Netzwerkverkehrsanalyse mit Wireshark

Version 2.2

Inhaltsverzeichnis

Vorwort zu diesem Handout

Wir haben als Trainer und Seminarteilnehmer über Jahre hinweg die Erfahrung gemacht, dass Wissen am besten verinnerlicht werden kann, wenn es durch Praxis erworben wurde. Daher werden wir in diesem Kurs wo immer es möglich ist alle Inhalte direkt am Gerät vermitteln. Wir glauben daher auch nicht an ausgedruckte PowerPoint-Folien als „Handout“. Wir sind der Meinung, ein Handout zu einem Training muss so aufgebaut sein, dass es die wichtigsten Informationen kurz und prägnant zusammenfasst.

Daher werden Sie in diesem Handout kaum Aufzählungen und bloße Wissensrepräsentationen nur in begrenztem Umfang finden. Vielmehr werden wir wo immer es möglich ist direkt auf andere, möglichst aktuelle und in der Regel frei zugängliche Quellen verweisen. So lernen Sie bereits im Training, wo Sie wichtige Informationen finden, wenn Sie sie benötigen.

Nur, wo es uns zur späteren Auffrischung oder zum besseren Verständnis als sinnvoll erscheint, werden wir hier kurze Erklärungen oder Skizzen anführen.

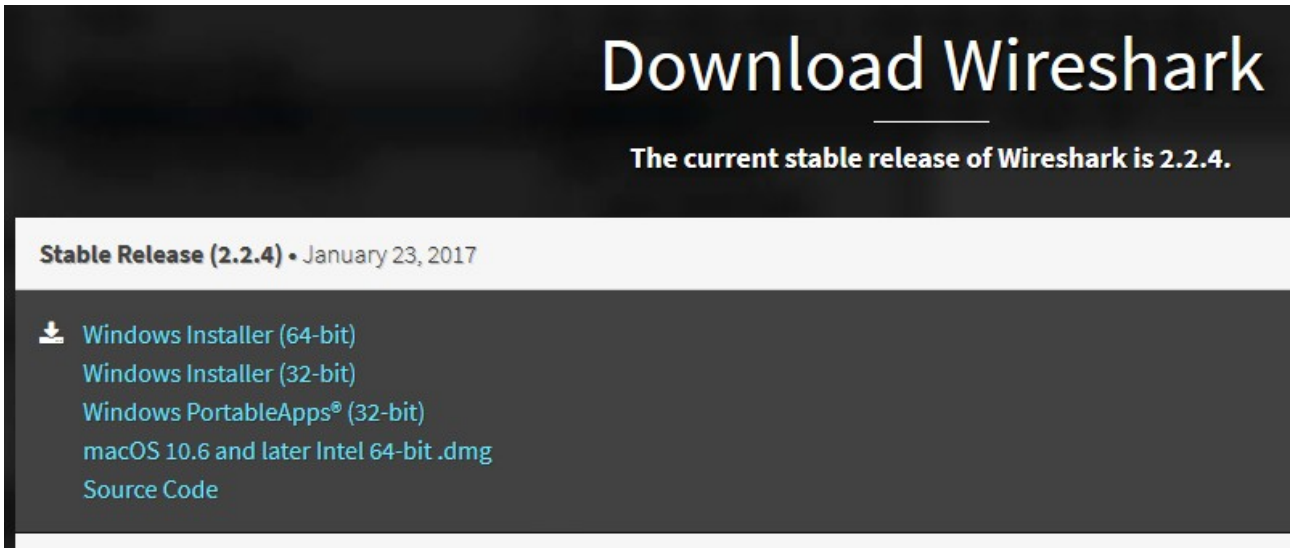
Wireshark – ein schneller Einstieg

Installation

Wireshark ist für verschiedene Betriebssysteme verfügbar und kann frei heruntergeladen werden. Dabei sollte darauf geachtet werden, das Installationsprogramm direkt von der Entwicklerseite zu beziehen:

