgeschlüsselt. Dem Info-Dialog können Sie außerdem entnehmen, wie sich der Anteil der Aufzeichnung auf die verschiedenen Protokolle verteilt und wie lange die Aufzeichnung bereits läuft.

Der *Capture Info*-Dialog wird standardmäßig nicht nach dem Starten des Capture-Vorgangs eingeblendet. Sie müssen dazu die Option *Hide capture info dialog* in den Capture-Optionen deaktivieren.

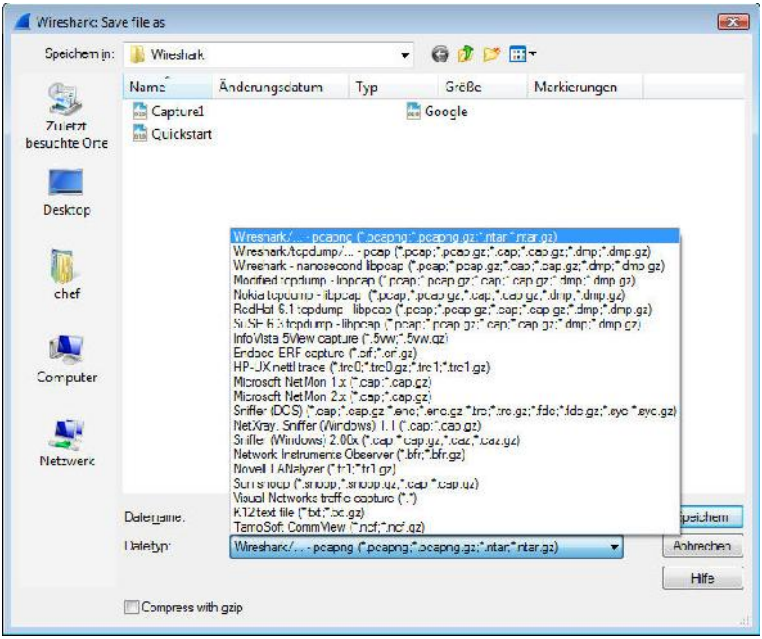
Sie können die Aufzeichnung einfach anhalten, indem Sie im *Capture Info*-Dialog auf *Stop* klicken. Leider ist ein Fortsetzen nicht möglich, da der Dialog mit dem Stoppen der Aufzeichnung geschlossen wird.

Ein Fortsetzen der Aufzeichnung ist nur über die *Restart*-Taste der Wireshark-Symbolleiste möglich.

3 Mit Aufzeichnungen hantieren

Die Live-Aufzeichnung von Netzwerk-Traffic ist eine der elementarsten Aufgaben von Wireshark. Doch häufig sichert man die Aufzeichnung, um sie zu einem späteren Zeitpunkt zu analysieren. Oftmals werden die Aufzeichnungen auch auf spezielle Analyserechner übertragen und einer späteren Analyse zugeführt. Wireshark stellt Ihnen hierfür umfangreiche Öffnen- und Speichern-Funktionen zur Verfügung. In diesem Kapitel schauen wir uns die verschiedenen Funktionen an, die Ihnen zum Hantieren mit Wireshark-Aufzeichnungen zur Verfügung stehen.

Wireshark stellt Ihnen nicht nur flexible Funktionen zum Speichern und Öffnen zur Verfügung. Vielmehr können Sie Ihre Aufzeichnungen flexibel zwischen verschiedenen Wireshark-Systemen austauschen, Dateien exportieren und sogar ausgewählte Inhalte ausdrucken. Sie können sogar Aufzeichnungen zusammenführen.



Wireshark unterstützt vielfältige Sicherungsformate.

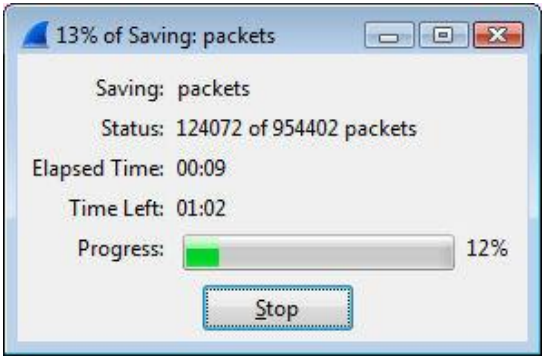
3.1 Aufzeichnungen speichern

Nachdem Wireshark entsprechend Ihrer Capture-Konfiguration den Traffic aufgezeichnet hat, können Sie Ihre Aufzeichnung sichern. Dazu führen Sie den Befehl *File > Save* bzw. *Save as*. In beiden Fällen präsentiert Ihnen Wireshark den gleichen Dialog *Wireshark: Save file as*.

Bestimmen Sie das Zielverzeichnis, in das die Aufzeichnung geschrieben werden soll. Weisen Sie der Datei eine Bezeichnung zu. Im Auswahlmenü *Dateityp* bestimmen Sie den Dateityp, den Sie Ihrer Aufzeichnung zuweisen wollen. Wireshark verwendet standardmäßig das Format *PCAPNG*. Sie können die Aufzeichnung auch durch das Aktivieren des Kontrollkästchens *Compress with GZIP* komprimieren.

Bei der Speicherung – auch ohne Komprimierung – gehen immer auch Ausgangsinformationen verloren. Während bei Vorgängerversionen von Wireshark hin und wieder formatspezifische Anpassungen für die Sicherung existierten, sind diese in der diesem Buch zugrundeliegenden Version 1.12.x nicht mehr vorhanden.

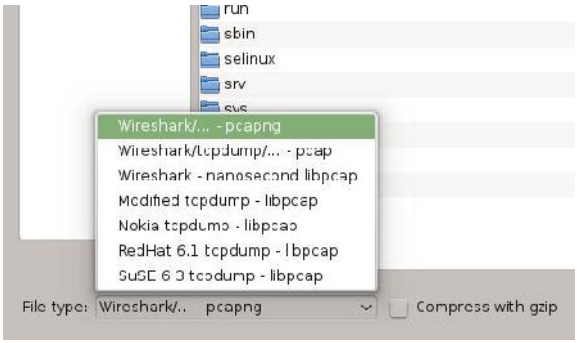
Mit einem Klick auf *Speichern* sichern Sie die Aufzeichnung. In einem Infodialog können Sie den Sicherungsvorgang verfolgen. Dem Dialog können Sie die Gesamtzahl der Pakete, die bereits gesicherte Zahl, die veranschlagte Dauer sowie die verbleidende Zeit für die Sicherung entnehmen. Die Fortschrittsanzeige zeigt Ihnen außerdem an, wie weit die Sicherung abgearbeitet ist.



Die Aufzeichnung wird gespeichert.

Wenn Sie die Sicherung unterbrechen wollen, klicken Sie auf die *Stop*-Schaltfläche. Wireshark bietet Ihnen folgende Möglichkeiten zur Speicherung:

- Wireshark – PCPNG
- Wireshark/tcpdump – PCAP
- Wireshark nanosecond Libcap – PCAP
- Modified tcpdump – LIBPCAP
- Noia tcpdump – LIBPCAP
- RedHat 6.1 tcpdump – LIBPCAP
- SuSE 6.3 tcpdump – LIBPCAP
- InfoVista 5 View Capture
- Endace ERF Capture
- HP-UX
- Microsoft NetMon 1.x und 2.x
- Sniffer (DOS)
- Network Instruments Observer
- Novell LANalyzer
- Sun snoop
- Visual Networks Traffic Capture
- K12-Textdatei
- TamoSoft CommView



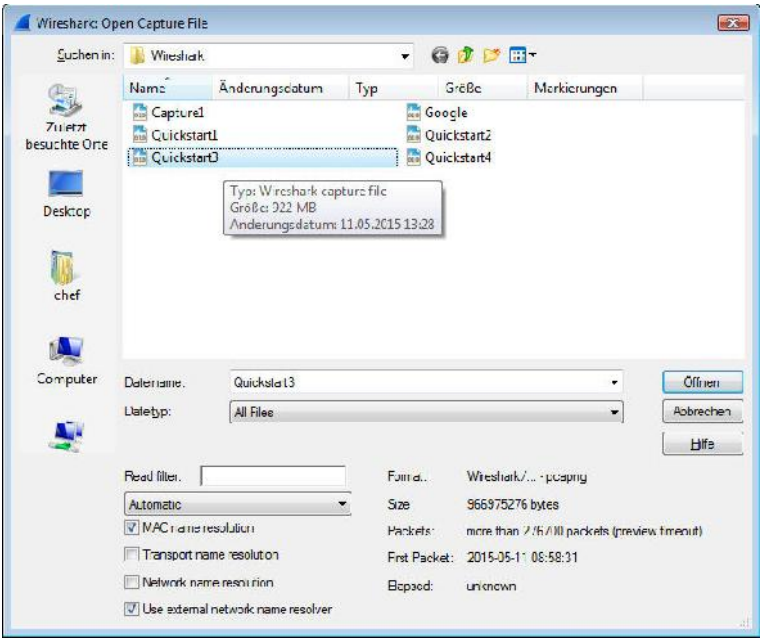
Die Sicherungsvarianten unter Linux.

Obige Liste gilt für die Sicherung Ihrer Aufzeichnungen unter Windows. Unter Linux sind Sie lange nicht so flexibel. Dort stehen Ihnen nur sieben Sicherungsformate zur Verfügung.

Da Wireshark-Aufzeichnungen sehr mächtig werden können, sollten Sie möglichst immer auch die Komprimierung mit Hilfe von GZIP aktivieren.

3.2 Aufzeichnungen öffnen

Nachdem Sie eine erste Aufzeichnung gesichert haben, können Sie diese zu einem späteren Zeitpunkt wieder öffnen und dann prüfen.



Der Öffnen-Dialog von Wireshark.

Der Sniffer legt die gesicherten Aufzeichnungen standardmäßig in einen eigens angelegten Ordner mit der Bezeichnung *Wireshark* ab. Wenn Sie Wireshark unter Windows ausführen, handelt es sich dabei um einen Unterordner des *Dokumente*-Ordners.

Wenn Sie eine gespeicherte Datei öffnen, so bietet Ihnen der *Öffnen*-Dialog zunächst die Möglichkeit, die gewünschte Ablage anzusteuern und durch die Wahl eines Dateiformats die Auswahl auf bestimmte Dateien zu beschränken. Indem Sie eine Datei in der Ablage markieren, werden im unteren Dialog das Format sowie verschiedene technische Details sowie die Größe und die Anzahl der Pakete eingeblendet.

Unter Linux können Sie mit einem Klick auf die Filterschaltfläche auf die Display-Filter zugreifen und so die Darstellung bereits beim Öffnen einschränken. Unter Windows müssen Sie den Filter manuell eingeben.

Sie können außerdem bestimmen, welche Namesauflösung auf die zu öffnende Datei angewendet wird. Mit einem Klick auf *Öffnen* laden Sie die Datei in Wireshark. Beachten Sie, dass die Aufzeichnungen meist sehr umfangreich sind und ein vollständiges Laden längere und/oder komplexe Aufzeichnungen einige Zeit beanspruchen kann.

Der einfachste Weg unter vielen Desktop-Betriebssystemen ist ansonsten das Öffnen per Drag&Drop: Markieren Sie einfach die gewünschte Datei bzw. Dateien (beispielsweise im Dateimanager) und ziehen Sie diese in das Wireshark-Fenster.

3.3 Aufzeichnungen zusammenführen

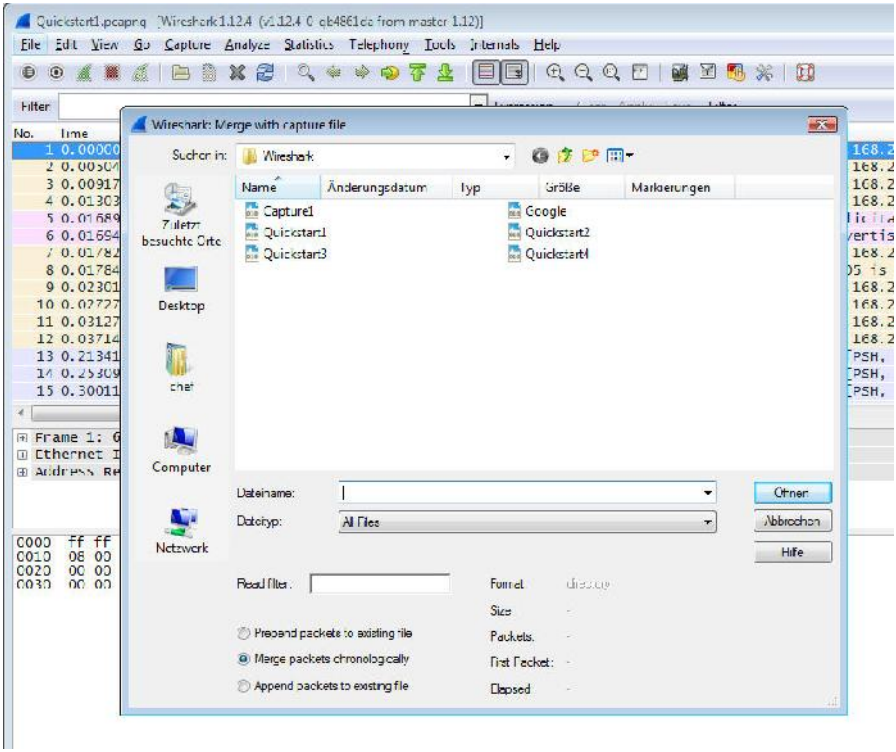
Wie wir in Kapitel 3.4 sehen werden, können Sie Ihre Aufzeichnungen in mehrere Dateien aufsplitten. Das ist für die Sicherung und Verarbeitung der Aufzeichnungen in der Regel von Vorteil. Doch für die spätere Analyse ist es oftmals auch sinnvoll, wenn man mehrere Dateien zu einer zusammenführt. Hierfür bietet Wireshark mehrere Möglichkeiten:

- Sie verwenden den *Merge*-Befehl, der über das *File*-Menü verfügbar ist.
- Sie ziehen mehrere Capture-Dateien in das Programmfenster. Wireshark versucht dann, diese anhand des Zeitstempels in der richtigen Reihenfolge aneinanderzureihen.
- Schließlich besitzt Wireshark noch das Konsolenwerk, mit dem Sie Dateien bündeln können.

Und dann bietet der Sniffer auch noch die Möglichkeit, Daten zu importieren.

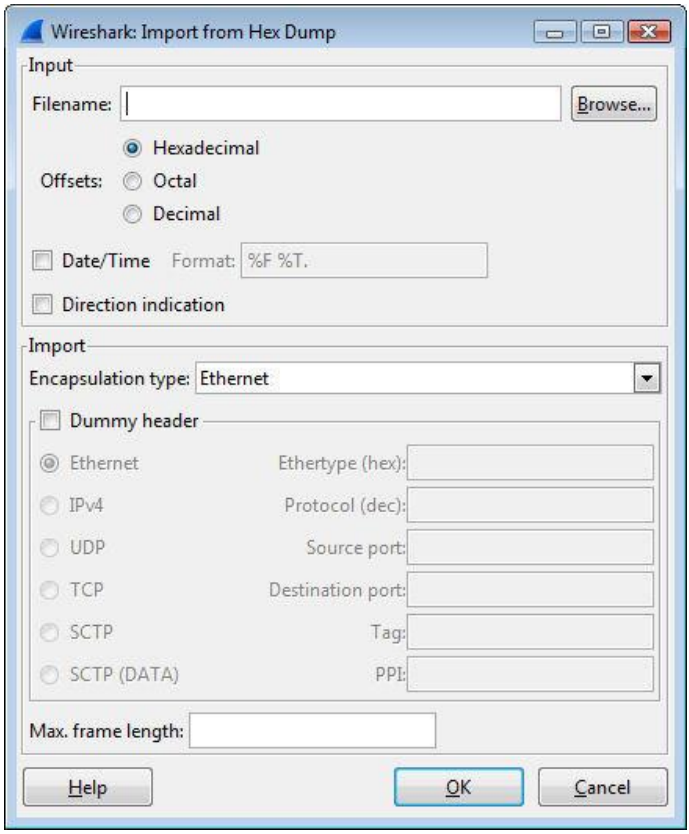
Besonders einfach ist das Zusammenführen (Mergen), wenn Sie bereits eine Datei geöffnet haben. Dann führen Sie den Menübefehl *File* > *Merge* aus. Im Merge-Dialog bestimmen Sie die weitere Capture-Datei, die Sie der bereits geöffneten

Datei hinzufügen wollen. Beim Zusammenführen können Sie wieder auf die Darstellungsfilter zurückgreifen. Unterhalb des Filters finden Sie drei Optionen, mit denen Sie bestimmen, ob die angehängte Datei chronologisch, vor oder nach der geöffneten Datei eingefügt wird.



Das Mergen von verschiedenen Capture-Dateien.

Wenn Sie von bereits durchgeführten Aufzeichnungssessions Paketdaten in Hexdump-Format besitzen und diese ebenfalls einer eingehenden Analyse mit Wireshark unterziehen wollen, können Sie entsprechende Dateien mit dem Menübefehl *File > Import from Hex Dump* importieren.



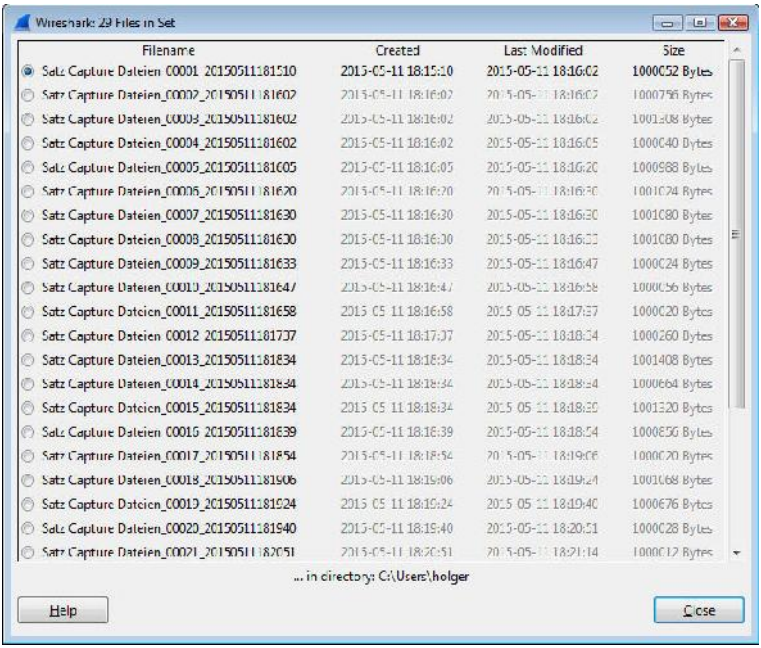
Der Import einer Hexdump-Datei.

Der Import einer solchen Datei ist einfach: Sie bestimmen unter *Input* die zu importierende Datei. Die Offset-Konfiguration *Hexadecimal* behalten Sie in der Regel bei. Im Bereich *Import* können Sie insbesondere den Encapsulation-Typ und den Header anpassen. Mit einem Klick auf *OK* führen Sie den Import durch.

3.4 Satz mit Capture-Dateien

Wenn Sie in den Capture-Optionen die Aufsplittung der Aufzeichnung konfiguriert haben, so stellt sich für Sie natürlich auch die Frage, wie man mit derlei Dateisätzen umgeht. Ein manuelles Handling der Dateien wäre umständlich, gerade auch bei sehr umfangreichen, netzwerkübergreifenden Aufzeichnungen.

Wireshark stellt uns zum Glück komfortable Funktionen für den Umgang mit diesen Datensätzen. Im *Capure Options*-Dialog weisen Sie dem Datensatz im Eingabefeld *Capture Files* eine Hauptbezeichnung zu. Wireshark legt die Teile im Benutzerordner ab, macht sie aber über GUI wie eine Einheit verfügbar.



Eine Aufzeichnung besteht aus 29 einzelnen Dateien.

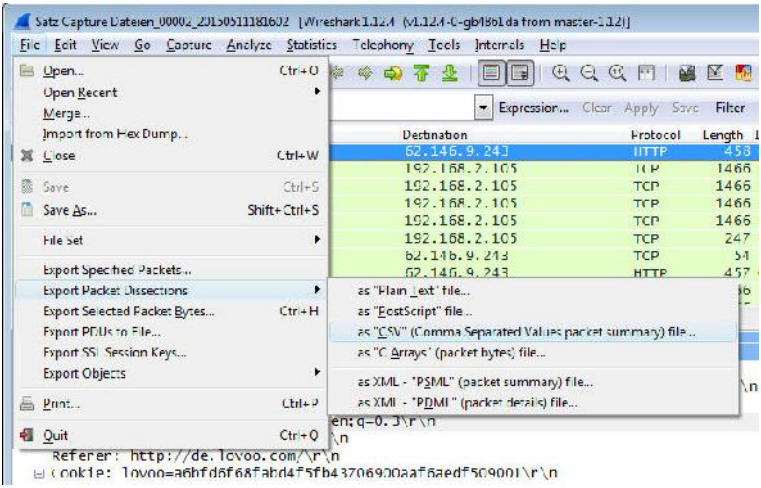
Über den Dialog, der die Dateien des Satzes aufführt, können Sie zu den einzelnen Paketinhalten navigieren. Wireshark aktualisiert diesen im Hintergrund. Der Vorteil dieser Vorgehensweise ist, dass Sie schnell in den Segmenten navigieren können. Auch alle weiteren Aktionen wie das Filtern und Suchen gehen wesentlich schneller von der Hand, als es bei mächtigen Aufzeichnungsdateien möglich ist.

Der Zugriff auf die Dateiliste erfolgt über das Menü *File* > *File Set* > *List Files*. Das *File Set*-Menü erlaubt auch das Wechseln zur nächsten Datei – und wieder zurück.

Mit einem Klick auf *Close* schließen Sie die Dateiliste und können wieder unmittelbar mit dem Aufzeichnungen arbeiten.

3.5 Datenexport

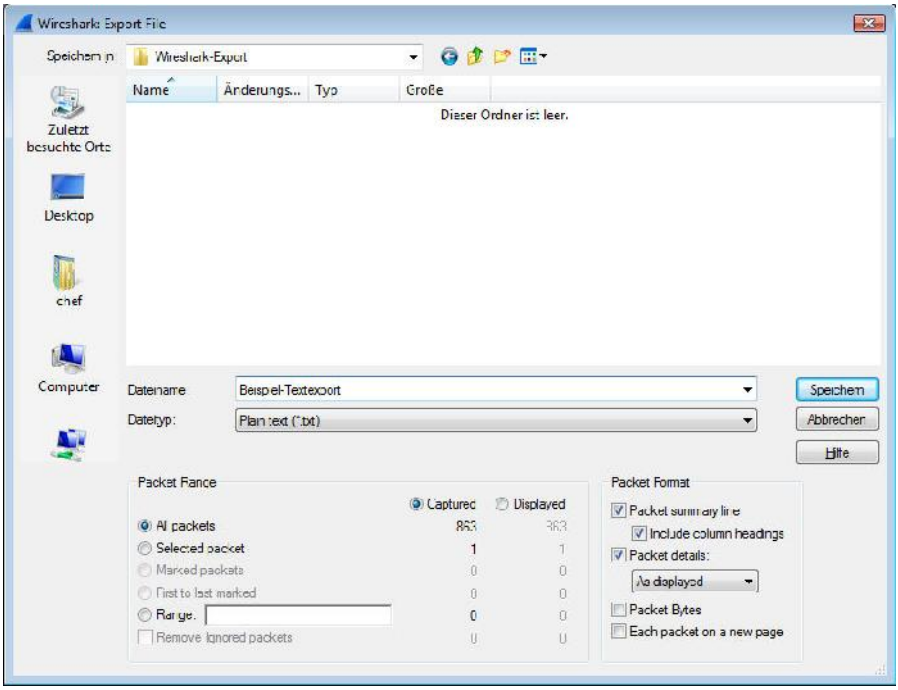
Das Speichern, Öffnen und Importieren von Dateien ist wichtig, um die eigenen Aufzeichnungen sichten zu können. Wenn Sie nun aber Ihre Aufzeichnungen anderen Anwendern zur Analyse oder Begutachtung überlassen wollen, müssen Sie dies häufig in einem Nicht-Wireshark-spezifischen Format tun. Das wiederum setzt eine Funktion voraus, mit der Sie Ihre Aufzeichnungen umwandeln können.



Wireshark verfügt über umfangreiche Exportfunktionen.

Wireshark bietet Ihnen verschiedene Exportmöglichkeiten für die aufgezeichneten Pakete. Die Exportfunktionen sind über das *File*-Menü verfügbar. Mit dem Menübefehl *File* > *Export Packet Dissection* > *as Plain Text file* können Sie die Pakete in eine Textdatei schreiben.

Verwenden Sie dabei den Bereich *Paket Range*, um festzulegen, ob alle Pakete oder nur ausgewählte Pakete exportiert werden sollen.



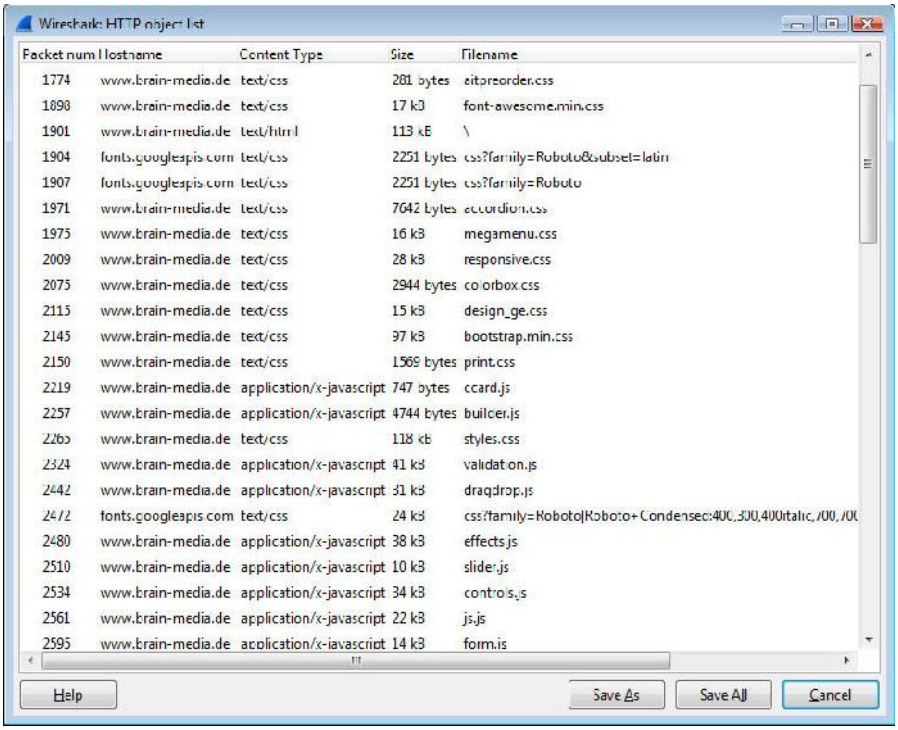
Der Textexport Ihrer Aufzeichnungen.

Die exportierte Textdatei können Sie dann mit einem Editor Ihrer Wahl öffnen und die Inhalte prüfen. Das ist oft einfacher, als die Aufzeichnungen mit dem Sniffer unter die Lupe zu nehmen.

Das gleiche Untermenü bietet Ihnen auch die Möglichkeit, Ihre Daten nach CSV, PDML und PostScript zu exportieren. Die beiden erstgenannten Formate eignen sich bestens, um die Aufzeichnungen in Drittprogrammen weiter zu verarbeiten.

Die Exportfunktion hat eine weitere Besonderheit zu bieten: Sie können aus den HTTP-Streams beispielsweise eingebettete Objekte herausfiltern und diese sogar speichern. Dazu führen Sie den Befehl *File > Export Object > HTTP* aus. Die Analysefunktion von Wireshark präsentiert Ihnen eine Tabelle, der Sie den Hostnamen, den Content-Typ, die Größe und den Datei entnehmen können.

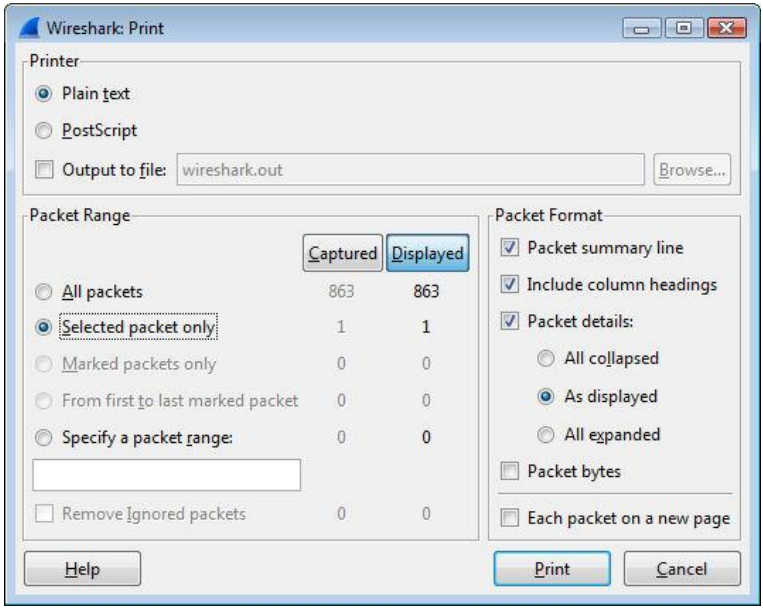
Durch Markieren können Sie einzelne Objekte sichern. Alternativ können Sie mit *Save all* auch alle Objekte sichern.



Der Objektexport.

3.6 Paketliste drucken

Auch wenn es eher die Ausnahme als die Regel sein dürfte, so können Sie Ihre Aufzeichnung dennoch auch über einen Drucker ausgeben und diesen dann in Papierform untersuchen oder zur Analyse weiterreichen. Beachten Sie allerdings bei einer Druckausgabe, dass diese schnell Hunderte Seiten füllt.



Der Druckdialog von Wireshark.

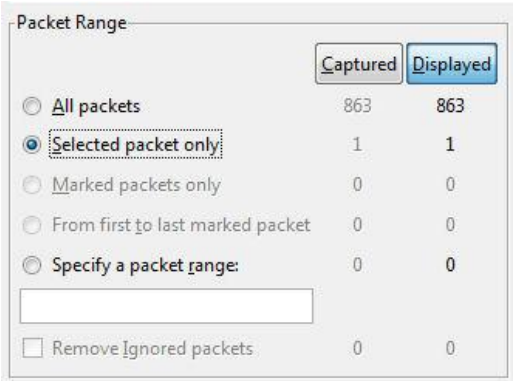
Die Druckausgabe steuern Sie über den Druckdialog, den Sie mit dem Menübefehl *File > Print* aufrufen. Alternativ verwenden Sie die Tastenkombination *Strg + P*. Der zugehörige Druckdialog ist ein wenig irreführend, denn im Bereich *Printer* findet man nicht die Druckerauswahl, sondern vielmehr die Konfiguration des Druckformats. Hier stehen Ihnen drei Formate zur Auswahl:

- **Plain text**: Diese Option erzeugt reinen Text in der Druckausgabe.
- **PostScript**: Für eine bessere gestalterische Ausgabe, verwenden Sie diese Option. Diese Option sollte nur bei PostScript-fähigen Druckern verwendet werden.

- **Output to file**: Diese Druckoption schreibt die Druckausgabe in einer Datei, deren Dateiname und Verzeichnis Sie bestimmen. Standardmäßig schreibt Wireshark in die Datei *wireshark.out*.Sie können natürlich auch jede andere Bezeichnung verwenden.

3.7 Paketbereich und Format

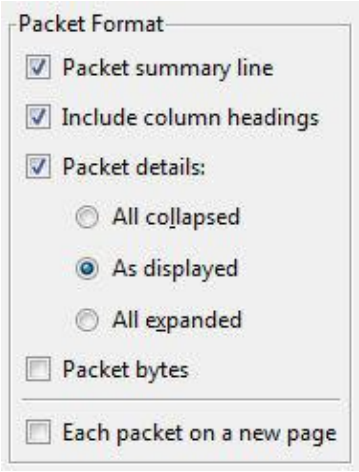
Im Druck- und Exportdialog begegnen Sie immer wieder zwei Bereichen, die ich in diesem Abschnitt gebündelt besprechen möchte: *Packet Range Frame* und *Packet Format Frame*. Mit dem Range Frame bestimmen Sie den Paketbereich, mit dem Format Frame den Umfang der Ausgabe.



Die Konfiguration des Paketbereichs.

Mit dem Paketbereich legen Sie fest, ob die Ausgabe auf alle aufgezeichneten Pakete bzw. nur ausgewählte und markierte Bereiche angewendet wird. Mit dem Eingabefeld *Specify a packet range* können Sie auch einen spezifischen Bereich ausgeben. Eine entsprechende Ausgabe kann wie folgt aussehen: *10-20, 100-200, 300-*.

Mit Hilfe des Bereichs *Packet Format* bestimmen Sie, welche Informationen in der Ausgabe enthalten sein sollen. Standardmäßig ist mit *Packet summary line* eine Zusammenfassung enthalten. Unter *Packet Details* bestimmen Sie, ob alle Details in der Ausgabe aufgeführt werden. Der Übersichtlichkeit wegen können Sie durch Aktivieren der Option *Each packet on a new page* jedes Paket auf einer neuen Seite ausgeben.

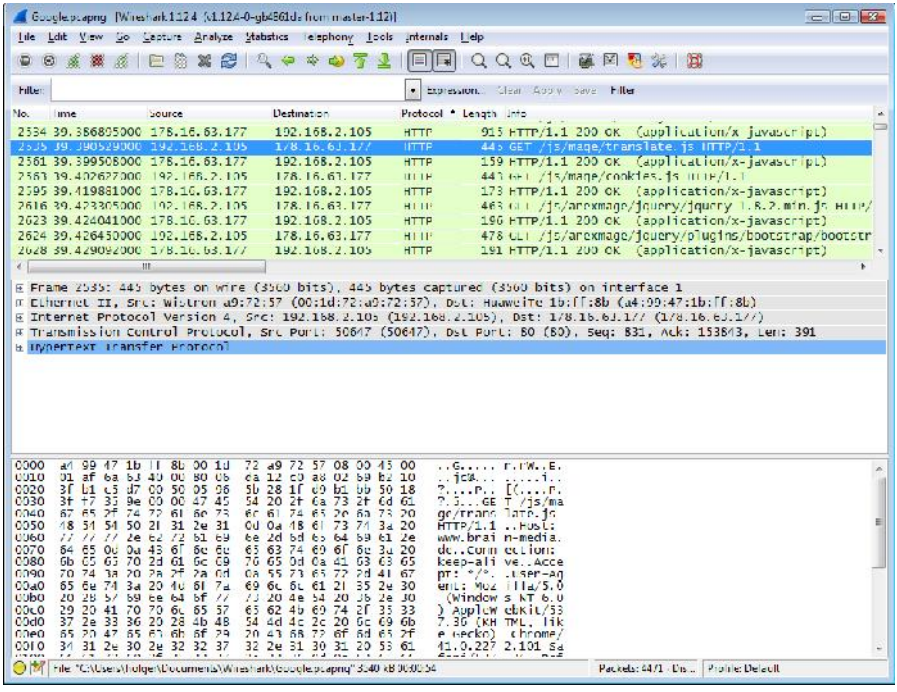


Die Konfiguration des Paketformats für die Ausgabe.

4 Mit Aufzeichnungen arbeiten

Wireshark unterstützt die Echtzeit- und die spätere Analyse von Aufzeichnungen. Meist kann man erst bei einer Analyse eines längeren Zeitraums bestimmte Schwachstellen und Netzwerkanomalien aufdecken. Die bei einer Live-Analyse zu finden, ist nahezu unmöglich. Hier müssen Sie die Netzwerkaktivitäten über einen längeren Zeitraum hinweg aufzeichnen und dann einer sorgfältigen Analyse unterziehen.

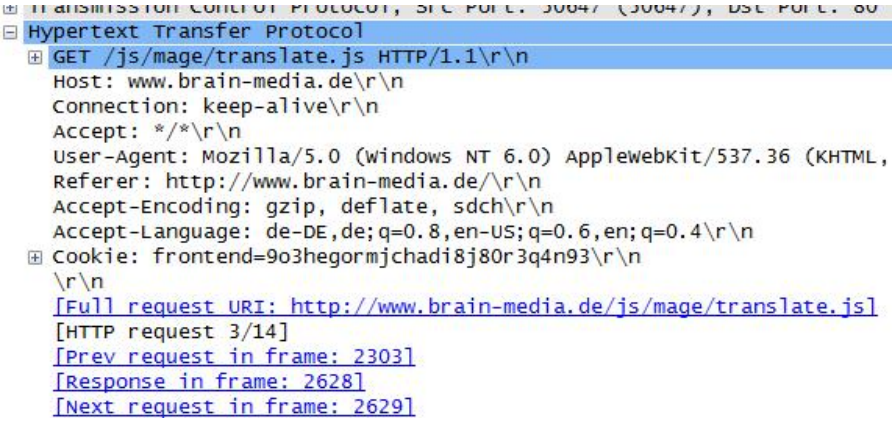
Sie haben im vorangegangenen Kapitel verschiedene Möglichkeiten von Wireshark zur Aufzeichnung und Sicherung kennengelernt. Gerade auch solche, mit denen Sie längere Zeiträume aufzeichnen können – Stichwort Aufzeichnung aufsplitten.



Eine gespeicherte Aufzeichnung in Wireshark.

Nachdem Sie eine Aufzeichnung geöffnet haben, können Sie sich mit den vielfältigen Funktionen, die Wireshark zu bieten hat, an die Analyse machen. Sie können durch Markieren eines Pakets in der Paketliste die zugehörigen Informationen in den weiteren Ansichten aktivieren.

In der Detailansicht können Sie dann über das Pluszeichen bzw. ein entsprechendes Symbol auf die Detailinformationen zugreifen. Nachstehende Abbildung zeigt einen aufgeklappten Eintrag des HTTP-Protokolls. Der kann weiter aufgeklappt werden, um beispielsweise Informationen zum Austausch von HTTP-Kommandos, Cookies etc. abzurufen.

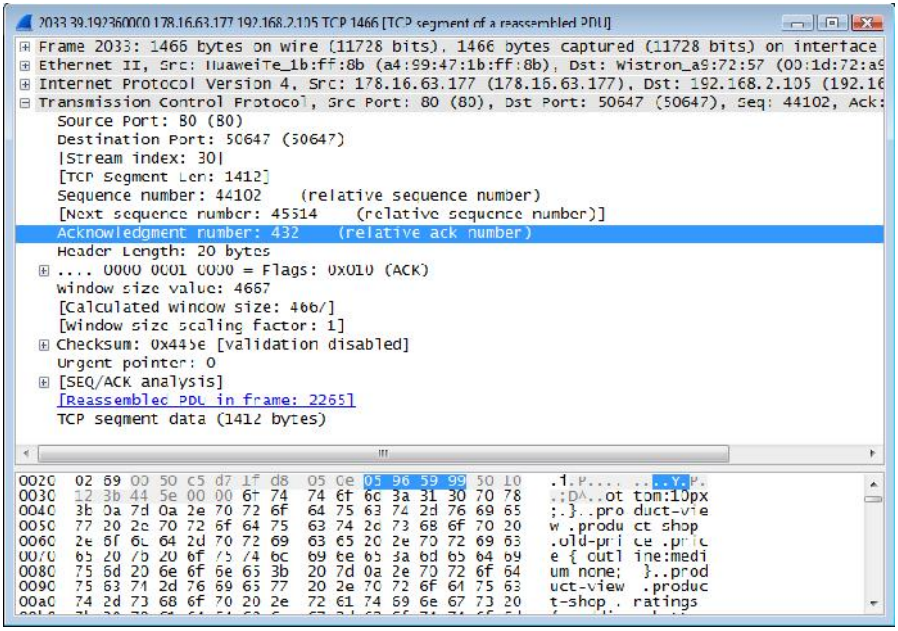


Ein aufgeklappter Eintrag in der Detailliste.

Wireshark zeichnet bei einer typischen Session meist Tausende Datenpakete auf. Bei dieser Informationsflut ist es alles andere als einfach, sich durch die Aufzeichnungen zu bewegen und die relevanten Informationen konzentriert zu analysieren.

Die Paketanalyse vereinfacht sich, indem Sie das Paket in einem neuen Fenster öffnen. Dazu klicken Sie doppelt auf einen Paketeintrag in der Paketliste. Alternativ markieren Sie den gewünschten Eintrag und führen den Menübefehl *View > Show Packet in New Window* aus.

Auf diesem Weg können Sie auch zwei oder mehr Pakete parallel öffnen und die Inhalte miteinander vergleichen.



Ein Paket in einem eigenen Fenster.

4.1 Mit Kontextmenüs arbeiten

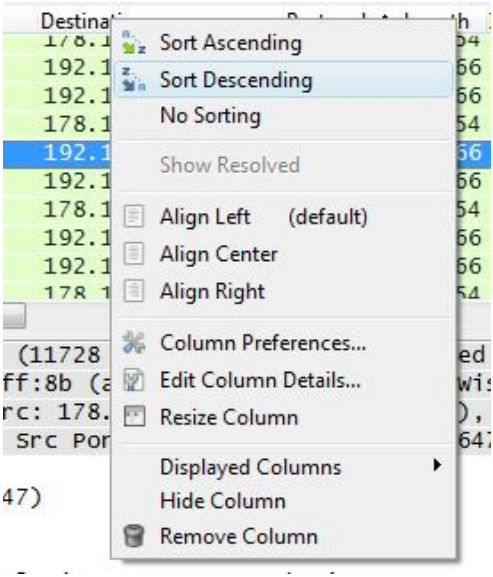
Wireshark bietet nicht nur umfangreiche Ansichts- und Capture-Filter, sondern eine Vielzahl an interessanten Funktionen, um die Ansichten zu bearbeiten und um die Darstellung anzupassen. Hier sind insbesondere die Kontextmenüs der rechten Maustaste eine große Hilfe.

Alleine für die Paketliste stehen Ihnen zwei unterschiedliche Kontextmenüs zur Verfügung: Das eine öffnen Sie, indem Sie mit der rechten Maustaste in die Kopfzeile klicken, das andere mit einem Klick in die Paketliste.

Mit einem Rechtsklick in den Kopf der Paketliste öffnen Sie das Kontextmenü, das Ihnen folgende Funktionen zur Verfügung stellt, wobei die Einstellungen und Funktionen für die Spalte gelten, auf die Sie klicken:

- **Sort Ascending**: Diese Funktion sortiert die Einträge in aufsteigender Richtung. Bei Buchstaben beispielsweise in aufsteigender alphabetischer Richtung, bei Zahlen oder Daten entsprechend aufsteigend.

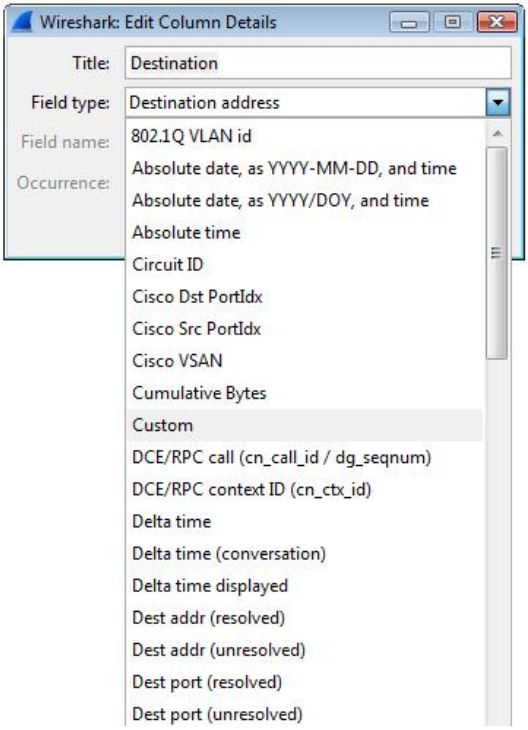
- **Sort Descending**: Diese Sortierung verwendet die absteigende Reihenfolge. Bei Protokollen also beispielsweise von UDP nach ARP. In der Protokollspalte steht Ihnen hierfür auch das Pfeilsymbol neben der Header-Bezeichnung *Protocol* zur Verfügung. Prinzipiell können Sie in allen Spalten die Reihenfolge mit einem Klick in die Kopfzeile ändern.
- **No Sorting**: Diese Funktion entfernt die gewählte Sortierung der markierten Spalte.
- **Show Resolved**: Wie wir weiter unten noch sehen werden, kann Wireshark auch Hostnamen auflösen. Sofern das geschehen ist, können Sie mit dieser Funktion die Ansicht auf bereits aufgelöste Adressen beschränken.



Das Kontextmenü der rechten Maustaste beim Klick in den Paketlisten-Header.

- **Align Left**: Richtet die Spalteneinträge links aus.
- **Align Center**: Richtet die Spalteninhalte mittig aus.
- **Align Right**: Diese Option richtet die Listeneinträge rechts aus.

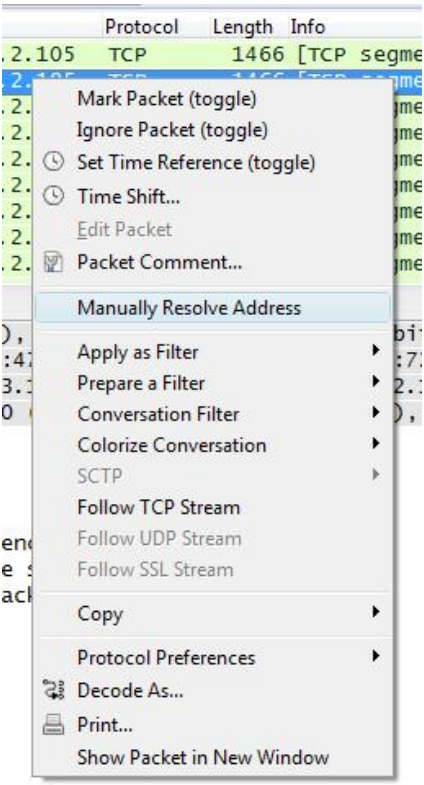
- **Column Preferences**: Mit diesem Befehl greifen Sie auf die Spaltenkonfiguration der Wireshark-Programmeinstellungen zu. Damit können Sie neue Spalten hinzufügen und nicht benötigte wieder entfernen. Wir kommen in Kapitel 7 detailliert auf diese Einstellungen zu sprechen.
- **Edit Column Details**: In dem zugehörigen Dialog können Sie den Titel und den Feldtyp ändern. Das Auswahlmenü *Field type* stellt Ihnen alle von Wireshark unterstützen Typen zur Auswahl.



Die editierten Spaltendetails.

- **Resize Column**: Passt die Spaltenbreite so an, dass die Inhalte in die jeweiligen Spalten passen.

- **Display Columns**: Dieses Untermenü erlaubt Ihnen das Ein- und Ausblenden der konfigurierten Spalten. Die entsprechenden Spalten können in der Paketliste ein- und ausgeblendet werden.
- **Hide Column**: Blendet die markierte Spalte aus. Sie kann dann über das Menü *Display Columns* wieder eingeblendet werden.
- **Remove Column**: Entfernt eine Spalte dauerhaft aus der Paketliste.