`https://www.wireshark.org/`

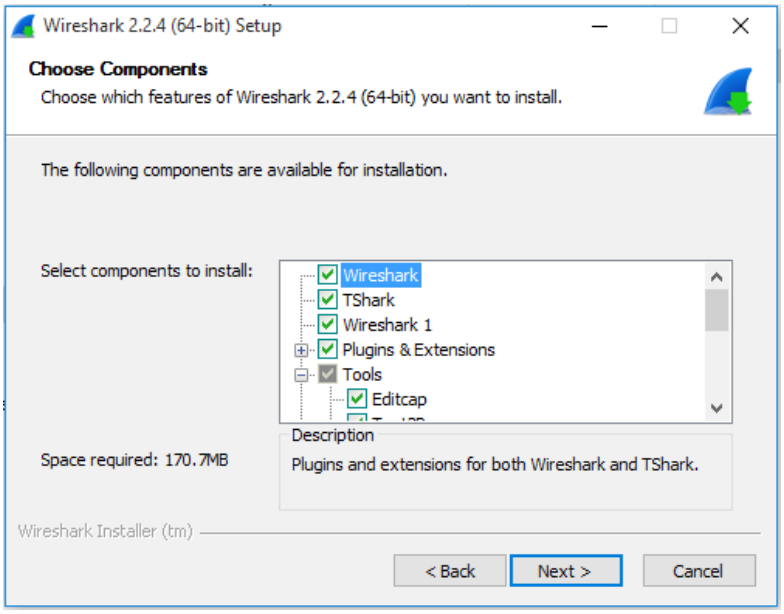
Für Linux[1] steht kein direkter Download zur Verfügung. Es wird empfohlen die Installation mittels apt durchzuführen und dabei ein PPA zu verwenden, damit Wireshark so aktuell wie möglich ist.



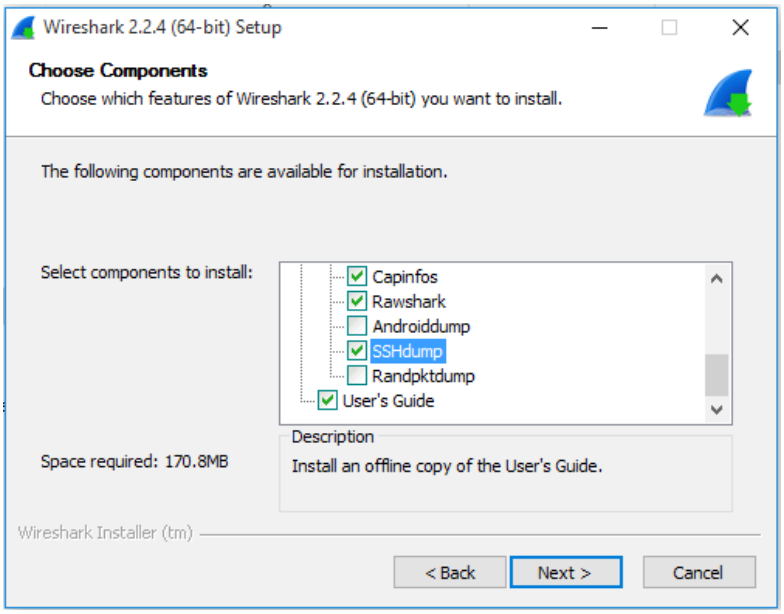
Wireshark-Downloadseite: https://www.wireshark.org/#download

Während der Installation gibt es ein paar Dinge zu beachten, die für den erfolgreichen Einsatz von Wireshark von Bedeutung sind.
So wird z.B. während der Installation die Auswahl der zu installierenden Komponenten angeboten. Im Zweig Tools wählen wir zusätzlich den Punkt SSHdump wie unten dargestellt. Dadurch wird es möglich aus Wireshark heraus eine SSH-Verbindung zu einem entfernten Host aufzubauen und dort direkt Mitschnitte anzufertigen. Dazu später mehr.