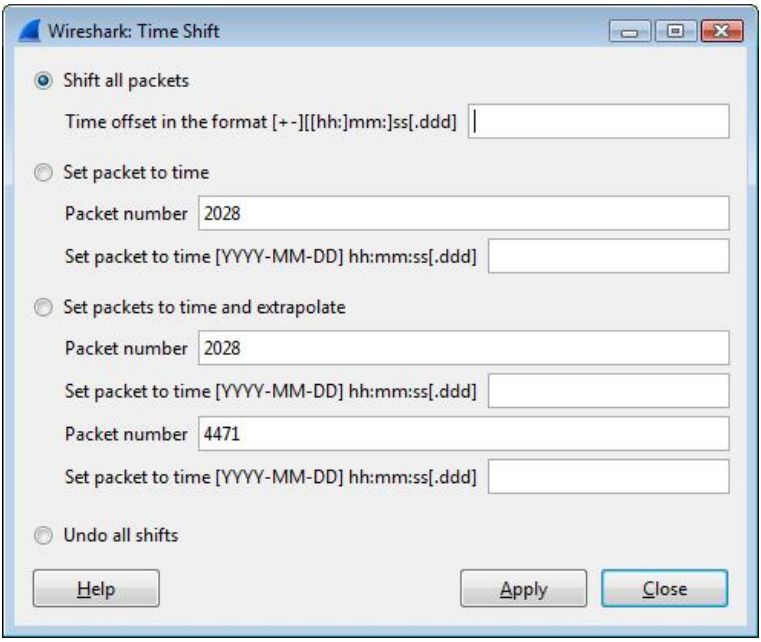


Das Kontextmenü in der rechten Maustaste in der Paketliste.

Innerhalb der Paketliste steht Ihnen ein noch weit umfangreicheres Kontextmenü zur Verfügung, mit dem Sie eine Fülle von Funktonen ausführen, die ansonsten aber auch über die Menüs *Edit* und *Analyze* zu finden sind. Damit erleichtert sich insbesondere die Paketanalyse.

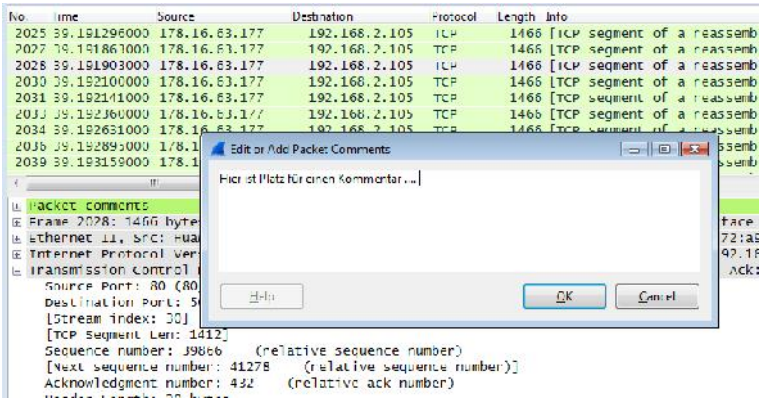
Die Befehle im Überblick:

- **Mark Packet (toggle)**: Markiert ein Paket bzw. hebt die Markierung wieder auf. Alternativ verwenden Sie die Tastenkombination *Strg + M*. Diesen Befehl finden Sie auch im *Edit*-Menü.
- **Ignore Packet**: Ignoriert das markierte Paket bzw. markiert es für die Analyse. Alternativ verwenden Sie die Tastenkombination *Strg + D*. Diesen Befehl finden Sie auch im *Edit*-Menü.
- **Set Time Reference (toogle)**: Setzt eine Zeitreferenz in dem markierten Datenpaket. Das erkennen Sie nach dem Setzen an dem Eintrag **REF** in der *Time*-Spalte.
- **Time Shift**: Dieser Dialog erlaubt Ihnen das Ändern des Zeit-Offsets. Sie können den neuen Zeitwert auf alle oder nur auf Pakete in einem bestimmten Zeitfenster vornehmen.



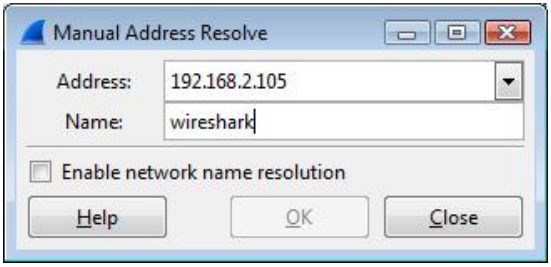
Die *Time Shift*-Funktion.

- **Packet Comment**: Während einer Datenanalyse ist es immer wieder praktisch, wenn man Anmerkungen und Notizen in den bereits abgearbeiteten Paketen vornehmen kann. Diese Funktion stellt Ihnen einen einfachen Eingabedialog zur Verfügung, in den Sie Ihre Aufzeichnungen eingeben können. Nun stellen Sie die berechtigte Frage, wo man denn die Anmerkungen und Aufzeichnungen später findet? Auch das ist einfach: Wireshark erstellt in der Detailansicht einen Ordner *Packet Comments*, in dem Sie die Kommentare später finden.



Die Kommentarfunktion in Aktion.

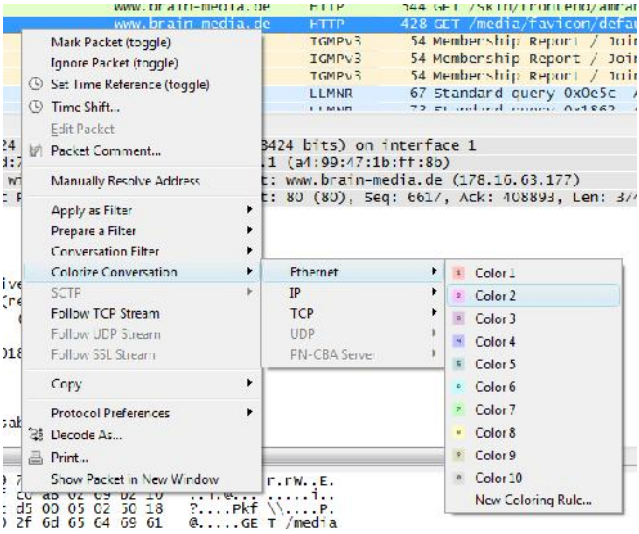
- **Manual Address Resolve**: Mit dem zugehörigen Dialog können Sie einer IP-Adresse manuell einen Hostnamen zuweisen. Die Änderungen werden anschließend über die gesamte Aufzeichnungsdatei hinweg vorgenommen.



Die manuelle Adressauflösung.

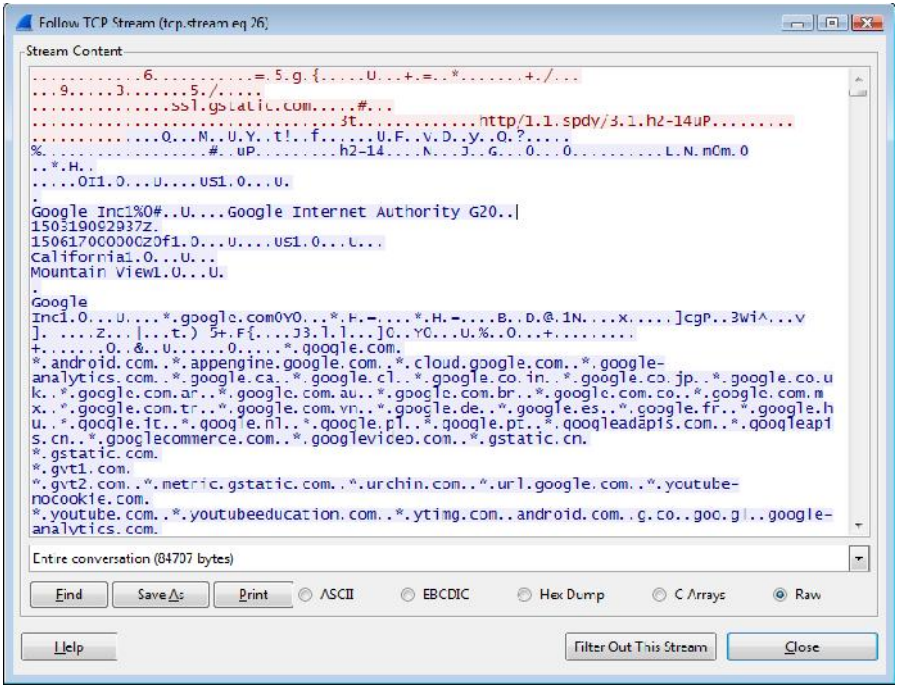
- **Apply as Filter**: Dieses Untermenü erlaubt es Ihnen, die Darstellung auf Grundlage eines markierten Pakets einzuschränken. Es handelt sich dabei um einen Ansichtsfilter. Sie können dabei den Filter mit logischen Operatoren verwenden:
  - Wie gewählt
  - Nicht gewählt
  - Und markiert
  - Oder markiert
  - Und nicht markiert
  - Oder nicht markiert

- **Prepare as Filter**: Diese Option bereitet die Auswahl als Filter vor – im Unterschied zur Anwendung (*Apply as Filter*).
- **Conversion Filter**: Dieser Darstellungsfilter verwendet die Adressinformationen des gewählten Pakets. Haben Sie beispielsweise ein Paket mit dem IP-Protokoll markiert, so wird die Ansicht auf den Traffic zwischen zwei IP-Adressen beschränkt.



Die Regeln für die Farbkennzeichnung.

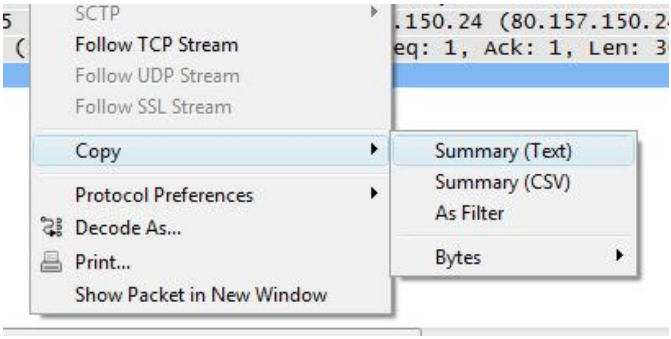
- **Colorize Conversation**: Dieses Untermenü stellt Ihnen umfangreiche Möglichkeiten zur farbigen Kennzeichnung unterschiedlichen Traffics zur Verfügung. Sie können insbesondere Ethernet, IP, TCP und UDP-Traffic farblich kennzeichnen.
- **SCTP**: Dieses Untermenü erlaubt Ihnen die Analyse und das Anwenden eines Filters auf SCTP-Traffic (Stream Control Transmission Protocol).



Das Folgen eines TCP-Streams.

- **Follow TCP Stream**: Mit dieser Funktion können Sie einem TCP-Stream zwischen zwei Knoten folgen. Auf diese Weise stellen Sie exakt fest, welche Daten zwischen zwei Systemen geflossen sind. Der zugehörige Darstellungsfilter lautet *tcp.stream*.
- **Follow UDP Stream**: Entsprechend können Sie auch einem UDP-Stream folgen und den UDP-Traffic zwischen zwei Systemen unter die Lupe nehmen.

- **Follow SSL Stream**: Mit dieser Funktion können Sie dem SSL-Traffic zwischen zwei Knoten folgen. Diese und auch die beiden voranstehenden Folgefunktionen sind über das Menü *Analyse* verfügbar.



Die Kopierfunktion von Wireshark.

- **Copy**: Dieses Untermenü stellt Ihnen verschiedene Kopiermöglichkeiten zur Verfügung, mit denen Sie Ihre Inhalte kopieren und dann in Drittanwendungen weiter verarbeiten können. Das Menü erlaubt Ihnen mit *Summary (Text)* das Kopieren der Paketzusammenfassung in Textform. Den in die Zwischenablage kopierten Text können Sie dann an anderer Stelle einfügen. Ein entsprechender Eintrag sieht wie folgt aus:

```
63778  515.952034000192.168.2.105178.16.63.177HTTP
       342    GET / HTTP/1.1
```

  Sie können die Paketzusammenfassung auch als CSV-Datei kopieren und dann beispielsweise in einer Tabellenkalkulation oder Datenbank verarbeiten. Hierzu führen Sie den Befehl *Summary (CSV)* aus. Der entsprechende kommaseparierte Eintrag sieht wie folgt aus:

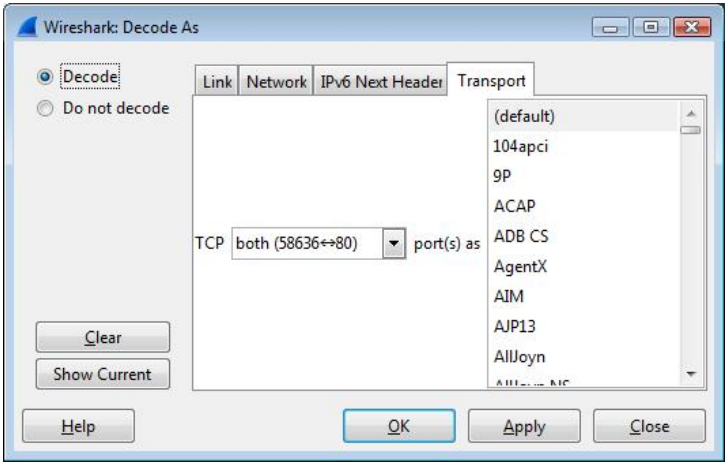
```
"63778","515.952034000","192.168.2.105","178.16.63.177"
,"HTTP","342","GET / HTTP/1.1 "
```

  Sie können die kopierten Inhalte auch als Darstellungsfilter verwenden. Dazu führen Sie den Befehl *Copy > As Filter* aus. Mit diesem Befehl kopieren Sie die Filterbedingung in die Zwischenablage und fügen diese dann in das Filterfeld ein:

```
ip.dst == 178.16.63.177
```

Schließlich können Sie mit dem Untermenü *Bytes* verschiedene weitere Byte-Darstellungen in die Zwischenablage kopieren und weiterverarbeiten.

- **Protocol Preferences**: Über dieses Menü greifen Sie auf die Wireshark-Programmeinstellungen zu, in denen Sie Art der Darstellung und Auswertung bestimmen. Wir kommen in Kapitel 7 noch einmal auf diese Einstellungen zu sprechen.



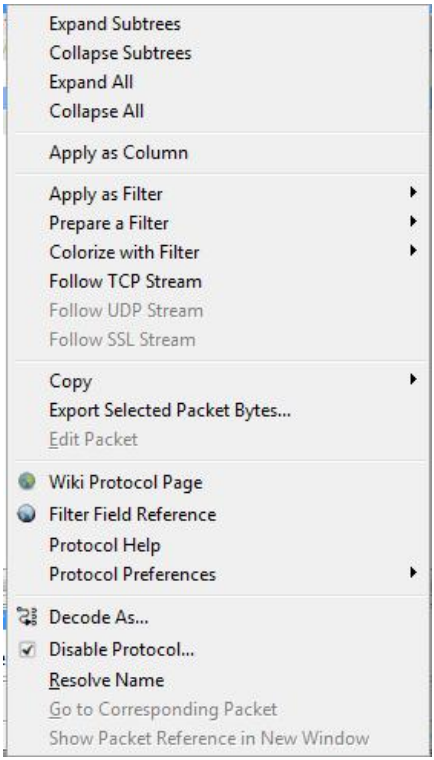
Die Beziehung zwischen zwei Dissektoren.

- **Decode as**: Mit den Funktionen des zugehörigen Dialogs können Sie die Beziehung zwischen zwei Dissektoren neu konfigurieren. Der *Decode as*-Dialog bietet Ihnen je nach Protokoll verschiedene Anpassungsmöglichkeiten. Der Befehl ist auch über das *Analyze*-Menü verfügbar.
- **Print**: Öffnet den Druckdialog, den Sie in Kapitel 3.6 kennengelernt haben. Er erlaubt die Druckausgabe der Paketliste.
- **Show Packet in New Window**: Auch diesen Befehl kennen Sie bereits. Er öffnet das markierte Datenpaket in einem neuen Fenster. Dieser Befehl ist auch über das *View*-Menü verfügbar.

4.2 Kontextmenü in der Detailansicht

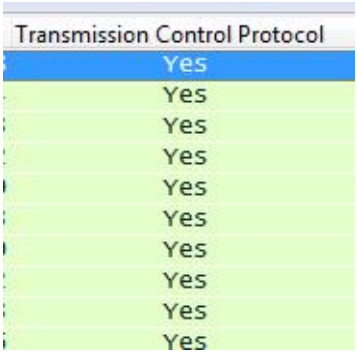
Auch in der Detailansicht steht Ihnen das Kontextmenü der rechten Maustaste zur Verfügung. Damit können Sie je nach markiertem Inhalt folgende Aktionen ausführen:

- **Expand Subtrees**: Mit diesem Menübefehl klappen Sie alle Zweige des markierten Elements auf.
- **Collapse Subtrees**: Entsprechend klappen Sie mit diesem Untermenü alle Zweige der markierten Elemente wieder ein.
- **Expand All**: Mit diesem Befehl klappen Sie alle Äste auf.
- **Collapse All**: Hiermit klappen Sie entsprechend alle Äste ein. All diese vier Befehle sind auch über das *View*-Menü verfügbar.



Das Kontextmenü der rechten Maustaste in der Detailansicht.

- **Apply as Column**: Führen Sie diesen Befehl aus, um das verwendete Protokoll der Paketliste hinzuzufügen. Dabei wird eine neue Spalte erzeugt, der Sie dann die Verwendung des Protokolls entnehmen können.



Das Protokoll TCP ist nun auch in der Paketliste zu finden.

- **Prepare a Filter**: Bereitet einen Filter auf Grundlage des markierten Elements vor.
- **Colorize with Filter**: Verwendet das markierte Element als Darstellungsfilter und weist ihm dabei die gewünschte Farbmarkierung zu.
- **Follow TCP/UDP/SSL Stream**: Diese Funktion entspricht der in Abschnitt 6.1 beschriebenen Verfolgung eines Protokollstromes.

! **Hinweis**

Beachten Sie, dass das Kontextmenü der rechten Maustaste nur in der Detailansicht verfügbar ist, solange Sie sich im Hauptfenster befinden. Wenn Sie ein Datenpaket in einem neuen Fenster geöffnet haben, steht das Menü nicht zur Verfügung.

- **Copy**: Auch in der Detailansicht steht Ihnen eine Kopierfunktion zur Verfügung. Die ist über das Untermenü *Copy* verfügbar. Wenn Sie einen HTTP-Request in der Detailansicht markiert haben und die Beschreibung (Description) kopiert haben und dann an anderer Stelle einfügen, sieht das wie folgt aus:

```
Request Method: GET
```

Bei anderen markierten Zeilen entsprechend anders:

```
Request Version: HTTP/1.1
```

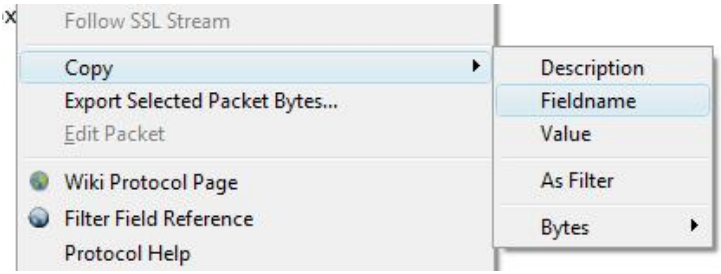
Bleiben wir bei dem Beispiel des HTTP-Requests. Sie können auch einen Feldnamen in die Zwischenablage kopieren. Das sieht dann wie folgt aus:

```
http.request.method
```

Im Falle des HTTP-Requests lautet der kopierte Wert (*Value*) dann:

```
GET
```

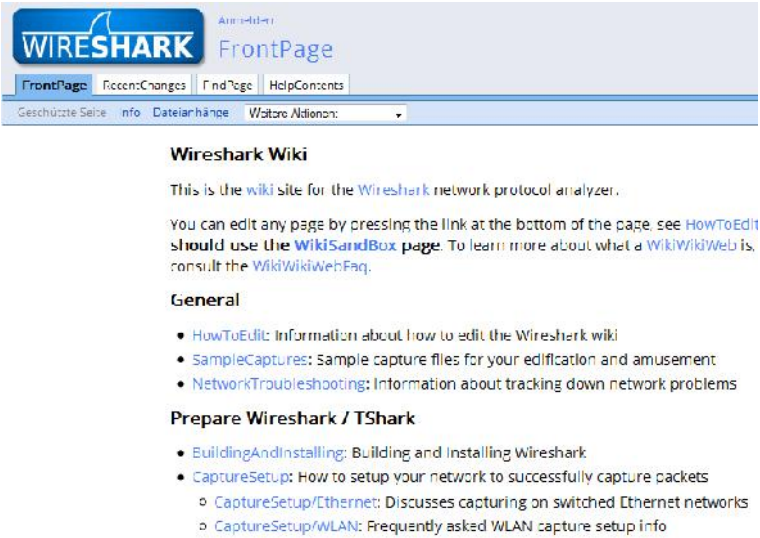
Sie können in der Detailansicht außerdem die Markierung als Filter verwenden und Inhalte Byte-weise kopieren.



Die Kopierfunktion in der Detailansicht.

- **Export Selected Packet Bytes**: Dieser Menübefehl öffnet den Exportdialog, der den Export der Paketdaten erlaubt, insbesondere ins RAW-Format.
- **Edit Packet**: Dieses Untermenü ist in meiner Wireshark-Installation nicht belegt. Es scheint, also könnte man hier einen externen Paketeditor wie beispielsweise WireEdit (*https://wireedit.com*) einbinden. Wireshark ist hervorragend für die Aufzeichnung und Analyse geeignet, nicht aber für das Editieren. Wie wir im Anhang noch sehen werden, verfügt Wireshark zwar mit editcap über ein Konsolenwerkzeug, bei dem man eine entsprechende Funktionalität vermuten könnte. Aber die wichtigste Aufgabe von

editcap ist das Entfernen von Paketen aus den Capture-Dateien. Auch die Konvertierung in andere Formate ist damit möglich.



Das Wireshark-Wiki bietet jede Menge technisches Hintergrundwissen.

Die vier nächsten Funktionen bringen Sie zu weiterführenden Informationen bzw. zu den jeweiligen Protokolleinstellungen des Sniffers:

- **Wiki Protocol Page**: Das Wireshark-Team betreibt ein umfangreiches Wiki, in dem Sie jede Menge Hintergrundinformationen zu den verschiedenen Protokollen finden. Die Wiki-Seite bezieht sich immer auf das gerade markierte Protokoll.
- **Filter Field Reference**: Entsprechend können mit diesem Befehl die Feldreferenz öffnen. Auch hier greift Ihre Wireshark-Installation auf die webbasierte Dokumentation zurück.
- **Protocol Help**: Diese Funktion scheint in Wireshark 1.12.x nicht belegt zu sein.
- **Protocol Preferences**: Öffnet die Protokollvoreinstellungen, in denen Sie protokollspezifische Anpassungen vornehmen können. Mehr dazu in Kapitel 7.