1 Für Ubuntu wird `ppa:wireshark-dev/stable` angeboten.

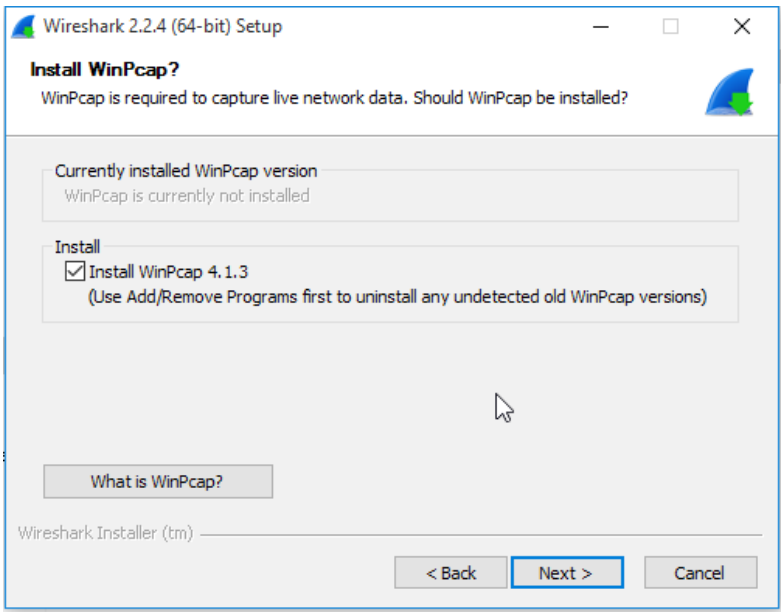


Auswahl der zu installierenden Komponenten



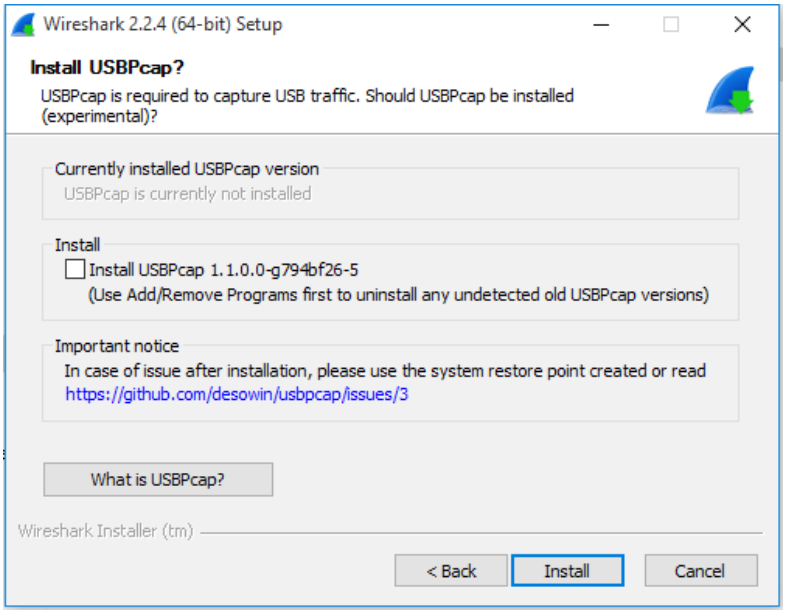
Bei Bedarf zusätzliche Komponenten auswählen

Die Installationsroutine von Wireshark startet einen weiteren Installer, der dazu dient den WinPcap-Treiber zu installieren. Dieser wird benötigt um Mitschnitte anfertigen zu können. Details hierzu im weiteren Verlauf.

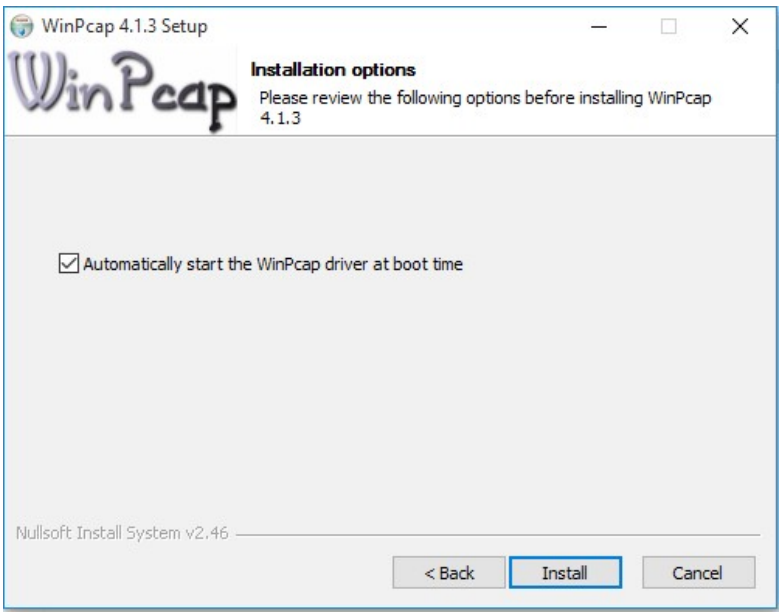


Installation des WinPcap-Treibers zulassen

Wireshark unterstützt seit einiger Zeit auch das Mitschneiden von Verkehr an USB-Interfaces. Hierfür wird ebenfalls ein spezieller Treiber namens USBPcap benötigt. Leider hat die zum Zeitpunkt der Erstellung dieser Unterlagen aktuelle Version dazu geführt, dass die USB-Controller vom Betriebssystem nicht mehr verwendet werden konnten. Dieser Treiber wird deshalb nicht mitinstalliert.