Es folgt die letzte Funktionsgruppe des Kontextmenüs mit fünf weiteren Einstellungen und Funktionen:

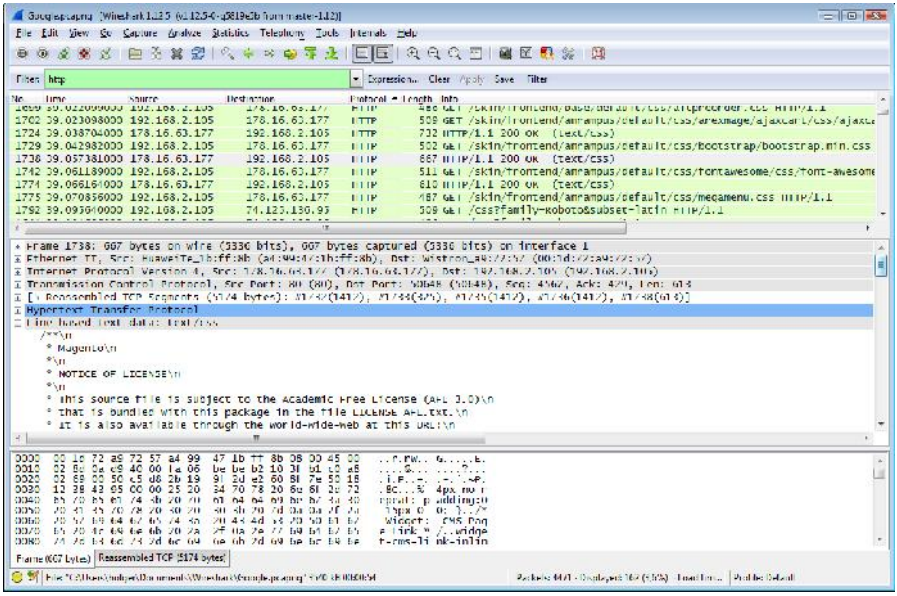
- **Decode As**: Öffnet den Zuweisungsdialog für die Verknüpfung zweier Dissektoren.
- **Disable Protocol**: Deaktiviert den Protokoll-Dissektor temporär.
- **Resolve Name**: Führt eine Namensauflösung für das markierte Paket aus, nicht aber für alle Pakete.
- **Go to Corresponding Packet**: Besitzt das markierte Datenpaket ein korrespondierendes Paket, so wechseln Sie mit diesem Befehl zu dem Paket. Korrespondierende Pakete begegnet man meist bei Request-Response-Vorgängen.
- **Show Packet Reference in New Window**: Öffnet die Paketreferenz in einem neuen Fenster. So können die Pakete einfach miteinander verglichen werden.

Damit kennen Sie die wichtigsten Funktionen für die Analyse in den verschiedenen Ansichten. Da Sie nun die Navigation, die Sortierung und das Hantieren mit Ihren Aufzeichnungen beherrschen, schauen wir uns als Nächstes an, wie Sie exakt die Daten aufspüren, die für Sie relevant sind.

5 Mit Filtern jonglieren

Aus Kapitel 1 wissen Sie, dass Wireshark zwei verschiedene Filtertypen kennt: Aufzeichnungs- und Darstellungsfilter. Die Verwendung der Capture-Filter kennen Sie bereits. In diesem Kapitel schauen wir uns an, wie Sie die Ansicht Ihrer Aufzeichnungen mit den Darstellungsfiltern gezielt einschränken.

Das Prinzip der Darstellungsfilter ist einfach: Sie blenden die Informationen aus, die für Sie nicht oder noch nicht von Interesse sind und reduzieren so die gigantischen Datenmengen auf das Wesentliche.



Der Einsatz eines simplen Darstellungsfilters: *http*.

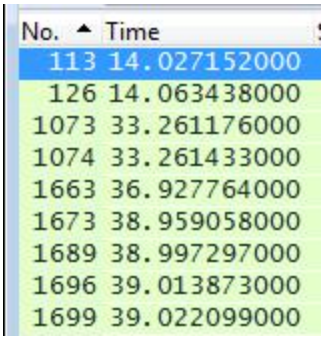
Wireshark stellt Ihnen für die Beschränkung der Ansicht verschiedene Funktionen zur Verfügung. Sie können neben dem Eingabefeld *Filter* unterhalb der Symbolleiste den Dialog *Filter Expression* verwenden.

Mit Hilfe der Darstellungsfilter können Sie die Darstellung auf folgende Inhalte beschränken:

- Protokoll
- Existenz eines Feldes
- Feldwert
- Vergleich von zwei oder mehreren Werten
- viele weitere Optionen

Besonders einfach ist die Beschränkung auf einen Protokolltyp. Geben Sie einfach den Protokolltyp in das *Filter*-Eingabefeld ein – und zwar in Kleinbuchstaben. Am besten probieren Sie es einfach einmal aus und geben Sie *tcp*, *ip* oder *http* in das Feld ein. Den Filter wenden Sie an, indem Sie die Return-Taste betätigen.

Was für den Protokolltyp gilt, gilt auch für die Feldnamen: Alle Angaben sind in Kleinbuchstaben vorzunehmen. Und vergessen Sie nicht, die Enter-Taste zu betätigen.



Die Nummerierung der Pakete bleibt bei der Filterung erhalten.

Wenn Sie die Ansicht der Pakete mit einem Filter Ihrer Wahl einschränken, bleibt die Paketnummerierung erhalten. Allerdings werden die Pakete ausgeblendet, die nicht das Filterkriterium passieren. Ich hatte es bereits oben einmal angedeutet: Bei der Darstellungsfilterung bleibt die Ausgangsaufzeichnung erhalten. Es erfolgt lediglich ein Ausblenden von Inhalten, nicht aber ein Bearbeiten der Inhalte.

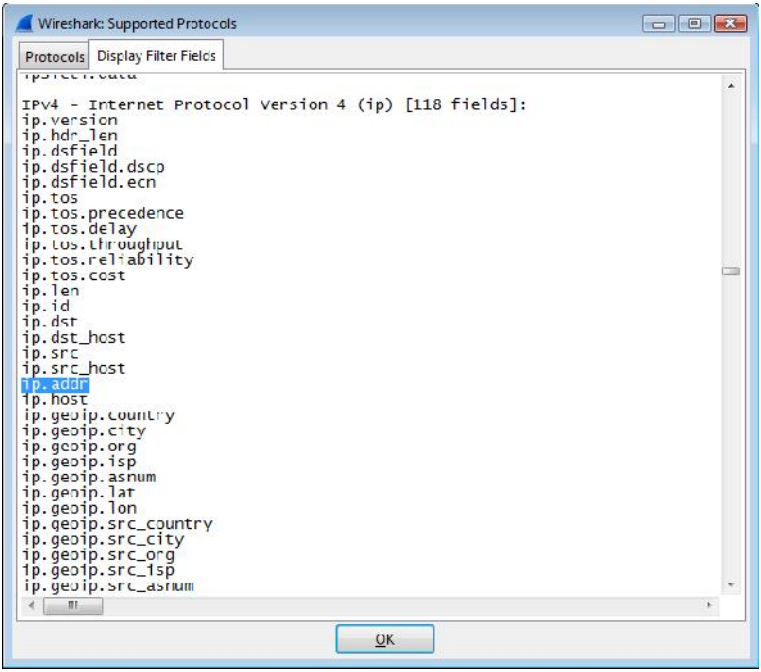
Prinzipiell kann die Filterung auf Grundlage jedes Protokolls erfolgen, das Wireshark unterstützt. Außerdem kann die Filterung mit jedem Feld erfolgen, das einen Dissektor der Baumansicht hinzufügt. Eine Einschränkung gibt es hierzu allerdings: Die Filterung mit der Feldbezeichnung ist nur dann möglich, wenn ein Dissektor hierfür eine Abkürzung angelegt hat. Wir kommen später nochmal auf diese Abkürzungen zu sprechen.

Für den Moment soll ein Beispiel genügen. Um die Darstellung auf die IP-Adresse *192.168.1.100* zu beschränken, würde ein entsprechender Filter wie folgt aussehen:

```
ip.addr==192.168.1.100
```

An diesem Beispiel erkennen Sie, dass Sie auch konkrete Werte in einer Filterkonfiguration verwenden können.

Sie heben eine Filterung auf, indem Sie rechts neben dem Eingabefeld auf die *Clear*-Schaltfläche tippen.



Wireshark 1.12.5 kennt über 115.000 Felder.

5.1 Aufbau von Darstellungsfiltern

So richtig interessant wird die Filterung erst dann, wenn Sie für die Filterung mehr oder minder komplexe Ausdrücke verwenden. Sie können dabei Vergleiche nutzen, logische Operatoren verwenden und auch fixe Werte vorgeben. Auch die Verwendung von Text und IP-Adressen ist möglich. Sie können jedes Feld, das in den Paketdetails auftaucht, für die Reduzierung der Ansicht verwenden.

Auf dem Screenshot zu Beginn dieses Kapitels finden Sie einen simplen Filter: *http*. Der schränkt die Aufzeichnung auf den HTTP-Traffic ein. Sie kennen mit *ip.addr* einen zweiten Filter. Nun liegt die Vermutung nahe, dass Sie auch alle weiteren Ihnen bekannten Protokolle für die Filterung verwenden können. Aber welche konkret? Und welche Felder können Sie verwenden?

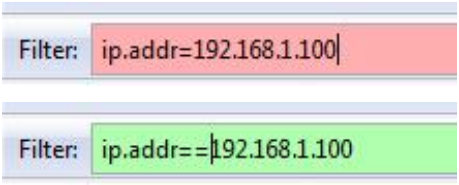
Diese Frage lässt sich schnell und exakt beantworten. Wireshark verrät Ihnen mit dem Menübefehl *Internals* > *Supported Protocols*, welche Protokolle und welche Felder für die Filterung herangezogen werden können. Der zugehörige Dialog umfasst zwei Registerkarten: *Protocols* und *Display Filter Fields*. Die diesem Buch zugrunde liegende Programmversion 1.12.x unterstützt 1378 Protokolle. Wenn Sie auf der Registerkarte *Display Filter Fields* nach ganz unten navigieren, finden Sie dort eine weit mehr beeindruckende Zahl: Wireshark unterstützt 115.683 Felder. Der Tabelle können Sie auch die zulässigen Werte entnehmen. Dazu müssen Sie ein wenig nach rechts navigieren, denn diese Information ist ein wenig versteckt.

All diese Protokolle und Felder kann und muss man nicht kennen. Vielmehr genügt es zu wissen, wo man diese Informationen findet. Im Admin-Alltag sind es in der Regel immer wieder die gleichen Services, deren Funktionstüchtigkeit geprüft werden sollten. Die haben Sie samt relevanten Feldern schnell drauf.

Fast noch wichtiger als die Kenntnis der Protokolle und Felder ist, dass Sie die Vergleichsoperatoren kennen. Einen haben wir oben kennengelernt: ==, das doppelte Gleichheitszeichen, das für *equal*, also *ist gleich* steht. Neben *Equal* unterstützt Wireshark weitere Operatoren:

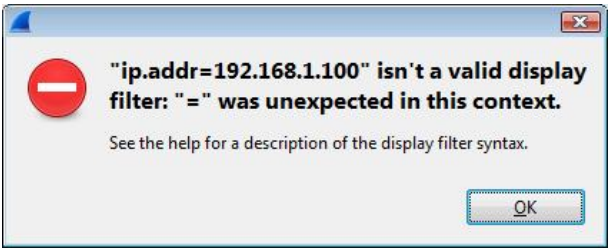
Vergleichsoperator	Notation	Beispiel
Not equal	!=	ip.src!=192.168.1.100
Greater than	>	frame.len > 10
Less than	<	frame.len < 128
Greater than or equal to	>=	frame.len ge 0x100
Less than or equal to	<=	frame.len <= 0x20

Damit ein Filter auch tatsächlich das gewünschte Ergebnis liefert, ist es essentiell, dass Sie die korrekte Syntax verwenden. Wireshark unterstützt Sie dabei mit einer einfachen, aber sehr effizienten Syntax-Prüfung. Wenn Sie in das Filter-Feld Ihre Eingabe vornehmen, wird der Hintergrund so lange rot eingefärbt, bis die Syntax korrekt ist. Versuchen Sie eine fehlerhafte Filterkonfiguration mit *Enter* auszuführen, gibt Wireshark eine entsprechende Fehlermeldung aus.



Die Syntaxprüfung der Filterkonfiguration.

Die Syntaxprüfung der Filtereingabe verhindert somit, dass Sie Ihre meist sehr umfangreichen Aufzeichnungen einer unsinnigen Analyse unterzogen werden.



Die fehlerhafte Filterkonfiguration kann nicht ausgeführt werden.

Bei der Verwendung von Zahlenwerten können Sie neben der dezimalen immer auch die hexadezimale Schreibweise verwenden.

Oben haben wir ein Beispiel für die exakte Verwendung einer IP-Adresse kennengelernt. Sie können die Darstellung auch auf ein gesamtes Subnetz beschränken. Hierzu ein Beispiel, das die Darstellung auf den gesamten Traffic des 178.16-Subnetzes beschränkt:

```
ip.addr==178.16.0.0/16
```

Wenn Sie die Aufzeichnung auf einen bestimmten String beschränken wollen, verwenden Sie hierfür beispielsweise folgende Konfiguration:

```
http.request.uri == "http://www.brain-media.de/"
```

Nun können Sie nun nicht nur derart einfache Filterkonfigurationen nutzen, sondern die Ausdrücke auch miteinander kombinieren. Konkret können Sie die logischen Operatoren *AND*, *OR*, *XOR* und *NOT* verwenden. Auch die Verwendung eines sogenannten Substring-Operators ist möglich. Die Teilstring-Funktion dient dazu, nur einen Teil der gespeicherten Daten zu erfassen. Der Teilstring wird dabei in eckigen Klammern eingefasst.

Schauen wir uns zunächst die vier logischen Operatoren an. Nachstehende Tabelle fasst diese samt Beispielen zusammen. Wichtig ist dabei, dass Sie anstelle der ausgeschriebenen Verknüpfung auch die C-ähnlichen Operatoren verwenden können:

Ausdruck	Notation	C-ähnlich	Beispiel
AND	and	&&	ip.src==10.0.0.5 and tcp.flags.fin
OR	or	||	ip.scr==10.0.0.5 or ip.src==192.1.1.1
XOR	xor	^^	tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29
NOT	not	!	not arp

Durch die Verwendung des sogenannnten Substring-Operators ergeben sich weitere interessante Möglichkeiten. Sie können damit einen Unterbereich definieren und somit die Filterung genauer spezifizieren. Ein solcher Teilstring wird mit eckigen Klammern angelegt, wobei der Wertebereich durch eine kommaseparierte Liste angegeben wird.

Das folgende Beispiel bestimmt durch das n:m-Format einen einzelnen Wertebereich, wobei der n-Wert, in diesem Fall die 0, den Anfangs-Offset-Wert und m, in diesem Beispiel die 5, die Länge des Bereichs spezifiziert:

```
eth.src[0:5] == 00:00:99
```

Sie können auch einen speziellen Bereich angeben. Hierfür verwenden Sie das n-m-Format:

```
eth.src[1-3] == 00:88
```

Wenn der Ausgangspunkt bei Null beginnt, so können Sie auch das :m-Format für die Filterung verwenden. Ein entsprechendes Beispiel:

```
eth.src[:5] == 00:00:88:00
```

In diesem Beispiel werden alle Daten von Anfang der Sequenz bis zum Wert 5 verwendet. Der Substring *:m* entspricht also *0:m*.

Entsprechend können Sie auch einen Ausgangspunkt bestimmen und alle Daten bis zum Ende der Sequenz analysieren. Ein Beispiel:

```
eth.src[5:] == 20:20
```

Mit dem n:-Format bestimmen Sie den Anfangspunkt der Sequenz.

Sie können mit Substrings auch mehrere Bereiche angeben. Diese trennen Sie dann durch Kommata. Ein Beispiel:

```
eth.src[0:3,1-2,:4,4:,2] ==
00:00:83:00:83:00:00:83:00:20:20:83
```

Vorsicht

Aus obiger Tabelle wissen Sie, dass Sie das Ausrufungszeichen ! als logischen Operator NOT verwenden können. Hierbei ist zu beachten, dass die Verwendung des Operators *!=* mit kombinierten Ausdrücken wie *eth.addr*, *ip.addr*, *tcp.port*, *udp.port* etc. oftmals nicht das gewünschte Ergebnis erzielt. Sie sollten daher auf diese Verwendung verzichten.

Bei der Filterkonfiguration sind weitere Besonderheiten zu beachten. Will man die Ansicht auf den Traffic von und zu einer IP-Adresse 192.168.1.100 beschränken, so verwendet man hierfür folgende Konfiguration:

```
ip.addr == 192.168.1.100
```

Wollte man die Ansicht nun auf die Pakete beschränken, die diese Adresse nicht enthalten, so wäre es logisch, wenn man diese mit dem logischen Operator *NOT* bestimmt. Der Filter würde demnach wie folgt aussehen:

```
ip.addr != 192.168.1.100
```

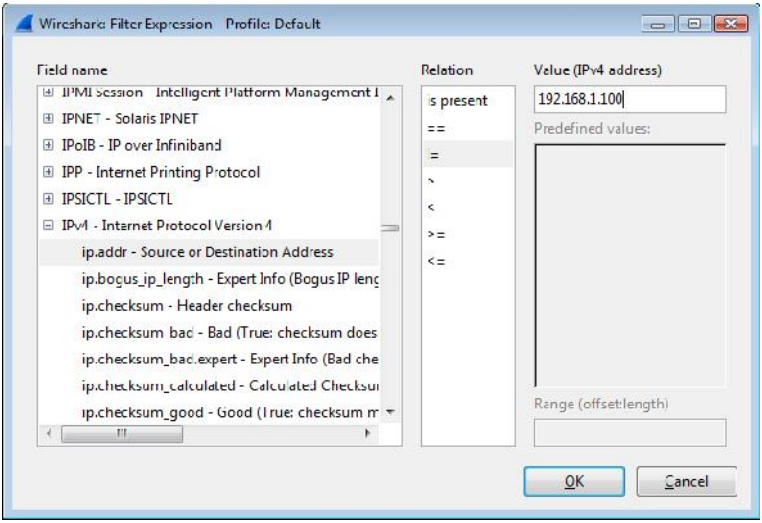
Leider ist dem nicht so, weil Wireshark den Ausdruck anders interpretiert. Wenn Sie dennoch alle Paket filtern wollen, die IP-Datagramme von oder zur IP-Adresse *192.168.1.100* senden, dann erzielen Sie das mit einer Klammerung:

```
!(ip.addr == 192.168.1.100)
```

Ähnlich vorsichtig sollten Sie bei vergleichbaren Konfigurationen sein. Es empfiehlt sich daher, bestimmte Ausdrücke mit Klammern zu fixieren. Hier ein weiteres Beispiel für einen komplexen Filter:

```
(!(ip.dst == 192.168.2.105)) || (ip.dst == 192.168.2.200)
```

Wir kommen in Kapitel 5.4 noch auf einige weitere Beispiele zu sprechen, die Ihnen zeigen, wie flexibel Sie bei der Filterung sind.



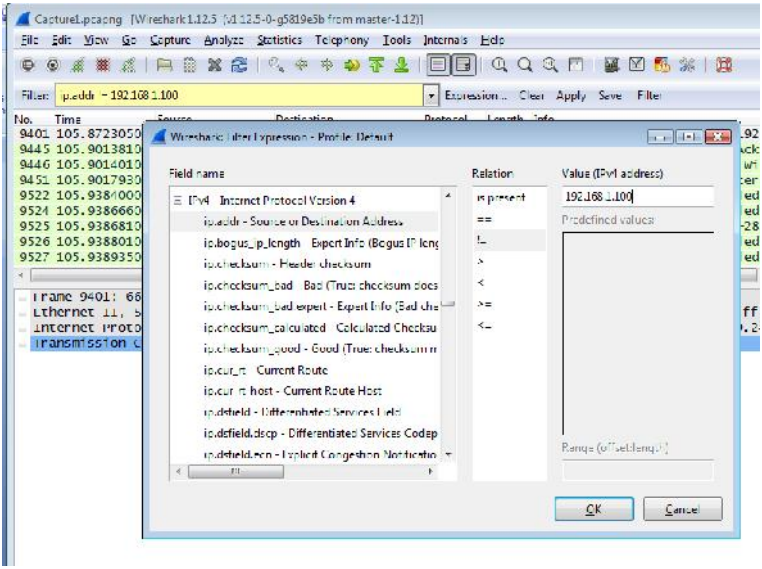
Filterung leicht gemacht: Mit dem Dialog *Filter Expression* bauen Sie mit wenigen Mausklicks einen Darstellungsfilter.

5.2 Dialog „Filter Expression“

Das Erstellen von Filtern ist nicht unbedingt einfach und aufgrund der vielen Protokolle und Felder auch recht fehleranfällig. Aber Wireshark stellt Ihnen ein weite-

res Werkzeug zur Verfügung, mit dem Sie die Darstellung auf spezifische Informationen konzentrieren können: den Dialog *Filter Expression*. Den Dialog öffnen Sie mit einem Klick auf die Schaltfläche *Expression* rechts neben dem Filterfeld.

Gerade für Einsteiger in das nicht immer einfach, sich in die Filtertechnik einzuarbeiten. Hier ist der Dialog *Filter Expression* eine große Hilfe, weil Sie damit die verschiedenen Elemente der Filterkonfiguration zusammenklicken. Er ist außerdem hervorragend geeignet, um die Filter kennen und einsetzen zu lernen.



Vorsicht: Mit dem *Filter Expression*-Dialog können Sie auch unsaubere Filter anlegen.

Die Verwendung des Filterdialogs ist prinzipiell sehr einfach. Unter *Field name* stehen die Protokolle und verfügbaren Felder bereit. Navigieren Sie zu dem gewünschten Feld und markieren Sie es. Als Nächstes bestimmten Sie über das Auswahlmenü *Relation* die Beziehung. Die Relation *is present* bedarf der Erläuterung: Hierbei handelt es sich um eine unäre, also einstellige Verknüpfung (im Unterschied zu binär). Sie ist wahr, wenn das gewählte Feld gelistet ist.

Bei allen anderen Relationen handelt es sich um binäre Relationen. Das bedeutet, dass Sie immer einen Wert benötigen, den Sie im Eingabefeld *Value* angeben. Wenn Sie mit Hilfe dieses Dialogs einen Filter anlegen, der entsprechend obigem

Beispiel den Traffic einer IP-Adresse ausblendet, so stellen Sie etwas Merkwürdiges fest: Wireshark erzeugt einen Filter mit folgendem Muster:

```
ip.addr != 192.168.1.100
```

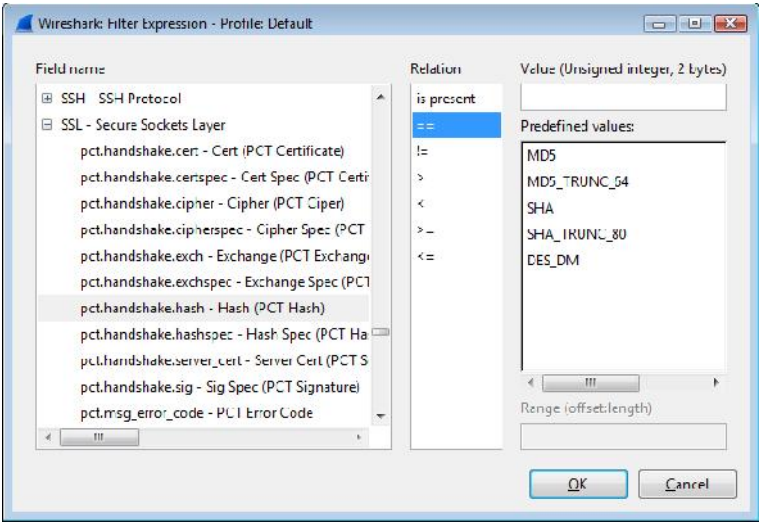
Der wird als gültig bewertet, aber in Filterfeld gelb hinterlegt. Ausführen können Sie den Befehl, auch wenn er nicht das gewünschte Ergebnis liefert.