USBPcap-Treiber **nicht** installieren

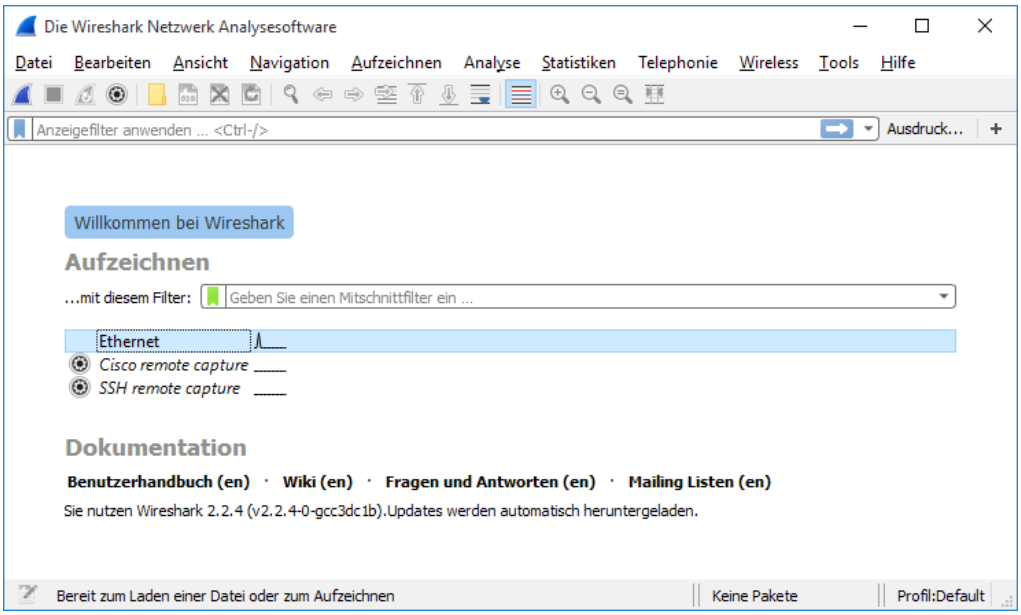


WinPcap-Treiber mit dem Betriebssystem starten

Ein erster Überblick

Schnellstart

Um direkt einen Mitschnitt zu starten, genügt es im Startfenster von Wireshark einen Doppelklick auf eine der dort angezeigten Netzwerkschnittstellen zu machen. Die Linie neben der Schnittstellenbezeichnung stellt das auf dieser Schnittstelle verzeichnete Verkehrsaufkommen dar.



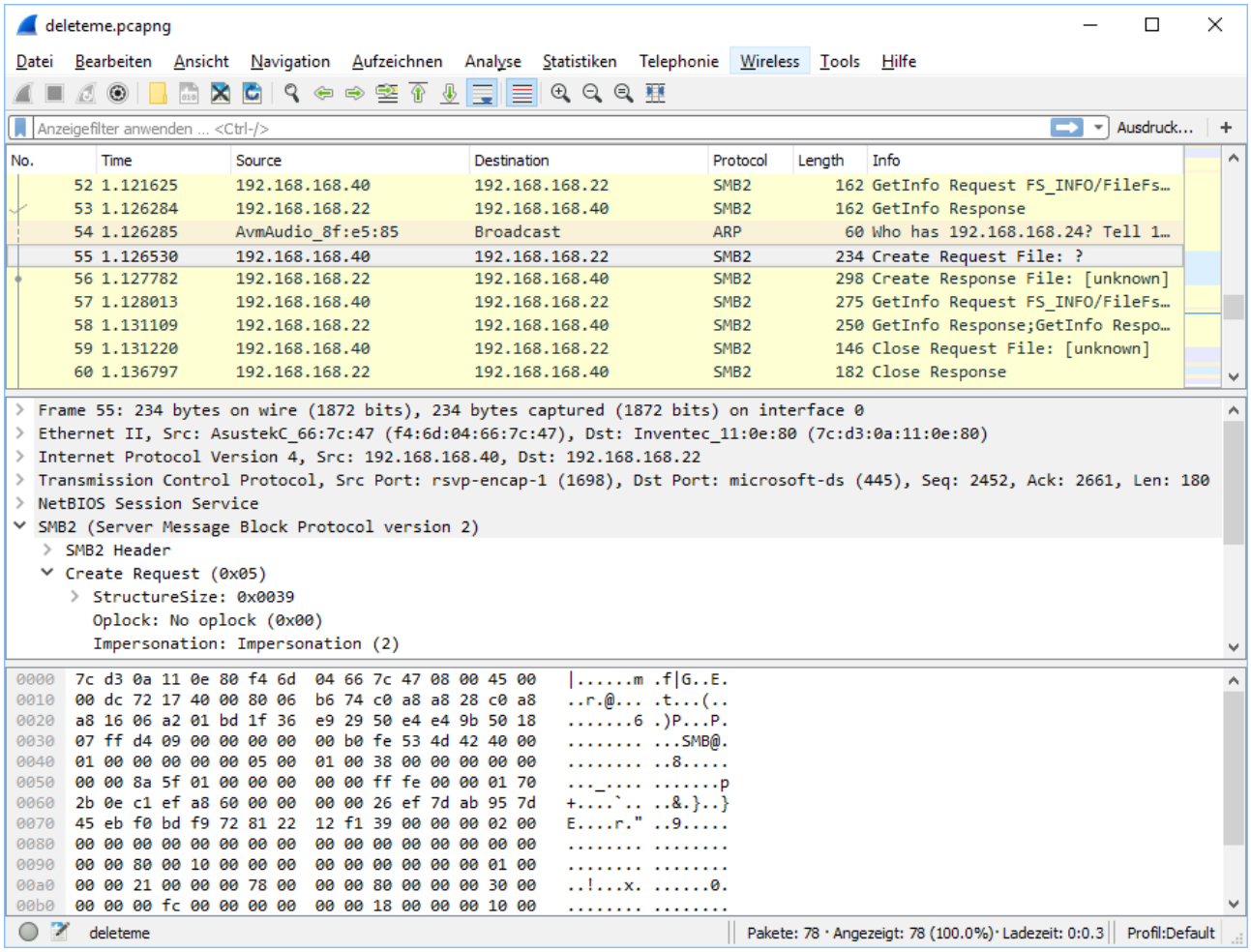
Startfenster von Wireshark mit Verkehr auf der Ethernet-Schnittstelle