Zurück zu den Funktionen des Dialogs *Filter Expression*. Im Bereich *Relation* können Sie neben *is present* acht weitere Operatoren angeben:

- == – Ist identisch
- != – Nicht identisch
- > – Größer als
- > – Kleiner als
- >= – Größer gleich
- <= – Kleiner gleich
- contains – enthält
- matches – entspricht

Im Eingabefeld *Value* geben Sie dann den gewünschten Wert an, der für die Operation herangezogen wird. Es muss sich dabei um einen Wert handeln, der von dem verwendeten Feld unterstützt wird. Sie können gegebenenfalls in der Übersicht der unterstützten Protokolle herausfinden, welche Werte zulässig sind.

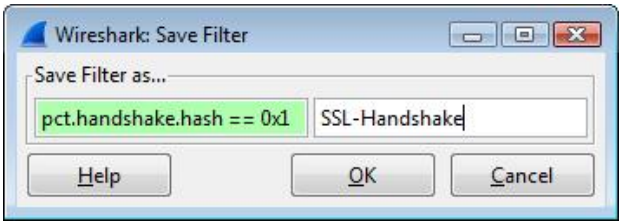
Bei der Wahl eines Feldtyps begegnen Sie immer wieder auch solchen, die vordefinierte Werte besitzen. So beispielsweise beim SSL-Protokoll. Wenn Sie eine Filterung auf Basis des Feldes *pct.handshake.hash* vornehmen wollen, stellt Ihnen das Feld *Predefined values* fünf verschiedene Werte zur Auswahl.



Für das SSL-Feld *pct.handshake.hash* stehen verschiedene vordefinierte Werte zur Verfügung.

Schließlich können Sie mit *Range* den Wertebereich bestimmen. Der besteht üblicherweise aus dem Wertepaar *Offset:Länge*.

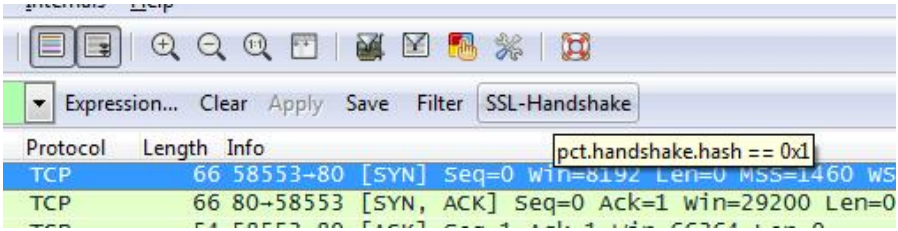
Mit einem Klick auf *OK* wird die Filterkonfiguration in das Eingabefeld *Filter* geschrieben. Dort können Sie die Konfiguration erneut prüfen. Um den Filter anzuwenden, klicken Sie auf *Apply*.



Das Speichern eines Filters.

Wenn Sie einen Filter häufiger verwenden wollen, können Sie ihn einfach sichern. Dazu klicken Sie rechts neben der Filtereingabe auf die Schaltfläche *Save*. Im Dialog *Save Filter* wird die Filterkonfiguration angezeigt und Sie sollten dem Fil-

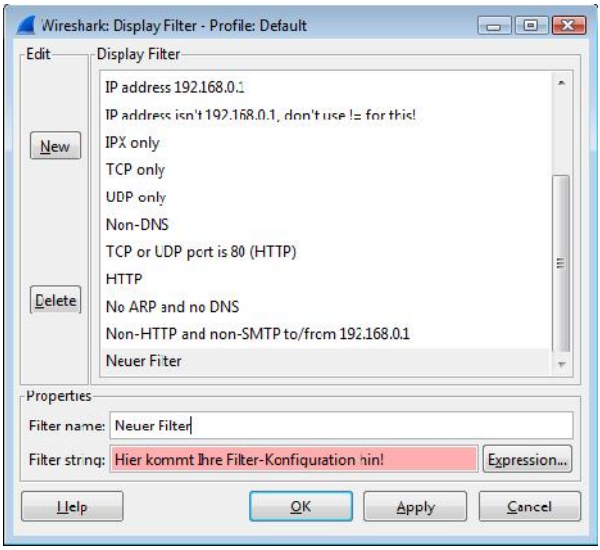
ter eine aussagekräftige Bezeichnung zuweisen. Mit einem Klick auf *OK* landet der neue Filter in der Filterverwaltung.



Die gespeicherte Filterkonfiguration steht nun über die Filterleiste zur Verfügung.

Über die Programmeinstellungen können Sie nicht mehr benötigte Filterkonfigurationen auch wieder aus der Filter-Funktionsleiste entfernen.

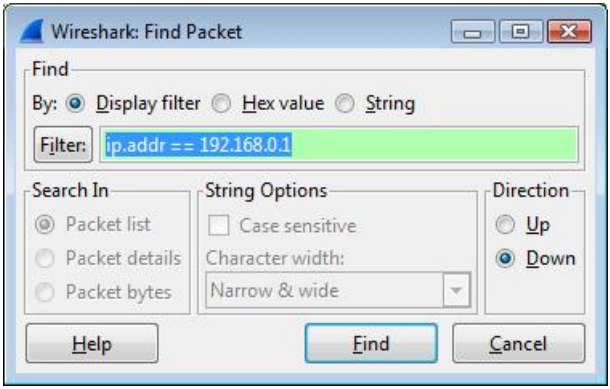
Sie können außerdem über den Dialog *Display Filter*, den Sie am einfachsten mit einem Klick auf das zugehörigen Icon in der Symbolleiste öffnen, weitere Filterkonfigurationen anlegen, bestehende bearbeiten, löschen etc.



Die Filterverwaltung von Wireshark.

5.3 Pakete suchen, finden und markieren

Während Sie mit Hilfe der Ansichtsfilter die Darstellung gezielt einschränken können, erlaubt Ihnen Wireshark auch die Suche nach Paketen, die bestimmte Kriterien erfüllen. Den Suchdialog öffnen Sie mit dem Menübefehl *Edit > Find Packet* oder mit der Tastenkombination *Strg + F*.



Die Suche nach bestimmten Paketen.

Für die Suche können Sie die Darstellungsfilter, eine hexadezimalen Wert oder eine Zeichenfolge verwenden. Abhängig von dieser Wahl können Sie weitere Suchoptionen bestimmen, beispielsweise, ob in den Paketbeschreibungen gesucht oder zwischen Groß- und Kleinschreibung bei der Suche unterschieden wird.

Mit dem Bereich *Find* bestimmen Sie zunächst, nach welchen Inhalten Sie suchen wollen. Mit *Display Filter* finden Sie die Pakete, die dem Filter entsprechen, den Sie in der Eingabefeld eingeben bzw. den Sie mit einem Klick auf die Schaltfläche *Filter* auswählen.

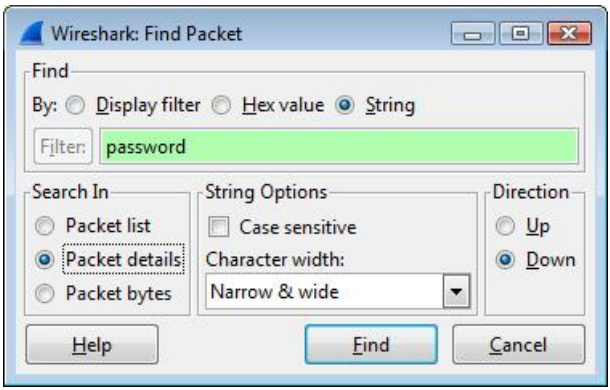
Wenn Sie nach einer bestimmten Byte-Sequenz suchen, aktivieren Sie das Kontrollkästchen *Hex value* und geben Sie die Zeichenfolge ein, die beispielsweise wie folgt lautet:

```
70 61 73 73 77 6f 72 64
```

Am flexibelsten sind Sie bei der Suche nach einer bestimmten Zeichenfolge. Hierfür wählen Sie das Kontrollkästchen *String*. Automatisch werden die beiden Berei-

che *Search In* und *String Options* aktiviert. Mit *Search In* bestimmen Sie, wo die Suche erfolgen soll:

- Packet list – Durchsucht die Paketliste.
- Packet details – Nimmt die Paketdetails unter die Lupe. Diese Option ist beispielsweise für die Suche nach Begriffen wie *Password*, *Login* etc. relevant.
- Packet bytes – Schließlich können Sie die Paket-Bytes durchsuchen.



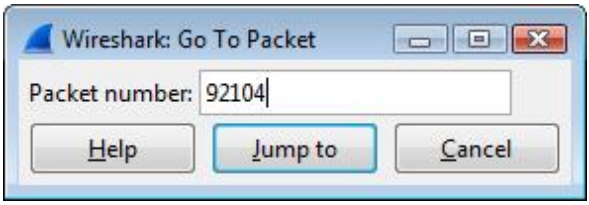
Die Suche nach einer Zeichenfolge in den Paketdetails.

Mit dem *String Options* bestimmen Sie, ob Groß- und Kleinschreibung sowie die Zeichenkodierung verwendet werden sollen. Die Suche erfolgt standardmäßig von oben nach unten. Mit *Direction* entscheiden Sie, in welche Richtung Sie die Suche durchführen wollen. Klicken Sie auf die Schaltfläche *Find*, um die Suche zu starten. Wird die Suche fündig, wird das entsprechende Paket in der Paketliste samt Paketdetails und zugehörige Byte-Ansicht markiert.

Um zur nächsten Fundstelle zu springen, verwenden Sie die Tastenkombinationen:

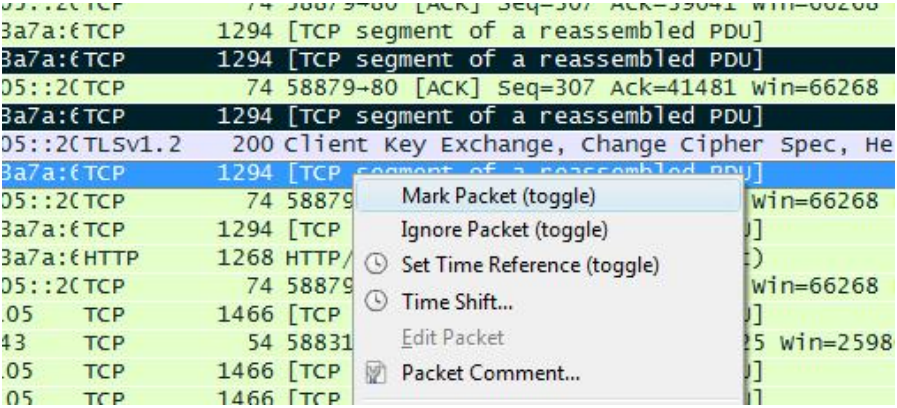
- *Strg* + *N* springt zur nächsten Fundstelle.
- *Strg* + *B* springt zur vorherigen Fundstelle.

Beide Kommandos können auch über das *Edit*-Menü von Wireshark ausgeführt werden.



Das direkte Sprung zu einem Paket.

Wenn Sie die exakte Paketnummer eines Pakets kennen, so können Sie dieses auch direkt anspringen und dann einer Analyse unterziehen. Hierfür verwenden Sie den Menübefehl *Go > Go To Packet*. Alternativ verwenden Sie die Tastenkombination *Strg + G*. Geben Sie in das Eingabefeld die Nummer ein und klicken Sie auf *Jump to*.



Einige Pakete wurden markiert.

Wenn Sie sich an die Analyse einer Aufzeichnung machen, so begegnen Sie immer wieder Paketen, die Sie sich später anschauen wollen. Diese können Sie einfach markieren. Dazu markieren Sie das Paket mit einem Rechtsklick und führen den Befehl *Mark Packet* aus. Die markierten Pakete werden dann schwarz hinterlegt, und zwar unabhängig von einer vorherigen Farbzuweisung.

Über das *Edit*-Menü stehen Ihnen weitere Markierungsmöglichkeiten zur Verfügung. Sie können mit *Mark All Displayed Packets* auch alle dargestellten Pakete

markieren. Eine etwaige Markierung können Sie mit dem Menübefehl *View > Unmark All Displayed Packets* auch wieder auflösen.

Die Markierung können Sie insbesondere für die Ausgabe, also beispielsweise den Export oder den Druck verwenden, damit nur die Daten der gekennzeichneten Objekte bei dem Vorgang berücksichtigt werden. Im Druck- bzw. Exportdialog können Sie dann mit *Packet Range* die Option *Marked packets only* verwenden.

Beachten Sie, dass die Markierung bei einer Speicherung nicht erhalten bleibt.

5.4 Beispiele für die Filterung

Zum Abschluss dieses Kapitels schauen wir uns noch einige Beispiele an, die Ihnen anhand typischer Alltagsanforderungen zeigen, wie Sie mit den Darstellungsfiltern arbeiten können.

Wenn Sie den Traffic beispielsweise auf SMTP- und ICMP-Traffic beschränken wollen, und Sie der Standardport 25 des SMTP-Dienstes interessiert, so verwenden Sie hierfür folgenden Filter:

```
tcp.port eq 25 or icmp
```

Oftmals ist man auch bei internen Netzwerken auf der Suche nach Anomalien und Flaschenhälsen. Wenn Sie den Traffic in Ihrem LAN (192.168.x.x) zwischen den Workstations und Servern interessiert, nicht aber der ein- und ausgehende Internet-Traffic, so begrenzen Sie die Ansicht damit wie folgt:

```
ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16
```

Ist ein TCP-Puffer voll und informiert die Quelle das Ziel darüber, keine weiteren Daten mehr zu senden, so finden Sie den entsprechenden Traffic wie folgt:

```
tcp.window_size == 0 && tcp.flags.reset != 1
```

Bei einem Windows-Netzwerk können Sie das Hintergrundrauschen einfach ausblenden und die Ansicht rein auf den Austausch von Windows-Clients und dem Domain Controller begrenzen:

```
smb || nbns || dcerpc || nbss || dns
```

Um die Ansicht auf Pakete mit HTTP-Requests zu beschränken, in deren URI die letzten Zeichen *gl=de* lautet, verwenden Sie folgenden Filter:

```
http.request.uri matches "gl=de$"
```

Das Dollar-Zeichen zeigt das Ende der Zeichenfolge an.

Wenn Sie einen Filter auf Grundlage eines Protokolls wie beispielsweise SIP durchführen wollen und alle unerwünschten IP-Adressen ausblenden wollen, erzielen Sie das mit folgendem Filter:

```
ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip
```

Verschiedene Filterfelder entsprechen anderen Prorokollfeldern. Die sollten Sie kennen, damit Sie sich nicht wundern, wenn unterschiedliche Filter identische Ergebnisse erzielen. So entspricht *ip.addr* der IP-Quelle und der Zieladresse im IP-Header. Das Gleiche gilt für *tcp.port*, *udp.port* und *eth.addr*. Ein konkretes Beispiel:

```
ip.addr == 192.168.1.100
```

entspricht

```
ip.src == 192.168.1.100or ip.dst == 192.168.1.100
```

Das mag gelegentlich ein wenig irritieren, aber Sie sollten diesen Umstand kennen. Wenn Sie den Traffic von *192.168.1.100* aus einer Aufzeichnung herausfiltern wollen, so verwenden Sie hierfür folgenden Filter:

```
ip.addr != 192.168.1.100
```

Das wiederum ist gleichbedeutend mit folgendem Filter:

```
ip.src != 192.168.1.100 or ip.dst != 192.168.1.100
```

Leider interpretiert Wireshark diese Konfiguration wieder nicht korrekt. Sie sollten daher die Negierung von der Adressenangabe platzieren:

```
! ( ip.addr == 192.168.1.100 )
```

Oder entsprechend:

```
! (ip.src == 192.168.1.100 or ip.dst == 192.168.1.100)
```

Wenn Sie sich lediglich für den SNMP-, DNS- und ICPM-Traffic interessieren, verwenden Sie folgenden Filter:

```
snmp || dns || icmp
```

```
snmp or dns or icmp
```

Um alle Pakete anzuzeigen, die den TCP-Port 25 als Quelle oder Ziel besitzen, verwenden Sie diesen simplen Filter:

```
tcp.port == 25
```

Sie können auch alle Ping-Anfragen zu bzw. von einer bestimmten IP-Adresse anzeigen:

```
ip.addr == 192.168.1.100 && icmp
```

```
ip.addr == 192.168.1.100 and icmp
```

Sie können die Ausgabe auch einfach auf einen Text bzw. eine Zeichenfolge beschränken:

```
tcp matches "Zeichenfolge"
```

```
tcp contains "Zeichenfolge"
```

Um die Konversation zwischen zwei IP-Adressen auszugeben, verwenden Sie folgenden Filter:

```
ip.addr==192.168.1.100 && ip.addr==192.168.1.101
```

Um den Traffic auf die TCP-Pakete zu beschränken, die den Port 8080 als Ziel oder Quelle besitzen, verwenden Sie folgende Filterkonfiguration:

```
tcp.port==4000
```

Der folgende Filter gibt alle TCP-Resets aus:

```
tcp.flags.reset==1
```

Um alle HTTP GET-Requests darzustellen, verwenden Sie diesen Filter:

```
http.request
```

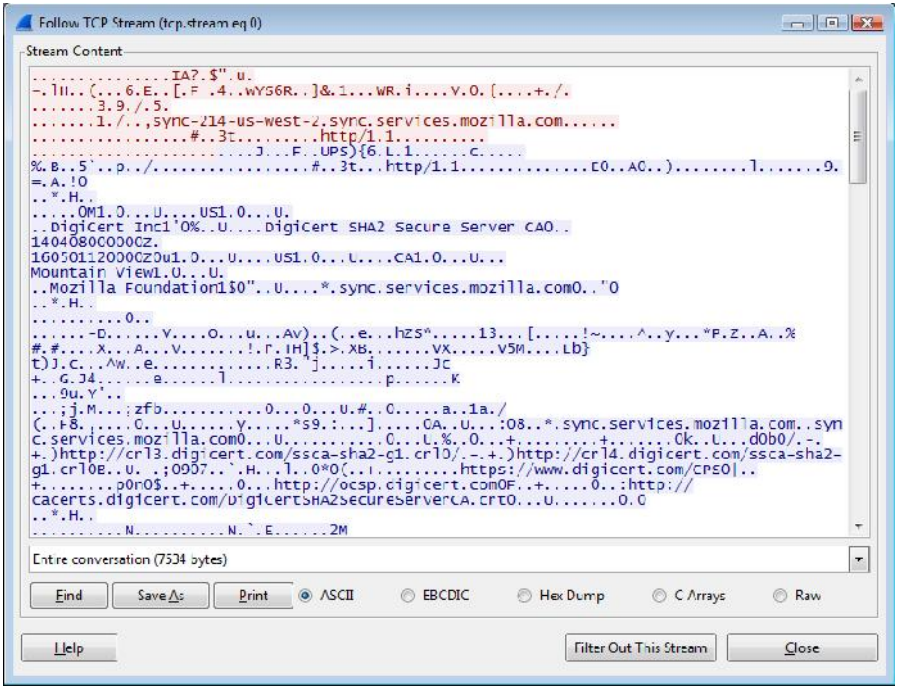
Ein letztes Beispiel zeigt, wie Sie alle Pakete anzeigen, die doppelt übertragen wurden:

```
tcp.analysis.retransmission
```

Im Wireshark-Wiki finden Sie weitere interessante Beispiele, die Sie an Ihre Anforderungen anpassen können.

6 Wireshark für Fortgeschrittene

Im bisherigen Verlauf dieses Buchs haben Sie die Grundfunktionen von Wireshark kennengelernt. Sie wissen, welche Bedienelemente der Sniffer besitzt, wie Sie die die unterschiedlichen Schnittstellen für eine Aufzeichnung verwenden, die Aufzeichnungen speichern und auswerten. Doch Wireshark hat noch eine Fülle weiterer Funktionen zu bieten, beispielweise die Stream-Funktionen, statistischen Auswertungen, die Experteninfos, Diagramme und weitere Auswertungen. In diesem Kapitel schauen wir uns die Funktionen an, die für fortgeschrittene Anwender interessant sind.



Das Folgen eines TCP-Streams.

6.1 TCP-Stream folgen

Wenn Sie den Traffic von TCP-basierten Protokollen analysieren, so ist es häufig hilfreich, wenn man die Daten des TCP-Stream auf Anwendungsebene begutachten kann. Das ist beispielsweise dann sinnvoll, wenn Sie die Passwörter von Telnet- oder Web-Sessions prüfen wollen. Genau hierfür eignet sich die Funktion *Follow TCP Stream*.

Der Aufruf der Funktion ist einfach: Markieren Sie zunächst ein Paket, das Sie verfolgen wollen und führen Sie dann aus dem Kontextmenü der rechten Maustaste den Befehl *Follow TCP Stream* aus. Dieser Befehl ist auch über das *Analyze*-Menü verfügbar.

Die Verfolgungsfunktion zeigt in einem neuen Dialog den Ablauf der Kommunikation zwischen zwei Endpunkten an. Der Stream-Content wird in der gleichen Abfolge im Dialog *Follow TCP Stream* dargestellt, wie er über das Netzwerk übermittelt wurde. Der Traffic von A nach B wird dabei rot und der von B zurück nach A wird blau eingefärbt. So erkennen Sie auf einen Blick, welche Daten von welchem Knoten stammen. Wie wir in Kapitel 7 noch sehen werden, können Sie die Farben auch ändern.

All die Zeichen, die der Dialog nicht korrekt ausgeben kann, werden durch Punkte ersetzt. Wenn Sie eine Live-Aufzeichnung durchführen, sollten Sie beachten, dass dabei keine Aktualisierung der Informationen im Stream-Dialog erfolgt. Sollte eine Aktualisierung gewünscht oder erforderlich sein, müssen Sie den Dialog schließen und erneut dem TCP-Datenstrom folgen.

Unterhalb des Darstellungsbereichs finden Sie ein Auswahlmenü, mit dem Sie die Darstellung weiter einschränken können. Standardmäßig wird mit der Option *Entire conversation* die gesamte Konversation darstellt. Sie haben aber auch die Möglichkeit, diese auf die Daten von A nach B bzw. von B nach A zu beschränken. Das Auswahlmenü zeigt Ihnen dabei die IP-Adressen und Ports der Dienste an.

Da auch die Verfolgung einer Konversation auf TCP-Basis sehr umfangreich sein kann, und damit das Auffinden bestimmter Inhalte nicht einfach ist, stellt Ihnen der Dialog *Follow TCP Stream* mit einem Klick auf *Find* eine simple Suche zur Verfügung. Sie bietet leider keinerlei Komfort.

Sie können den Ablauf auch mit einem Klick auf *Save* sichern und mit *Print* auf einem angeschlossenen Drucker ausgeben.

Mit einem Klick auf die Schaltfläche *Filter out this stream* wenden Sie einen Darstellungsfilter an, der dem gewählten TCP-Datenstrom von der aktuellen Darstellung ausblendet. Klicken Sie auf *Close*, um den Dialog zu schließen.

Der *Follow TCP Stream*-Dialog erlaubt außerdem die Darstellung der Daten in verschiedenen Formaten:

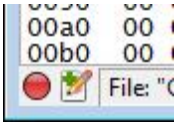
- **ASCII**: Bei diesem Format werden die Daten im ASCII-Format angezeigt. Die Verwendung eignet sich insbesondere bei ASCII-basierten Protokollen wie HTTP.
- **EBCDIC**: Das ist das bevorzugte Format für Freaks.
- **HEX Dump**: In der hexadezimalen Darstellung bekommen Sie alle Daten zu sehen. Es eignet sich am besten für binäre Protokolle und Daten.
- **C Arrays**: Dieses Format ist dann für Sie interessant, wenn Sie den Datenstrom in ein eigenes C-Programm importieren wollen.
- **Raw**: Hierbei handelt es sich um die Rohdaten. Die sollten Sie verwenden, wenn Sie die Daten in Drittprogrammen weiter verarbeiten wollen.