Das Mitschnittfenster – Überblick

Das Mitschnittfenster, welches gleichzeitig das Hauptfenster von Wireshark ist, zeigt im Normalfall 3 Hauptansichten:

- Paketliste
- Paketdetails
- Paket Bytes

Diese füllen den Großteil des Fensterinhaltes aus. Am oberen Rand des Fensters befindet sich die Menüleiste, die Werkzeugleiste und die Leiste für den Anzeigefilter. Am unteren Rand des Fensters ist die Statuszeile zu finden.



Mitschnittfenster

Das Mitschnittfenster – Details

Im Folgenden soll erläutert werden, was die einzelnen Bestandteile des Mitschnittfensters anzeigen und wofür sie zu verwenden sind.

Paketliste

In der Paketliste wird eine Übersicht aller Pakete angezeigt. Sie wird normalerweise chronologisch und automatisch fortlaufend sowie farblich hinterlegt dargestellt. In der Standardeinstellung wird eine fortlaufende Nummer, ein Zeitstempel, Quell- und Zieladresse, Protokoll, Länge und eine Kurzinformation angezeigt. Die Darstellung kann nach belieben gefiltert, sortiert und angepasst werden. Neben der allgemeinen Einstellung zu den anzuzeigenden Spalten, welche über das globale Einstellungsmenü gemacht werden, öffnet der Klick auf einen Spaltenkopf ein Kontextmenü, das es unter anderem erlaubt, die Spalte zu editieren bzw. konfigurieren. Beispiele hierzu an geeigneter Stelle im weiteren Verlauf.

Paketdetails

In den Paketdetails bereitet Wireshark das jeweils ausgewählte Paket unter Verwendung sogenannter Dissektoren (formale Beschreibung der Protokolle) menschenlesbar auf. Die Darstellung orientiert sich an den Schichten, die innerhalb des Paketes übereinanderliegen. Erweitert man den Eintrag zur jeweiligen Schicht (z.B. Internet Protocol), so findet man dort die Bestandteile des jeweiligen Headers (z.B. Quell- und Zieladresse) vor. Die Ansicht der Paketdetails kann durch einen Doppelklick auf ein bestimmtes Paket in einem eigenen Fenster geöffnet werden.

Paket Bytes

In der dritten Ansicht werden die Bytes des Pakets in üblicher Hexadezimal- und ASCII-Darstellung abgebildet. Wählt man ein Element in den Paketdetails aus, werden die entsprechenden Bytes markiert. Dies funktioniert auch umgekehrt bei Auswahl bestimmter Bytes.