Wenn Sie noch nicht so recht wissen, was Sie mit den extrahierten Informationen anstellen wollen, können Sie sich einen Überblick über die verschiedenen Formate und deren Darstellung verschaffen und dann entscheiden, welches das optimale Format ist.

Der wichtigste Anwendungsbereich der Funktion *Follow TCP Stream*: Sie können damit den Datenverkehr von typischen HTTP-, FTP- und Telnet-Sessions rekonstruieren.

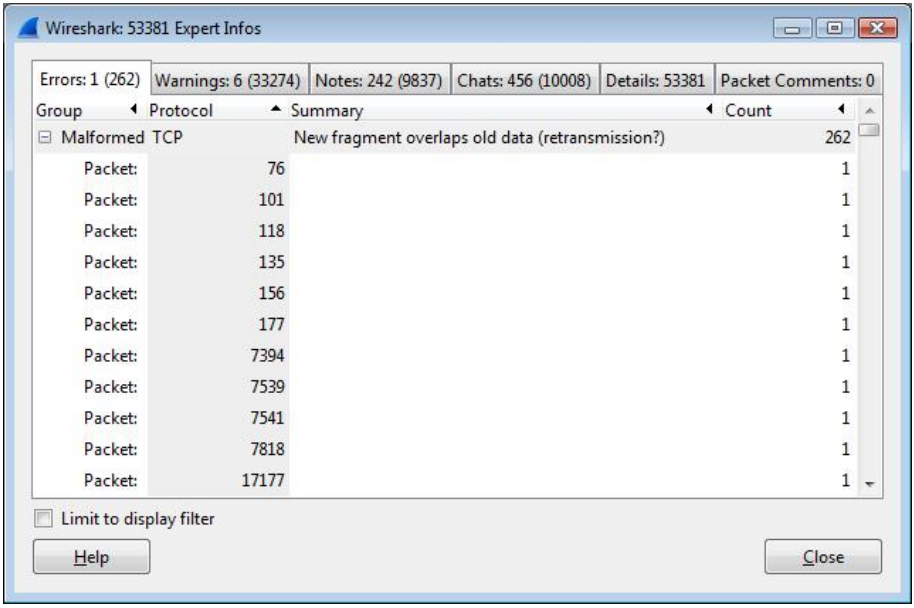
6.2 Experteninfos

Wireshark ist nicht nur ein unglaublich mächtiges und flexibles Werkzeug, sondern kann Sie auch auf Anomalien und Ungereimtheiten in Ihren Aufzeichnungen hinweisen. Aus Kapitel 1 wissen Sie bereits, wo Sie entsprechende Hinweise finden: In der linken unteren Ecke der Statusleiste werden Ihnen gegebenenfalls Warnungen angezeigt.



Kein gutes Zeichen: Der rote Punkt weißt auf Anomalien hin.

Der Hintergedanke der sogenannten Experteninfos ist einfach: Wireshark soll Ihnen einen besseren Blick auf Ungewöhnliches oder Auffälliges in Ihrem Netzwerk bzw. Ihren Aufzeichnungen bieten. Die Funktion ist so ausgelegt, dass sie sowohl Neulingen als auch Experten das Auffinden von Netzwerkproblemen vereinfacht. Den Dialog *Expert Infos* öffnen Sie mit einem Doppelklick auf das Kreissymbol.



Die Experteninfos fassen Auffälligkeiten zusammen.

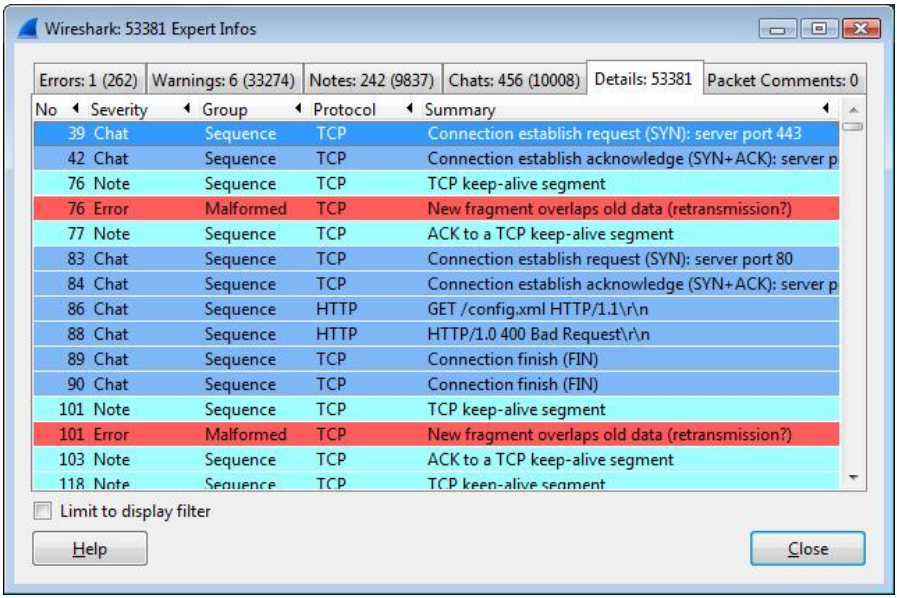
Bevor Sie allerdings zu viel von dieser Funktion erwarten, sollten Sie wissen, dass es sich hierbei lediglich um Hinweise handelt, denen Sie nachgehen sollten. Ein Eintrag in diesem Dialog bedeutet umgekehrt nicht zwangsläufig, dass es nicht noch weitere Anomalien geben kann. Der Dialog *Expert Infos* ist ein Element bei der Fehlersuche – nicht mehr, aber auch nicht weniger.

Prinzipiell gilt: Die Anzahl der Hinweise in diesem Dialog ist vom Protokoll abhängig. Insbesondere bei TCP/IP müssen Sie mit den meisten Fehlern rechnen, andere Protokolle gelten als deutlich weniger problematisch.

Der Dialog *Expert Infos* präsentiert Ihnen sechs Registerkarten: *Errors*, *Warnings*, *Notes*, *Chats*, *Details* und *Comments*. Zu jedem Register werden die Anzahl der Einträge in Klammern angezeigt. Den besten Überblick bietet Ihnen die Register-

karte *Details*, denn dort sind die wichtigsten Informationen in Tabellenform zusammengefasst. Außerdem erleichtern farbige Markierungen das Lesen und Verstehen. Eine Experteninfo auf dieser Registerkarte umfasst in der Regel mehrere Detailinformationen. Hier einige Beispiele:

Paketnummer (No)	**Schweregrad** (Severity)	**Gruppe** (Group)	**Protokoll** (Protocol)	**Details** (Summary)
1	Note	Sequence	TCP	Duplicate ACK (#1)
2	Chat	Sequence	TCP	Connection reset (RST)
8	Note	Sequence	TCP	Keep-Alive
9	Warn	Sequence	TCP	Fast retransmission (suspected)



Die Übersicht finden Sie auf der Registerkarte *Details*.

Neben der Paketnummer, die das auffällige Verhalten zeigt, ordnet der Sniffer den Auffälligkeiten einen Schweregrad zu, zu finden in der Spalte *Severity*. Der Grad

wird durch die Farbe des Statusleistensymbols gekennzeichnet. Den Bezeichnungen begegnen Sie im Expertendialog:

- **Chat**: Klassifiziert Informationen über einen „normalen“ Workflow. Farbe: grau.
- **Note**: Weißt auf erwähnenswerte Dinge wie einen üblichen Fehlercode hin, beispielsweise einen HTTP 404-Fehler. Farbe: Cyan.
- **Warn**: Diese Warnung deutet auf ungewöhnliche Fehlermeldungen hin, beispielswiese ein unerwartetes Verbindungsproblem. Farbe: Gelb.
- **Error**: Weist auf ein erhebliches Problem hin, beispielsweise missgebildete Pakete. Farbe: Rot.

In der Spalte *Group* begegnen Sie folgenden Informationen, wobei es sich lediglich um eine Klassifizierung handelt:

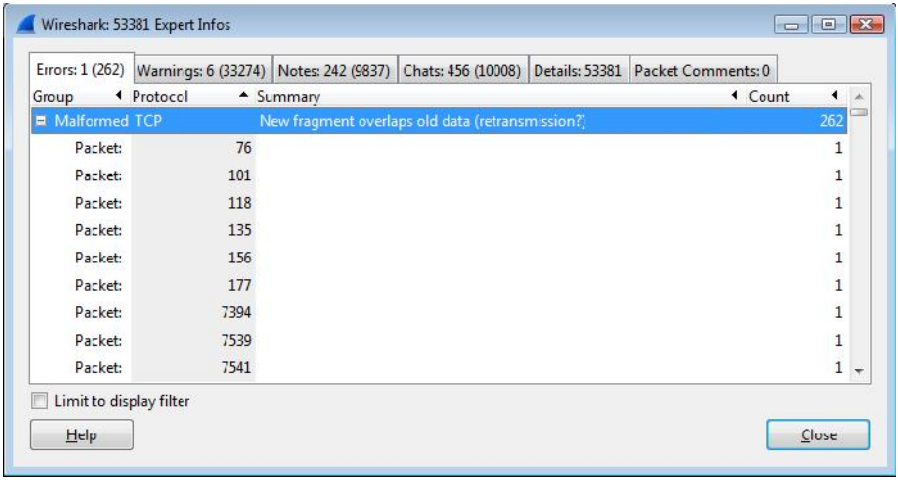
- **Checksum**: Die Checksumme war ungültig.
- **Sequence**: Es handelt sich um eine verdächtige Protokollsequenz. Beispiele hierfür: Die Sequenz wurde nicht kontinuierlich übermittelt oder es wurde ein Rücksendung ermittelt.
- **Response Code**: Es ist ein Problem mit dem Antwort-Code der Anwendung aufgetreten, beispielsweise eine HTTP 404-Fehlermeldung.
- **Request Code**: Zeigt einen Request einer Anwendung an.
- **Undecoded**: Die Daten konnten nicht dekodiert werden.
- **Reassemble**: Es ist ein Problem beim Reassembling aufgetreten.
- **Protocol**: Eine Verletzung der Protokollspezifikation wurde entdeckt. Das können beispielsweise ungültige Feldnamen oder unzulässige Längen sein.
- **Malformed**: Wireshark hat ein ungültiges Paket identifiziert. Die Dissektion des Pakets wird abgebrochen.
- **Debug**: In Preview-Versionen kann auch der Debugging-Modus auftreten.

Für die Zukunft kann mit weiteren Gruppenwerten gerechnet werden.

Die Funktionalität der Spalte *Protocol* ist schnell erklärt: Hier wird das Protokoll aufgeführt. Der Spalte *Summary* können Sie einige Hintergrundinformationen zu dem jeweiligen Eintrag entnehmen.

Der einfachste und vermutlich schnellste Weg, die für Sie relevanten Informationen herauszupicken, dürfte das Öffnen der Registerkarte mit der gewünschten Schweregradbewertung sein. Während die Registerkarte *Details* Ihnen einen ersten Überblick vermittelt, sollten Sie sich als Nächstes den Registerkarten *Errors* und *Warnings* zuwenden.

In der Regel treten eine Fülle von identischen Experteninformationen mehrfach auf – lediglich mit unterschiedlichen Paketnummern. Diese werden automatisch von Wireshark in einem Knoten zusammengefasst. Mit einem Klick auf den Knoten können Sie weitere Details wie die betreffenden Datenpakete abrufen.

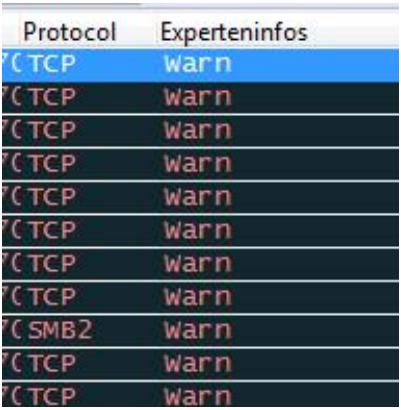


Die Details einer Fehlermeldung.

Die Darstellung der Registerkarte *Details* unterscheidet sich von den Darstellungen der übrigen Registerkarten. Es handelt sich hierbei um eine eher protokollähnliche Liste, die der Paketliste ähnelt.

Durch die Verwendung der oben beschriebenen farbigen Markierungen ist es aber einfach, sich einen Überblick über die Hinweise zu verschaffen. In der Details-Ansicht können Sie außerdem über die Kopfzeile die Sortierung ändern und beispielweise zunächst alle kritischen Fehler einblenden.

Sie können die Experteninfo, genauer den Schwergrad einer Experteninfo auch in der Paketliste einblenden. Dazu öffnen Sie die Spalteneinstellungen und fügen die Experteninfos hinzu. Mehr dazu erfahren Sie in Kapitel 7.

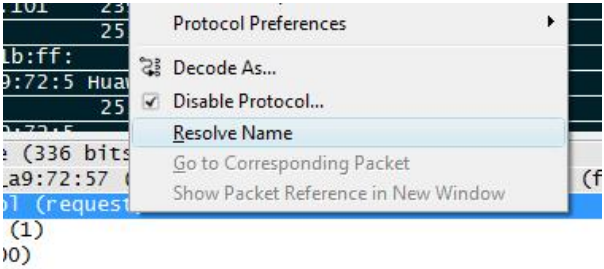


Eine sinnvolle Ergänzung: Die Experteninfos wurden der Paketliste hinzugefügt.

6.3 Namensauflösung

Wireshark verfügt über eine Funktion zur Namensauflösung, mit der Sie die numerischen Werte der Hosts in lesbare Zeichenfolgen konvertieren können. Wireshark übernimmt die Auflösung selbst nicht, sondern greift auf Funktionen wie *gethostname()* oder einen in der Wireshark-Konfiguration hinterlegten Dienst zurück.

Die Auflösung ist einfach auszuführen: Sie markieren ein Paket, klicken mit der rechten Maustaste in die Paketdetails und führen dann aus dem Kontextmenü den Befehl *Resolve Name* aus.



Der Aufruf der Namesauflösung. Meistens passiert allerdings nach der Ausführung einfach nichts.

Prinzipiell ist die Namensauflösung eine praktische Sache, doch in der Praxis müssen Sie mit so manchen Problemen und Schwächen leben. Oft scheitert die Auflösung. Ein weiteres Manko: Gelingt die Auflösung, wird die Auflösung nicht in der Aufzeichnungsdatei gespeichert. Die DNS-Abfragen führen außerdem zu zusätzlichen Einträgen in Ihren Aufzeichnungen.

6.4 Zahlen über Zahlen

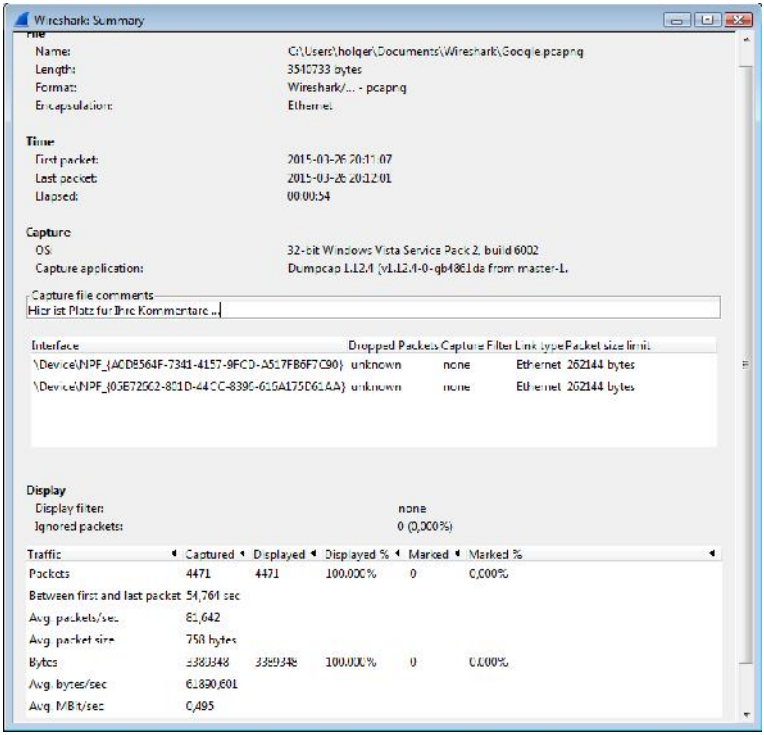
Wireshark stellt Ihnen verschiedene statistische Informationen zur Verfügung, die allesamt über das Menü *Statistics* verfügbar sind. Diese Statistiken decken eine große Bandbreite ab: Von allgemeinen Informationen über die geladene Capture-Datei über protokollspezifische Statistiken bis hin zu spezifischen Daten wie die Anzahl der aufgezeichneten HTTP-Requests und -Responses.

Zu den allgemeinen Statistiken gehören folgende Funktionen:

- Zusammenfassung zu einer Capture-Datei
- Protokollhierarchie der aufgezeichneten Pakete
- Konversation zwischen zwei IP-Adressen
- Endpunkte und Traffic von bzw. zu einer IP-Adresse
- Visualisierung der Paketanzahl in einer bestimmten Zeitspanne

Zu den protokollspezifischen Statistiken gehören beispielsweise die Antwortzeiten der Dienste bei Requests und Responses bestimmter Protokolle.

Um etwas mit diesen Statistiken anfangen zu können, sollte man zumindest Grundkenntnisse der wichtigsten Protokolle besitzen. Andernfalls ist es recht schwer, diese Informationen zu interpretieren.



Die statistische Zusammenfassung.

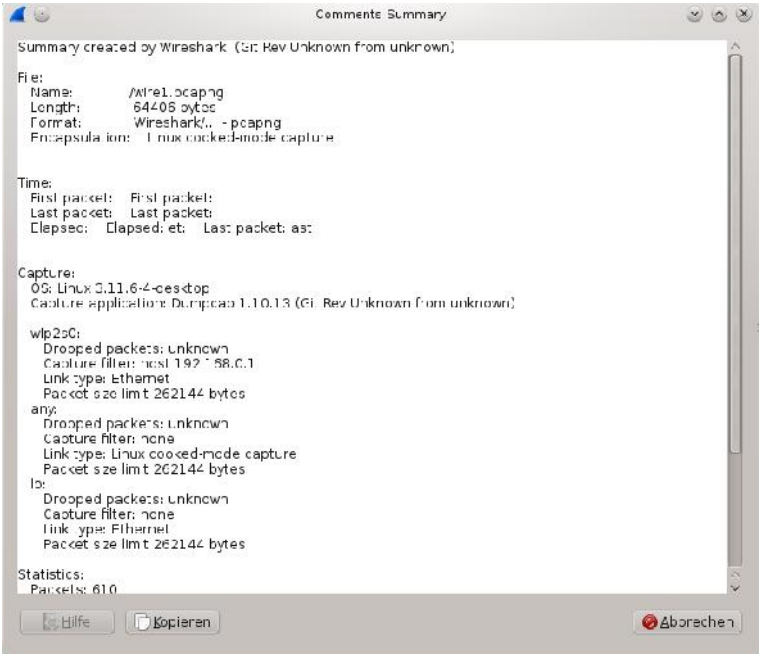
Mit dem Menübefehl *Statistics* > *Summary* öffnen Sie die Zusammenfassung zur aktuellen Capture-Datei. Dem zugehörigen Dialog können Sie verschiedene allgemeine Informationen wie den Dateinamen, die Größe, das Format und die Datenkapselung entnehmen.

Der Bereich *Time* zeigt Ihnen drei zeitspezifische Daten: den Anfangs- und Endzeitpunkt der Aufzeichnung sowie die Dauer.

Unter *Capture* werden das verwendete Betriebssystem, die Capture-Anwendung (in der Regel Dumpcap) und die Schnittstelle aufgeführt, die für die Aufzeichnung verwendet wurde. Sie können außerdem einen Kommentar zur Capture-Datei anle-

gen. Der Bereich *Display* zeigt Ihnen die verwendeten Darstellungsfilter und Anzahl der ignorierten Pakete an.

Den Abschluss bildet der Bereich *Traffic* mit verschiedenen Traffic-spezifischen Informationen wie der Anzahl der aufgezeichneten Pakete und die durchschnittliche Paketgröße.



Die Kommentarzusammenfassung.

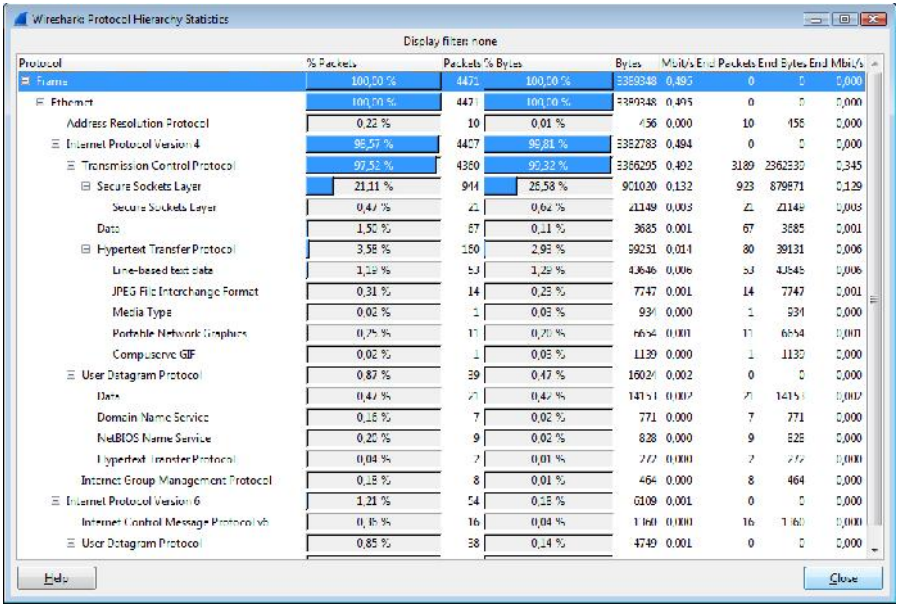
Die Zusammenfassung, die Wireshark für Sie bereitstellt, können Sie mit dem Menübefehl *Statistics* > *Comments Summary* auch in einem Editierfenster öffnen, bearbeiten oder kopieren und die Daten dann an anderer Stelle weiterverarbeiten.

6.5 Protokollhierarchie

Wireshark eignet sich nicht nur zur Analyse des Netzwerkverkehrs, sondern auch zum Aufspüren von verdächtigen Protokollen und Anwendungen. Hierbei leistet Ihnen die sogenannte Protokollhierarchie wertvolle Dienste.

Die Hierarchie stellt Ihnen eine baumartige Ansicht der Protokolle der Auszeichnungsdatei zur Verfügung, die Sie ein- und ausklappen können. Beim Öffnen der Ansicht sind die Äste vollständig ausgeklappt.

Jeder Eintrag besitzt statistische Werte zu einem Protokoll. Kommt ein Darstellungsfilter zum Einsatz, so werden dieser bzw. diese im Kopfbereich angezeigt.



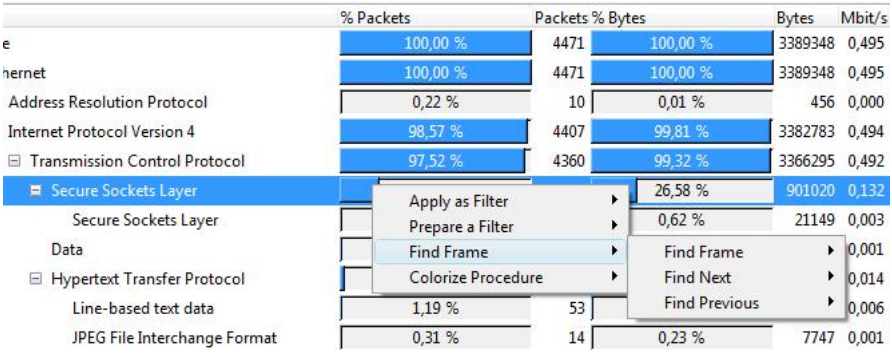
Die Protokollhierarchie.