Menüleiste

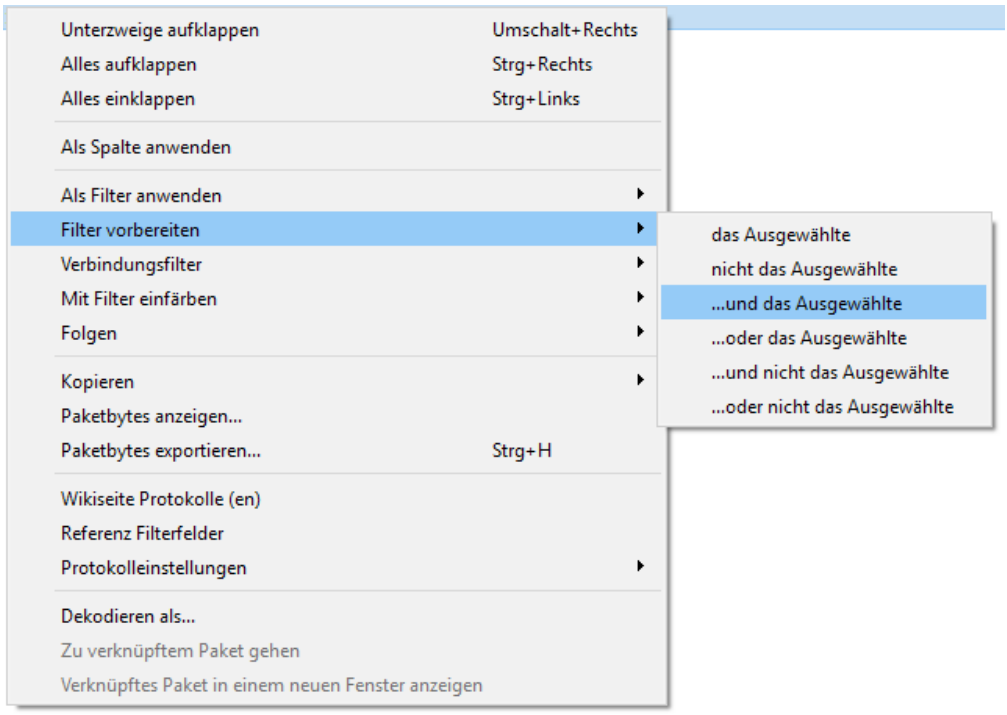
Die Menüleiste bietet Zugriff auf alle Funktionen von Wireshark. Viele Menüeinträge sind selbsterklärend. Auf interessantere Menüelemente wird im Verlauf dieser Unterlagen noch weiter eingegangen.

Werkzeugleiste

In der Werkzeugleiste befinden sich Bedienelemente zum Handling des aktuellen Mitschnitts und der Mitschnittdatei, sowie zur Navigation und Darstellung der Paketliste.
Mit dem Anzeigefilter kann bestimmt werden, welche der mitgeschnittenen Pakete tatsächlich angezeigt werden. Auf die genaue Funktion dieses Filters wird im Verlauf dieser Unterlagen noch weiter eingegangen. Eine wichtige Rolle spielt hierbei das Kontextmenü.

Kontextmenü

Das Kontextmenü bietet abhängig vom ausgewählten Element verschiedene Auswahlmöglichkeiten. Ein wichtiger Abschnitt ist der zur Auswahl von Darstellungsfiltern. Damit lassen sich anhand des gewählten Elements sehr einfach Filterausdrücke erstellen.



Kontextmenü

Grundlagen

Um besser verstehen zu können, was die Angaben in den eben beschriebenen Abschnitten des Mitschnittfensters aussagen und wie sie zu interpretieren und zu verwenden sind, werden solide Grundkenntnisse über Computernetzwerke benötigt. Dieser Abschnitt soll dazu dienen Bekanntes aufzufrischen und Wissenslücken zu schließen.

Netzwerkmodelle

Um die Zusammenhänge bei der netzwerkbasierten Kommunikation verschiedener Applikationen und Netzwerkknoten besser verstehen und darstellen zu können, bedient man sich verschiedener Modelle. Diese Modelle gliedern die Kommunikation meist in mehrere Schichten.

ISO OSI-Modell

Ein bekanntes Modell, das häufig zitiert wird, ist das OSI-Referenzmodell[2] (Open Systems Interconnection Model), welches von der International Organization for Standardization (ISO) als Standard veröffentlicht wird. Dieses Modell ist in 7 Schichten gegliedert:

7	Anwendungsschicht	Anwendungsschicht	HTTP(S) FTP SMTP
6	Darstellungsschicht		
5	Sitzungsschichtt		
4	Transportschicht	Transportschicht	TCP, UDP
3	Vermittlungsschicht	Internetschicht	IP, ICMP Router
2	Sicherungsschicht	Netzzugangsschicht	MAC Switch
1	Bitübertragungsschicht		Repeater, Hub

ISO OSI- und TCP/IP-Modell im Vergleich mit Geräten und Protokollen

2 https://de.wikipedia.org/wiki/OSI-Modell

TCP/IP-Modell

Für die meisten Anwendungsfälle im täglichen Umgang mit Netzwerken ist dieses Modell zu komplex. Etwas einfacher in der Darstellung ist das TCP/IP-Referenzmodell[3] des DoD. Dieses weist nur 4 Schichten auf, was meist völlig ausreichend ist.

Netzzugangsschicht

Die Netzzugangsschicht ist eine Abstraktion verschiedener Techniken zur direkten Datenübertragung zwischen zwei Endpunkten. Sie umfasst die OSI-Schichten 1 und 2 und damit die MAC-Adressierung aber auch Technologien wie Ethernet oder IEEE 802.11

Internetschicht

Auf der Netzzugangsschicht setzt die Internetschicht auf, welche mit der OSI-Schicht 3 identisch ist. Sie ist für das Routing von Paketen verantwortlich und ermöglicht es, komplexe Netzwerke darzustellen. In dieser Schicht werden z.B. IP-Adressen (IPv4, IPv6) verwendet.

Transportschicht

Die Transportschicht entspricht der OSI-Schicht 4. Auf dieser Ebene sind Protokolle wie TCP und UDP anzusiedeln, welche die Kommunikation zweier Netzwerkteilnehmer miteinander regeln. Die Übermittlung dieser Kommunikation auf tiefer liegenden Ebenen bleibt dabei transparent.

Anwendungsschicht

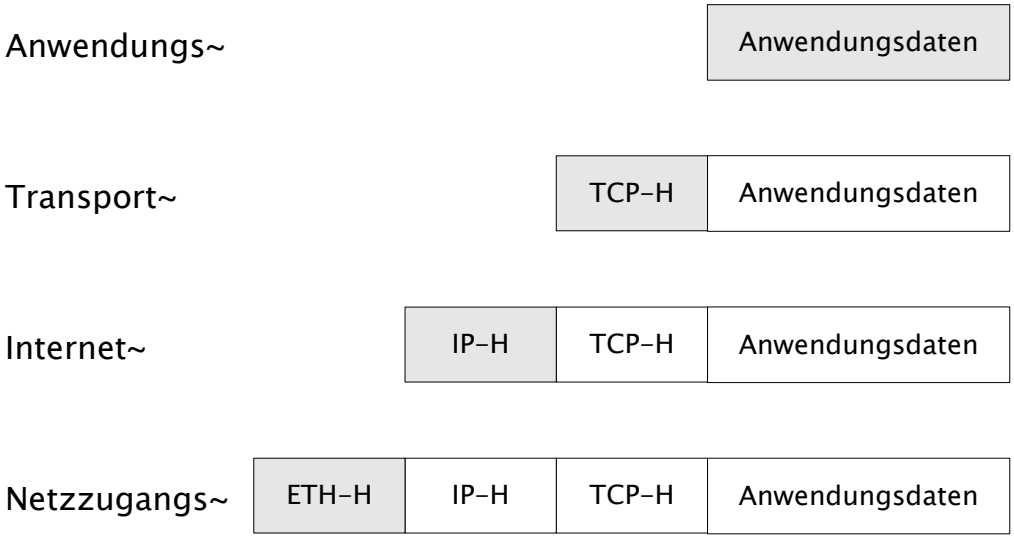
Die Anwendungsschicht des TCP/IP-Modells fasst die Schichten 5-7 des OSI-Modells zusammen. Dort sind alle Applikationsprotokolle anzusiedeln.

Header und Nutzdaten

Bei ihrem Weg durch die verschiedenen Protokollebenen werden Nutzdaten mit mehreren geschachtelten schicht- und protokollspezifischen Headern versehen. Die Header der jeweils darüberliegenden Schicht sind für die darunter befindliche

3 https://de.wikipedia.org/wiki/Internetprotokollfamilie#TCP.2FIP-Referenzmodell

Schicht transparent und werden zusammen mit den Anwendungsdaten als Nutzdaten behandelt.

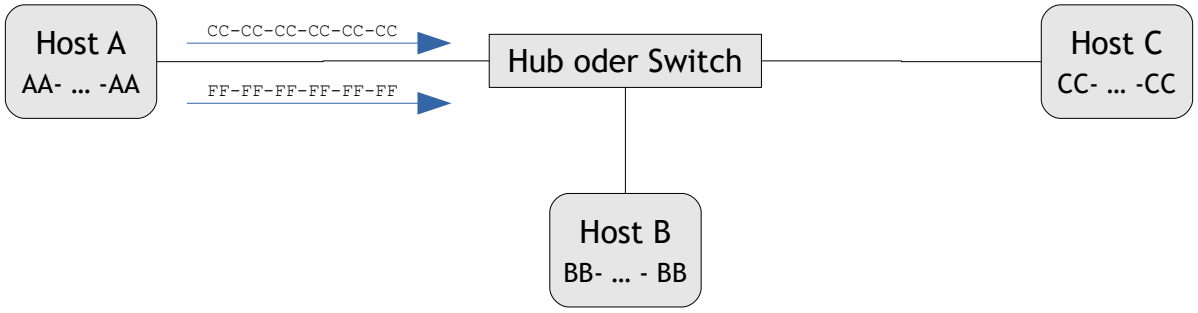


Schachtelung der Protokollebenen

Adressierung

MAC-Adressen und Switching

Auf Ebene 2 adressieren Hosts im Netzwerk den Empfänger anhand dessen MAC-Adresse. Diese ist 6 Byte lang und quasi eindeutig. Die ersten 3 Byte sind in der Regeln einem Hersteller zuordenbar. (z.B. 00-15-17-F0-0D-12 für eine Intel-Karte) Pakete mit der Adresse FF-FF-FF-FF-FF-FF werden von allen Geräten verarbeitet, denn es handelt sich dabei um die Broadcast-Adresse.