Die Protokollhierarchie bietet Ihnen neben der Protokollinformation folgende Informationen:

- **% Packets**: Hier erfahren Sie, wie hoch der Anteil dieses Protokolls am gesamten Traffic ist. Sollten Sie hier insbesondere bei den *Data*-Einträgen unverhältnismäßig hohe Werte finden, sollten Sie diesen Traffic genauer unter die Lupe nehmen.

- **Packets**: In dieser Spalte erfahren Sie die exakte Anzahl an Paketen eines Protokolls.
- **Bytes**: Hier erfahren Sie die absolute Zahl an Bytes für das jeweilige Protokoll.
- **MBit/s**: In dieser Spalte wird die Bandbreite eines Protokolls relativ zur Aufzeichnungsdauer angezeigt.
- **End Packets**: Gibt die absolute Anzahl an Paketen für dieses Protokoll an.
- **End Bytes**: Hier entsprechend die absolute Anzahl an Bytes.
- **End MBit/s**: Hier erfahren Sie die Bandbreite eines Protokolls.

Datenpakete enthalten in der Regel mehr als ein Protokoll. Auch in voranstehender Abbildung kommen mehrere Protokolle zum Einsatz.



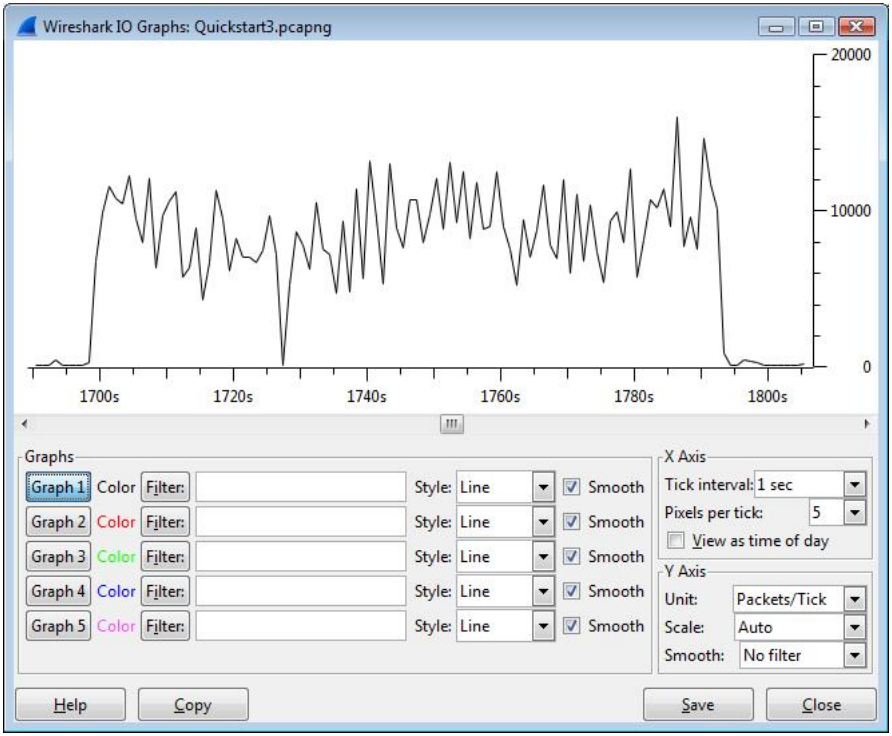
Die Auswahl eines Eintrags für die weitere Analyse.

Weist nun ein Eintrag in der Protokollhierarchie eine auffällig hohen Traffic-Anteil auf, so sollten Sie sich diesen näher ansehen. Dazu markieren Sie den Eintrag in der Hierarchie mit der rechten Maustaste und sehen ihn für die weitere Analyse vor.

Die Protokollhierarchie ist Ihr erstes Werkzeug, wenn es um die Aufdeckung von verdächtigem Netzwerkverkehr geht.

6.6 Bandbreitennutzung analysieren

Das Identifizieren von auffälligem Datenverkehr ist die eine Sache, aber um herauszufinden, ob es sich auch um unerwünschten oder gar bösartigen Traffic handelt, sollten Sie diese Eindrücke durch eine Bandbreitenanalyse ergänzen. Wireshark stellt Ihnen mit dem Menübefehl *Statistics > IO Graph* eine grafische Aufbereitung des Traffics zur Verfügung. Sie können über den Darstellungsfilter oder mit Hilfe der Protokollhierarchie die Darstellung entsprechend auf verdächtige Protokolle und Adressen beschränken.



Mit der grafischen Aufbereitung der Bandbreitennutzung können Sie den Datenfluss sehr schön verfolgen.

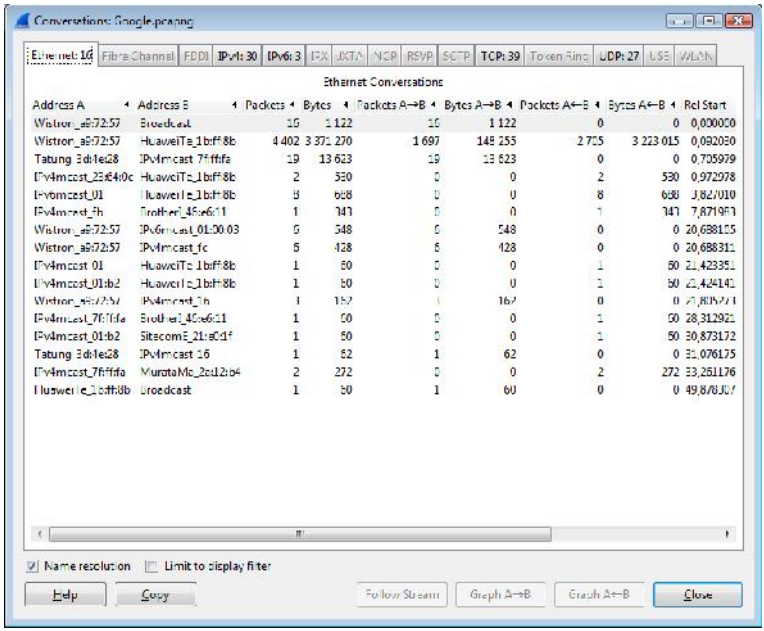
Die grafische Auswertung des Traffics zeichnet den Datentransfer, genauer die Datenmenge, auf der Zeitachse. Über den *Graphs*-Bereich können Sie den Traffic filtern und dabei unterschiedlichem Datenverkehr verschiedene Farben und Filter

zuweisen. Über die X- und Y-Achsenkonfiguration können Sie die Skalierung anpassen. Das Verstehen des Traffics vereinfacht sich, wenn Sie in der X-Achsenkonfiguration die Option *View as Time of day* aktivieren. Dann werden die tatsächlichen Zeitpunkte in der Visualisierung angezeigt.

6.7 Konversationen

Oftmals interessiert uns nicht nur der gesamte Traffic oder Teilbereiche des Traffic, der durch ein Netzwerk fließt, sondern man interessiert sich für den Traffic zwischen zwei Endpunkten. In der Wireshark-Terminologie handelt es sich es hierbei um Konversationen.

Auch hierfür stellt Ihnen das *Statistics*-Menü die entsprechenden Funktionen zur Verfügung. Sie öffnen den zugehörigen Dialog mit dem Menübefehl *Statistics* > *Conversations*.

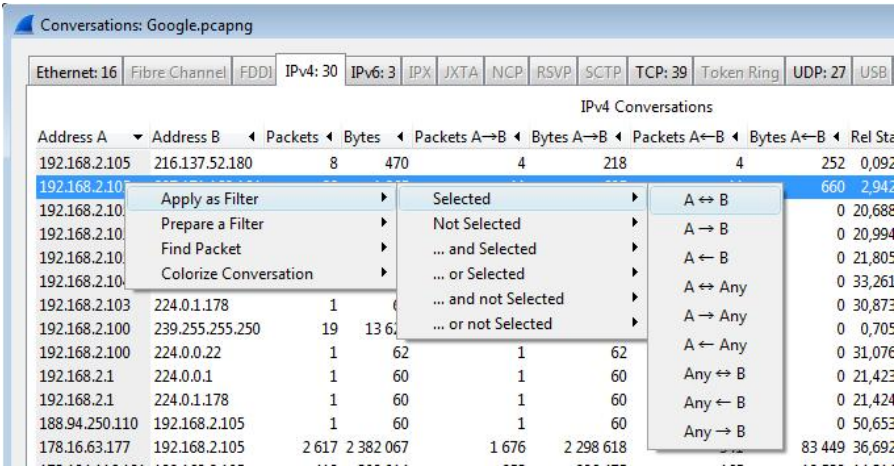


Die Konversationen in Ihrer Aufzeichnungsdatei.

Der Dialog führt neben der IP-Adresse und der Paket- und Byte-Anzahl vier weitere wichtige Informationen auf:

- Dauer zwischen dem Start der Aufzeichnung und dem Beginn der Konversation
- Status der Konversation
- Dauer der Konversation in Sekunden
- Durchschnittliche Datenmenge, die in jede Richtung fließt

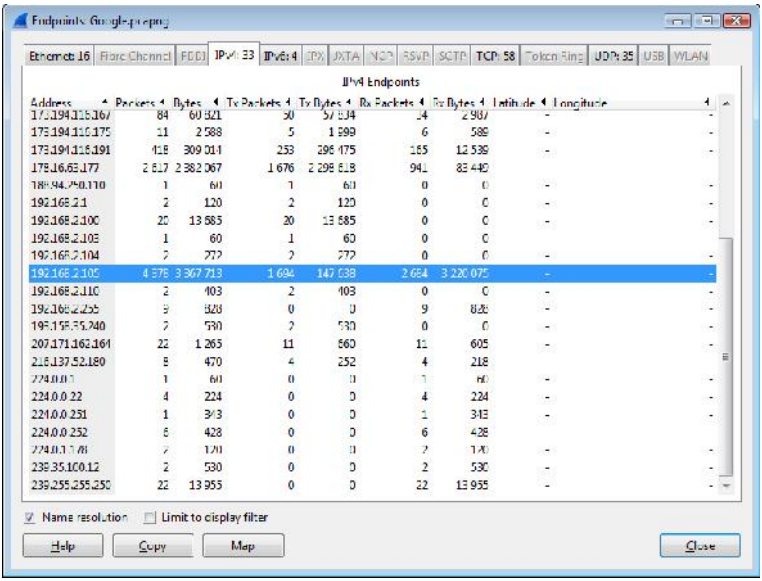
Sie können über die Registerkarten auch zu den IP4- oder IP6-Registern wechseln, um die Zielsysteme einfacher zu identifizieren. Jede Reihe entspricht einer Konversation. Damit ist auch klar, wie Sie die Ansicht auf eine bestimmte Konversation von zwei Endpunkten beschränken: Sie markieren den gewünschten Eintrag mit der rechten Maustaste und führen aus dem Kontextmenü den Befehl *Apply As Filter* aus. Aus dem Untermenü *Selected* können Sie dann beispielsweise die Konversation von A und B oder nur die in eine Richtung oder die von A mit beliebigen anderen Endpunkten wählen.



Die Beschränkung der Ansicht auf eine Konversation.

6.8 Endpunkte

Wireshark verfügt über eine weitere ähnliche Funktion: *Endpoints*. Damit können Sie die Endpunkte Ihrer Aufzeichnungen herausfinden. Auch hier steht jeder Eintrag wieder für einen Endpunkt. Sie können die Ansicht auch hier auf IP-Adressen umschalten oder aber einen Eintrag mit der rechten Maustaste als Filter verwenden.



Die Endpunkte der Aufzeichnungen.

6.9 Weitere statistische Funktionen

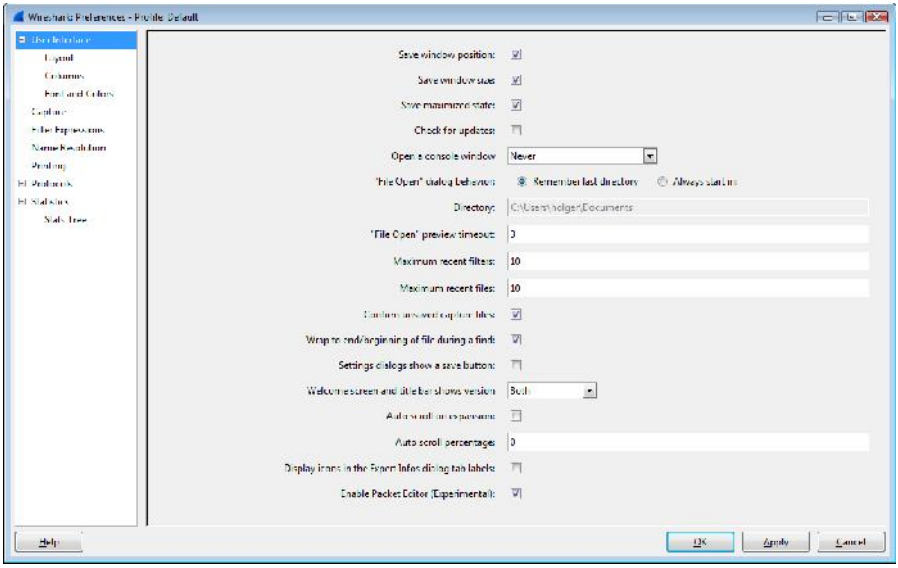
Das *Statistics*-Menü verfügt über weitere interessante Funktionen. Sie können mit dem Untermenü *Response Time* beispielsweise die Antwortzeiten von bestimmten Diensten abfragen.

Mit Hilfe des Untermenüs *Compare* können Sie zwei Capture-Dateien miteinander vergleichen. Wenn Sie einen WLAN-Adapter verwenden, können Sie sich auch mit dem Untermenü *WLAN Traffic* die WLAN-Statistiken anschauen.

7 Wireshark anpassen

Wireshark ist von Haus aus so konfiguriert, dass es für die Anforderungen der meisten Anwender gerüstet ist und unmittelbar nach der Installation für die ersten Aufzeichnungen und Netzwerkanalysen verwendet werden kann. Doch je intensiver Sie mit dem Programm arbeiten, um so mehr werden Sie hier und da an Stellschrauben drehen wollen. Einige Anpassungsmöglichkeiten haben wir bereits im bisherigen Verlauf dieses Buchs kennengelernt, beispielsweise das Einfügen einer neuen Spalten in der Paketliste.

Je nach Anwendungsbereich ist es auch manchmal sinnvoll, mit unterschiedlichen Konfigurationseinstellungen zu arbeiten. Auch hierfür hat Wireshark mit der Profilverwaltung die passende Lösung parat. Darüber hinaus bietet Ihnen Wireshark verschiedenste Anpassungsmöglichkeiten, die wir uns in diesem Kapitel genauer anschauen.



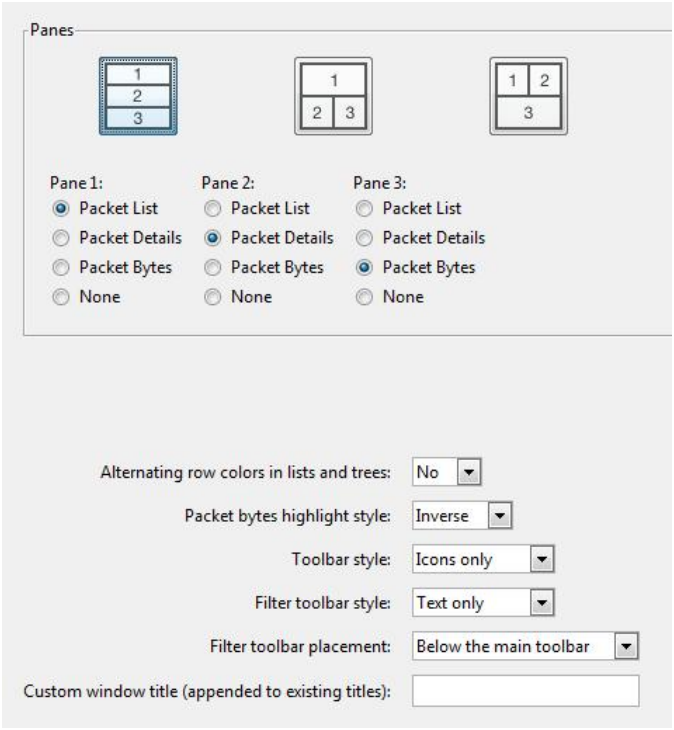
Die Programmeinstellungen von Wireshark.

7.1 Wireshark anpassen

Wireshark stellt Ihnen mit dem Menübefehl *Edit > Preferences* die Programmeinstellungen zur Verfügung. Hier können Sie verschiedene Anpassungen der Benutzeroberfläche vornehmen. Außerdem stehen Ihnen für alle unterstützen Protokolle Anpassungsmöglichkeiten zur Verfügung.

Die Programmeinstellungen umfassen sieben Untermenüs: *User Interface*, *Capture*, *Filter Expressions*, *Name Resolution*, *Printing*, *Protocols* und *Statistics*. Das Untermenü *User Interface* umfasst selbst wieder weitere Untermenüs.

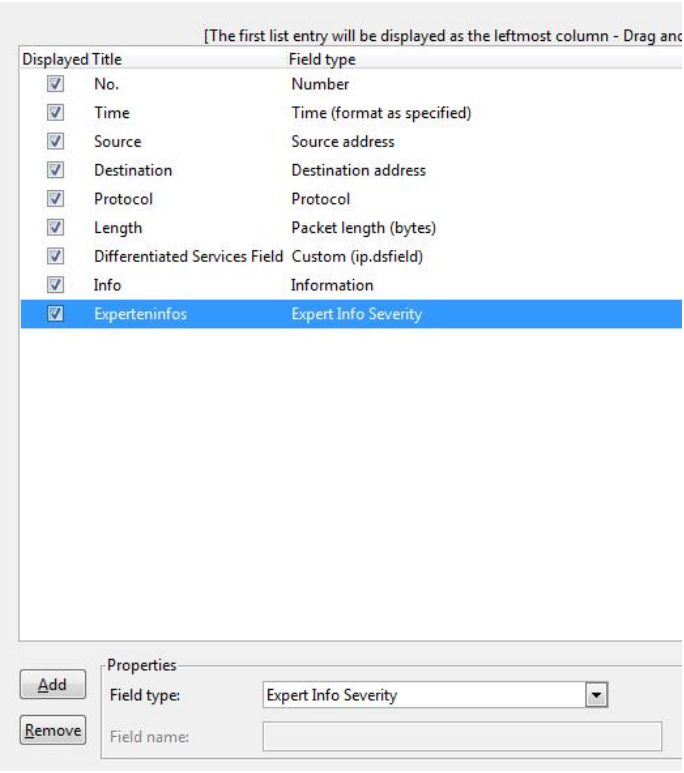
Mit den allgemeinen Einstellungen der Programmoberfläche bestimmen Sie, ob Wireshark sich die Fensterposition und Größe für den nächsten Programmstart merkt. Mit *File Open Dialog Directory* bestimmen Sie, ob Wireshark beim Öffnen von Aufzeichnungen das zuletzt verwendete oder ein bestimmtes Verzeichnis wählt.



Die Layout-Konfiguration.

Das Untermenü *Layout* erlaubt Ihnen die Anpassung des Layouts der drei Bereiche Paketliste, Paketdetails und Byte-Ansicht. Der *Layout*-Dialog stellt Ihnen sechs verschiedene Ansichten zur Auswahl, wobei Sie über *Pane1*, *Pane2* und *Pane3* die Zuordnung ändern können.

Mit den Auswahlmenüs *Toolbar style* und *Filter toolbar style* bestimmen Sie, ob die Symbol- und Filterleisten lediglich Icons, Text oder beides anzeigt.

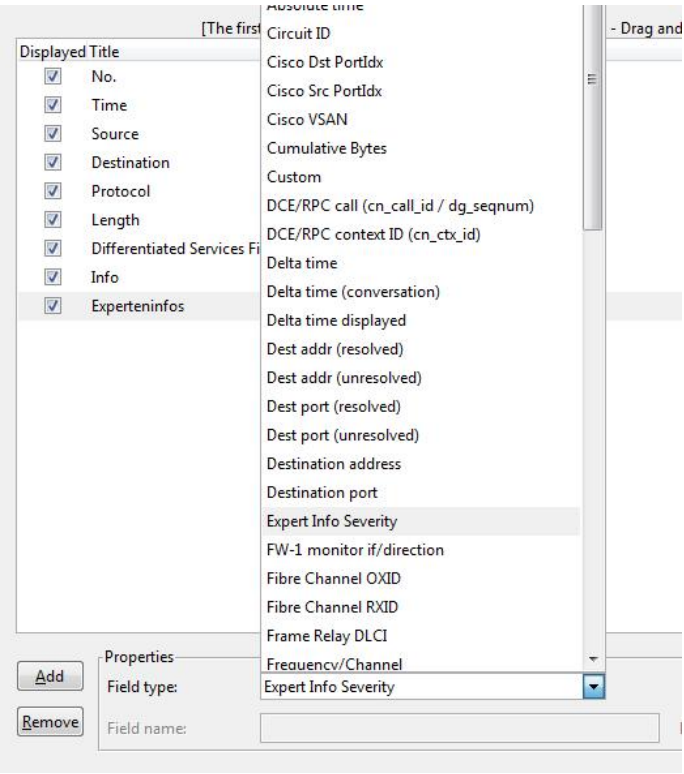


Die Anpassung der Spalten der Paketliste.

Oben hatte ich kurz angedeutet, dass Sie auch die Experteninfo in der Paketliste platzieren können. So haben Sie die entsprechenden Traffic-Bewertungen immer direkt nach dem Laden einer Capture-Datei verfügbar. Neben der Experteninfo können Sie aber auch andere Spalten in die Paketliste einfügen.

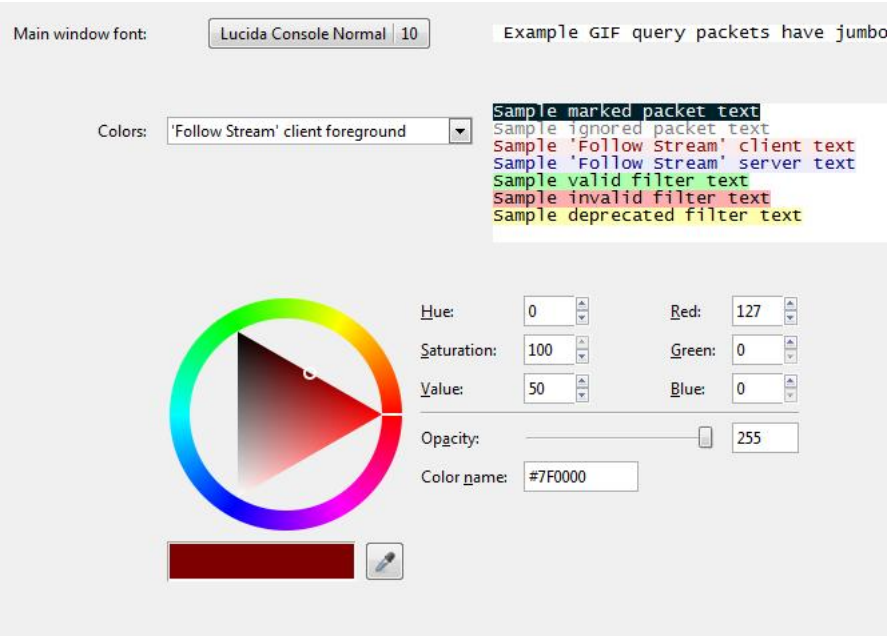
Im Untermenü *Columns* können Sie die Spalteninformationen ein- und ausblenden, die Bezeichnung, die Reihenfolge ändern und auch neue hinzufügen. Um eine Spalte auszublenden, deaktivieren Sie das zugehörige Kontrollkästchen in der Spalte *Displayed*. Mit einem Doppelklick auf den Titel können Sie diesen bearbeiten. Um eine Spalte an eine neue Position zu verschieben, markieren Sie diese und ziehen sie einfach auf die gewünschte Position.

Auch das Anlegen einer neuen Spalte ist einfach: Klicken Sie zunächst auf die Schaltfläche *Hinzufügen* und bearbeiten Sie gegebenenfalls den Spaltentitel. Dann klicken Sie unter *Properties* auf das Auswahlmenü *Field type*. Das zugehörige Auswahlmenü stellt Ihnen Dutzende Eigenschaften zur Auswahl. Um die Experteninformationen in der Paketliste einzublenden, wählen Sie den Eintrag *Expert Info Severity*.



Die Auswahl des Feldtyps.

Mit dem Untermenü *Font and Colors* bestimmen Sie die Schrift des Hauptfensters und die Farben für die wichtigsten Markierungen in der Paketliste. Um die Standardbelegung für markierte, ignorierte und gefolgten Streams sowie für Filter im Filterdialog zu ändern, wählen Sie diese Information im Auswahlmenü *Colors* aus und ändern über den Farbkreis und dessen Einstellungen die Farbgestaltung.

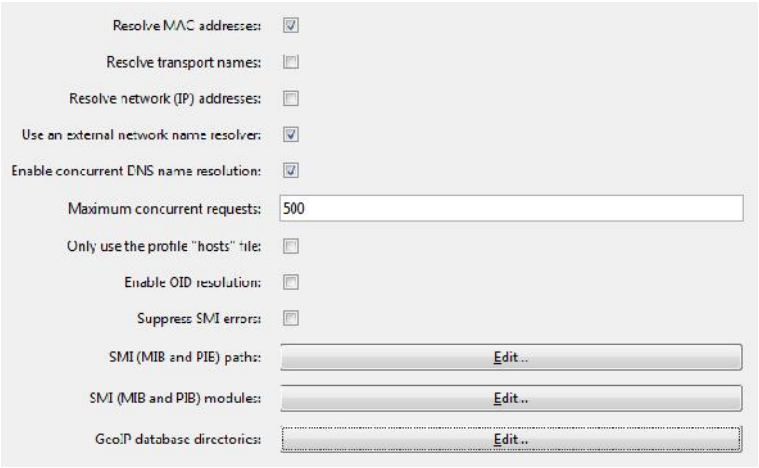


Die Anpassung der Schrift und Farben.

Im Untermenü *Capture* bestimmen Sie das Standard-Interface und können Sie mit *Edit* auf die Interface-Konfiguration zugreifen. Hier sollten Sie sicherstellen, dass der Promicuous Modus aktiviert ist und dass die Auszeichnung im PCAPNG-Format erfolgt.

Wireshark erlaubt Ihnen im Untermenü *Filter Expresssion* das Anlegen von eigenen Filterkonfigurationen, die dann rechts in der Filter-Symbolleiste angewendet werden können.

In Kapitel 6.3 hatte ich das Problem der Namensauflösung in Wireshark angesprochen. Im Untermenü *Name Resolution* konfigurieren Sie die Auflösung. Hier können Sie außerdem externe Dienste wie SMI und Geo IP-Datenbanken einbinden.



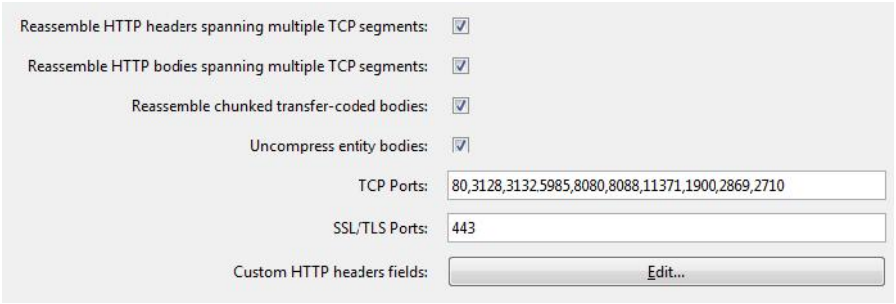
Die Konfiguration der Namensauflösung.

Um eine zuverlässige Namensauflösung zu erzielen, deren Ergebnisse dann auch in den Expertendialogen und an anderer Stelle zu finden sind, müssen Sie die Namensauflösung einrichten. Dabei greifen Sie am besten zu Diensten wie SMI und Geo IP-Datenbanken à la MaxMind zurück. Die SMI Tools finden Sie unter *http://www.ibr.cs.tu-bs.de/projects/libsmi/tools/*.

Als bester Geo IP-Datenbankdienst gilt MaxMind (*http://www.maxmind.com*). Um diesen Dienst in Ihrer Wireshark-Installation einzubinden, klicken Sie auf die *Edit*-Schaltfläche und geben Sie die Pfade an.

Im *Printing*-Untermenü können Sie das Format (Text/PostScript), den Druckbefehl und die Ausgabedatei bestimmen.

Sehr umfangreich fallen die Anpassungsmöglichkeiten des Untermenüs *Protocols* aus. Hier können Sie für jedes von Wireshark unterstützte Protokoll eigene Anpassungen vornehmen. Beim IPv4-Protokoll können Sie beispielsweise das Reassembling von fragmentierten Datagrammen und die Unterstützung für Geo IP-Abfragen aktivieren. Bei *HTTP* können Sie das Dekomprimieren des gesamten Body und die Standardports einrichten sowie benutzerdefinierte Header-Felder anlegen.



Die Konfiguration des HTTP-Protokolls.

Schließlich erlauben die Programmeinstellungen noch die Anpassung einiger statistischer Einstellungen. Hier sind in der Regel keine Änderungen notwendig.

7.2 Paketfärbung

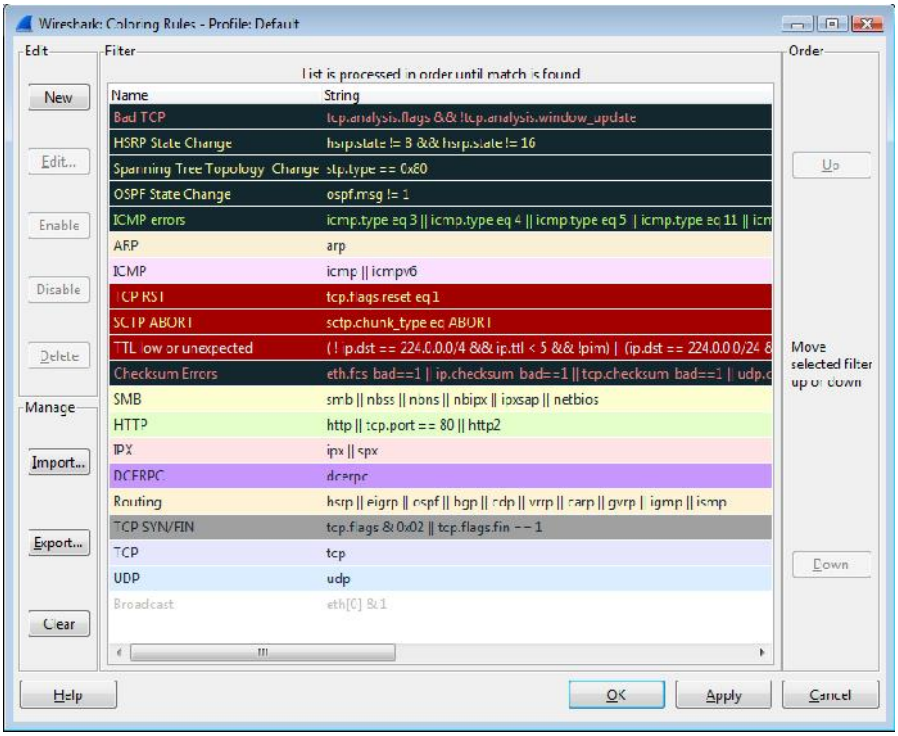
Ein ausgesprochen praktischer und hilfreicher Mechanismus in Wireshark ist die farbige Kennzeichnung von Paketen. Die Voreinstellungen sind über das Menü *View > Coloring Rules* einseh- und bearbeitbar.

Wireshark kennt zwei Typen an Farbregeln: Solche, die nur temporär bis zum Schließen des Programms gelten, und permanente, also solche, die auch bei der nächsten Wireshark-Session gültig sind.

Die temporären Farben sind nach dem Markieren eines Pakets verfügbar. Betätigen Sie die Tastenkombination *Strg + Ziffer*. Die Standardzuweisung ist über das Menü *View > Colorize Conversation* abrufbar.

Wenn Sie allerdings die permanenten Vorgaben bearbeiten wollen, müssen Sie den oben aufgeführten Menübefehl ausführen. Der öffnet den Dialog *Coloring Rules*, in dem Sie beispielsweise erkennen, dass dort der HTTP-Traffic standardmäßig hellgrün und der TCP-Traffic hellviolett hinterlegt ist.

Um eine Voreinstellung zu bearbeiten, markieren Sie den entsprechenden Eintrag und klicken dann auf die Schaltfläche *Edit*. In dem Editierdialog können Sie die Filterkonfiguration einsehen und die Farbzuweisung (Vorder- und Hintergrundfarbe) ändern.



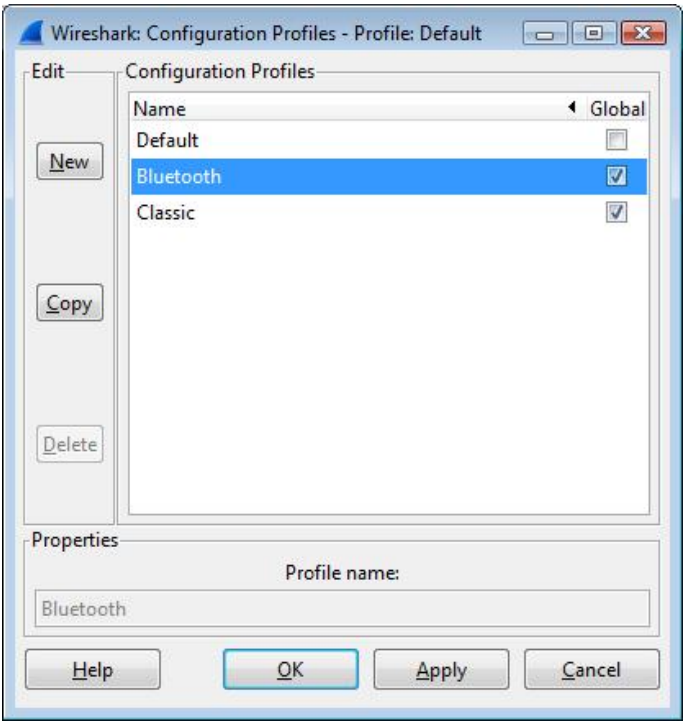
Die Konfiguration der Farbzuweisung.

7.3 Profile

Wireshark ist ein sehr flexibles Werkzeug, das in unterschiedlichen Kontexten eingesetzt werden kann. Sie können eine Installation beispielsweise für die Analyse des internen Traffics, dann zur Auswertung von WLAN-Verbindungen und dann für allgemeine Analysen verwenden.

Für derlei unterschiedliche Analysen sind oftmals verschiedene Konfigurationen erforderlich oder wünschenswert. Wireshark stellt Ihnen hierfür die sogenannte Profilverwaltung zur Verfügung.

Der Zugriff auf die Profilverwaltung erfolgt mit dem Menübefehl *Edit > Configuration Profiles*. Alternativ verwenden Sie die Tastenkombination *Umschalt + Strg + A*.



Die Profilverwaltung.

In einem Profil können folgende Daten gespeichert werden:

- Programmeinstellungen
- Capture-Filter
- Darstellungsfilter
- Farbregeln
- Deaktivierte Protokolle
- Benutzereinstellungen

Wenn Sie Wireshark starten, wird das Standardprofil *Default* ausgeführt. Wenn Sie Änderungen an einer der genannten Eigenschaften oder Einstellungen vornehmen, werden diese dem Standardprofil zugeordnet.

Über die Profilverwaltung können Sie weitere Profile anlegen. Über die Statuszeile von Wireshark können Sie dann zu anderen Profilen wechseln. Sowie Sie ein anderes Profil aktiviert haben und beispielsweise die Programmeinstellungen oder Filterkonfiguration ändern, werden diese auf das aktive Profil angewendet.

Anhang A – Konsolenwerkzeuge

Wireshark stellt Ihnen eine komfortable GUI zur Verfügung, über die Sie alle wichtigen Analysefunktion vornehmen können. Doch Sie können Wireshark auch nahezu vollständig auf der Konsole bedienen. Außerdem stehen verschiedene weitere Konsolenwerkzeuge zur Verfügung.

Wireshark auf der Konsole starten

Wenn Sie Wireshark auf der Konsole ausführen, so wird immer auch die GUI gestartet. Allerdings können Sie dabei so viele Parameter angeben, wie Sie wollen. Im Folgenden sind die wichtigsten Parameter beschrieben. Die Ausführung erfolgt dabei nach folgendem Muster:

```
wireshark [optionen] ... [datei]
```

Soll Wireshark die Aufzeichnung beim Eintreten einer bestimmten Bedingung beenden, so erzielen Sie das wie folgt:

```
-a <capture autostop bedingung>
```

Die Bedingung muss dabei einen der folgenden Werte annehmen:

- duration:wert – Beendet das Schreiben in die Capture-Datei nach der angegebenen Zeitspanne.
- filesize:wert – Beendet das Schreiben, sowie die Capture-Datei eine bestimmte Größe in Kilobyte erreicht hat.
- files:wert – Beendet das Schreiben in Capture-Dateien, nachdem eine bestimmte Anzahl an Dateien geschrieben wurden.

Wenn Sie die maximale Größe der Capture-Datei spezifiert haben, versetzt diese Option den Sniffer in den sogenannten Ring Buffer-Modus.

```
-b <capture ring buffer option>
```

In diesem Modus schreibt Wireshark in verschiedene Capture-Dateien. Dabei ist auch die Anzahl der Dateien anzugeben. Die Dateinamen erzeugt Wireshark auf Grundlage des Datums und der Anzahl an Dateien.

Unter Windows, allerdings nur unter der 32Bit-Variante, können Sie die Größe des Puffers bestimmen. Der ist meist 1 bis 2 MB groß. Die Puffergröße bestimmen Sie wie folgt:

```
-B <puffergröße>
```

Um die maximale Anzahl der Pakete festzulegen, die beim Live Capturing aufgezeichnet wird, verwenden Sie folgende Option:

```
-c <anzahl an pakete>
```

Diese Konfiguration sollten Sie in Verbindung mit der Option *-k* verwenden.

Um die Liste der Netzwerkschnittstellen auszugeben, die Wireshark nutzen kann, und um das Programm dann zu beenden, verwenden Sie folgende Option:

```
-D
```

Dabei werden für jede Schnittstelle die Nummerierung, der Interface-Name und eine womöglich hinterlegte Beschreibung ausgegeben.

Die folgende Option bestimmt den Anfangsfilterausdruck, der für die Aufzeichnung verwendet wird:

```
-f <capture filter>
```

Nach dem Einlesen einer Datei mit der Option *-r* bestimmen Sie mit der folgenden Option, zu welcher Paketnummer Wireshark springt:

```
-g <paket nummer>
```

Die folgende Option gibt den Hilfetext von Wireshark aus:

```
-h
```

Bestimmt den Namen des Interfaces für die Live-Aufzeichnung:

```
-i <capture interface>
```

Die Netzwerkschnittstellen sollten dabei mit den Namen übereinstimmen, die Wireshark bei der Verwendung der Option *-D* ausgibt. Wenn Sie mit einem unixartigen System arbeiten, können Sie mit den Befehlen *netstat -i* bzw. *ifconfig -a* die Schnittstellennamen abrufen.

Wenn Sie keine Schnittstelle angeben, sucht Wireshark nach der Schnittstellenliste. Kann das Programm keine Schnittstellen finden, so wird eine Fehlermeldung ausgegeben und es kann auch keine Aufzeichnung erfolgen.

Nach dem Einlesen einer Aufzeichnungsdatei mit der Option *-r*, können Sie mit folgender Option zum ersten Paket springen, das dem angegebenen Filter entspricht:

```
-J <filter>
```

Anstelle der groß geschriebenen Option *-J* suchen Sie mit der kleingeschriebenen Variante rückwärts:

```
-j
```

Die folgende Option sorgt dafür, dass Wireshark unmittelbar mit der Aufzeichnung beginnt. Sie müssen zusätzlich die Option *-i* verwenden, um die Schnittstelle anzugeben, die für die Aufzeichnung verwendet wird:

```
-k
```

Der folgende Schalter aktiviert das automatische Scrollen in der Paketliste, wenn neue Pakete bei der Aufzeichnung hinzufügt werden:

```
-l
```

Listet die Data Link-Typen, die von der verwendeten Schnittstelle unterstützt werden:

```
-L
```

Auf der Konsole können Sie sogar den Schriftnamen für die Textdarstellung von Wireshark bestimmen:

```
-m <font>
```

Um die Namensauflösung für Hostnamen, TCP- und UDP-Ports etc. zu deaktivieren, verwenden Sie die folgende Option:

```
-n
```

Um die Namensauflösung für bestimmte Adresstypen und Portnummern zu aktivieren, verwenden Sie folgende Konfiguration:

```
-N <namensauflösungszeichen>
```

Beim Start von Wireshark auf der Konsole können Sie sogar die Voreinstellungen bzw. die letzten Einstellungen überschreiben:

```
-o <voreinstellungen/letzte einstellungen>
```

Die werden standardmäßig gespeichert. Ein Beispiel für die Verwendung:

```
wireshark -o mgcp.display_dissect_tree:TRUE
```

Damit eine Schnittstelle nicht in den Promiscuous-Modus versetzt wird, verwenden Sie folgende Option:

```
-p
```

Um Wireshark mit bestimmten Einstellungen zu starten, die an anderer Stelle abgelegt sind, verwenden Sie folgende Option:

```
-P <pfad einstellungen>
```

Das kann beispielsweise beim Starten von einem USB-Stick sinnvoll sein.

Die folgende Option erzwingt das Beenden von Wireshark nachdem die Aufzeichnung beendet ist. Die Option muss in Verbindung mit *-i* und *-w* verwendet werden:

```
-Q
```

Um der Aufzeichnungsdatei einen bestimmten Namen zuzuweisen, verwenden Sie folgenden Schalter:

```
-r <dateiname>
```

Mit der folgenden Konfiguration bestimmen Sie das Format des Zeitstempels:

```
-t <format>
```

Mögliche Formate sind *r* (relativ), *a* (absolute), *ad* (absolute mit Datum), *d* (relativ zum vorherigen Paket) und *e* (Zeitstempel seit dem 01.01.1970).

Wenn Sie die Programmversion von Wireshark ausgeben wollen, verwenden Sie die folgende Option:

```
-v
```

Sie können auch den Dateinamen für das Speichern der Capture-Datei bestimmen:

```
-w <dateiname>
```

.

Um spezifische Optionen an das TShark-Modul zu übergeben, verwenden Sie folgendes Kommando:

```
-X <option>
```

Damit Wireshark verschiedene statistische Daten sammelt und diese quasi in Echtzeit darstellt, verwenden Sie folgende Option:

```
-z <statistik>
```

TShark

Bei TShark handelt es sich um eine konsolenorientierte Version von Wireshark für die Aufzeichnung und die Darstellung von Paketen, wenn die interaktive GUI nicht gefragt oder nicht verfügbar ist. Die Konsolenversion unterstützt die gleichen Optionen wie Wireshark. Die Verwendung:

```
tshark [optionen] ...
```

Mit der Option *-D* können Sie beispielsweise die verfügbaren Schnittstellen abrufen. TShark können Sie auch verwenden, um bestehende Capture-Dateien zu verarbeiten.

tcpdump

Manchmal ist es sinnvoll, die Datenpakete nicht mit Wireshark, sondern mit tcpdump aufzuzeichnen. Das ist insbesondere dann sinnvoll, wenn Sie den Traffic auf entfernten Systemen aufzeichnen wollen oder nicht zusätzlichen Traffic durch die Remote-Ausführung von Wireshark erzeugen wollen.

Da tcpdump standardmäßig nur die ersten 68 bis 96 Bytes jedes Pakets aufzeichnet, müssen Sie das Konsolenwerkzeug für eine vollständige Aufzeichnung wie folgt aufrufen:

```
tcpdump -i <interface> -s 65535 -w <datei>
```

Wichtig ist dabei, dass Sie korrekte Schnittstellenangaben verwenden und den Namen der Aufzeichnungsdatei spezifizieren. Nach einer Aufzeichnung mit tcpdump können Sie diese Aufzeichnungen in Wireshark importieren und auswerten. tcpdump (*http://www.tcpdump.org*) ist nicht Teil Ihrer Wireshark-Installation und muss gesondert heruntergeladen werden.

dumpcap

Mit dumpcap gehört ein Dump-Tool zu Ihrer Wireshark-Installation. Es zeichnet Datenpakete des Live-Traffic auf und schreibt diese in eine Capture-Datei. Das native Format von dumpcap ist das libpcap-Format, das auch von tcpdump, Wireshark und anderen Tools unterstützt wird. Die Verwendung:

```
dumpcap [optionen]
```

Mit der Option *-i <interface>* geben Sie den Namen der Schnittstelle für die Aufzeichnung an. Für Remote Capturing verwenden Sie folgendes Format:

```
rpcap://<host>/<interface>
TCP@<host>:<port>
```

Ein Beispiel für die Verwendung, bei dem die Pakete der Schnittstelle *eth0* für die Dauer von 60 Sekunden in die Datei *output.pcapng* geschrieben werden:

```
dumpcap -i eth0 -a duration:60 -w output.pcapng
```

Sie können das Tool jederzeit mit der Tastenkombination *Strg + C* beenden.

editcap

Mit editcap verfügt Wireshark über ein kleines Tool, mit dem Sie die Capture-Dateien editieren können – zumindest teilweise. Seine wichtigste Aufgabe ist das Entfernen von Paketen aus Aufzeichnungsdateien. Die Verwendung:

```
editcap [optionen] ... <eingabedatei> <ausgabedatei> [ <packet#>[-<packet#>] ... ]
```

Wichtig ist, dass Sie sowohl Ein- als auch Ausgabedatei angeben.

mergecap

Auch auf Konsolenebene können Sie mehrere Aufzeichnungsdateien zu einer einzigen zusammenfassen. Das Tool unterstützt verschiedene Formate und kann auch Dateien unterschiedlicher Formate verknüpfen. Ein Beispiel für die Ausführung:

```
mergecap -w ausgabe.libpcap dhcp-capture.libpcap imap-1.libpcap
```

Index

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

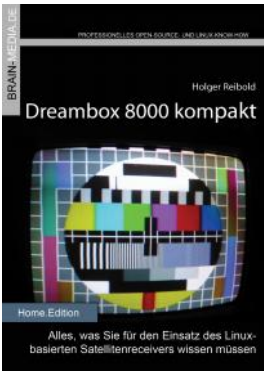
V

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

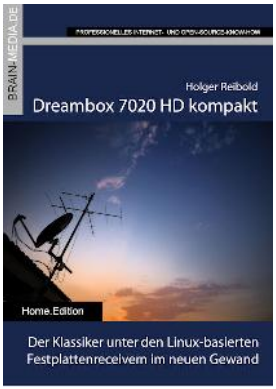
Der Klassiker unter den Flugsimulatoren geht in die zehnte Runde. Viele neue Funktionen und verbessertes Handling warten auf die Anwender. Kein Wunder also, dass die Fangemeinde wächst und wächst. Unser Handbuch beschreibt alles, was Sie für das Fliegen mit X-Plane wissen sollten.

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.