MAC-Adressierung

Ein Switch ist in der Lage anhand sogenannter Source Address Tables zu

entscheiden, an welche(n) Port ein Paket weitergeleitet werden muss. Unnötiger Netzwerkverkehr wird so reduziert.

IP-Adressen und Routing

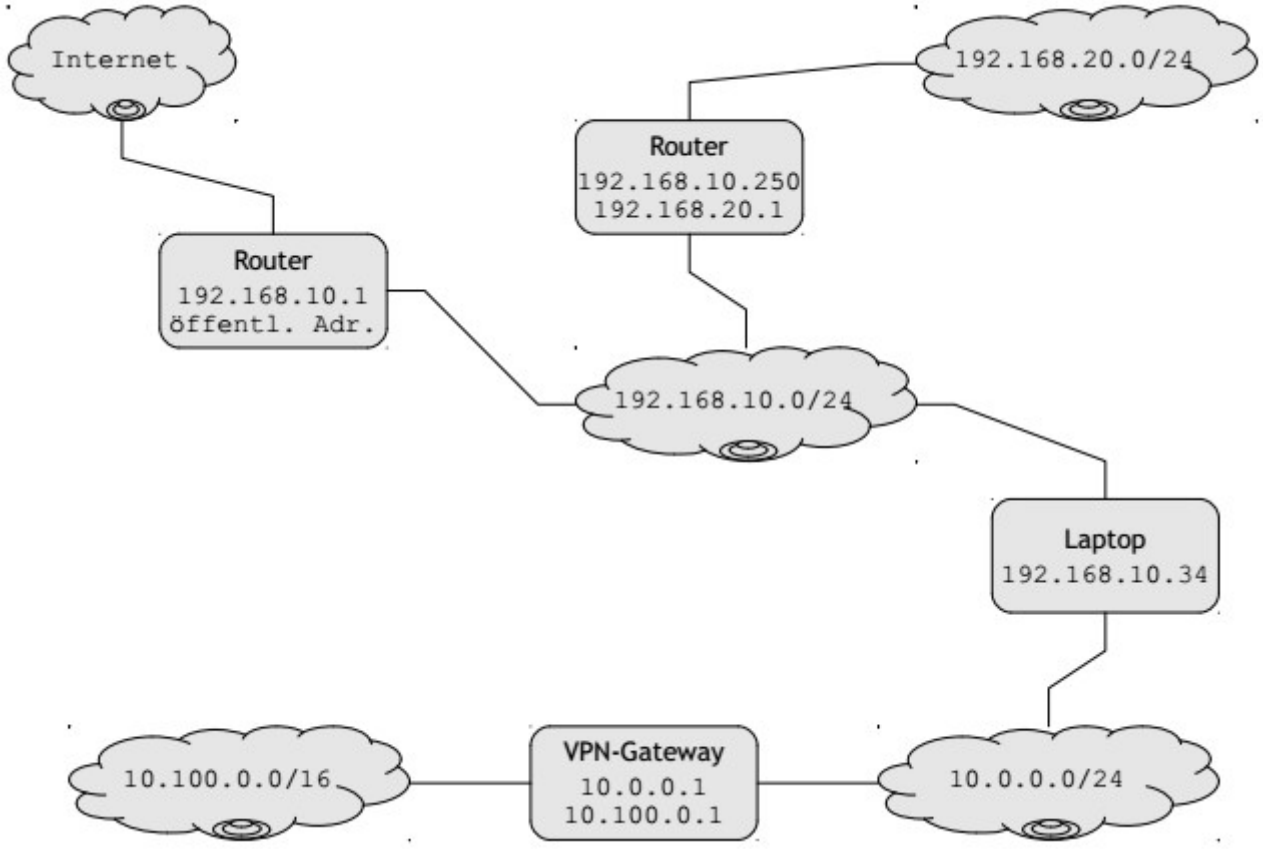
Auf Ebene 3 erfolgt die Adressierung anhand von IP-Adressen, was die Bildung von Subnetzen erlaubt und Routing-Technologie erfordert. Zur Aufteilung in Subnetze wird die Subnetzmaske verwendet (IPv6: Präfixlänge).

Netzadresse: `192.168.10.0/24` **Host:** `192.168.10.34`

192	168	10	34	IP-Adresse
1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 1 0 1 0	0 0 1 0 0 0 1 0	
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	Subnetzmaske
255	255	255	0	

Subnetzmaske

Befindet sich der Zielhost (z.B. 192.168.10.85) im gleichen Subnetz, so kann direkt dessen MAC-Adresse ermittelt werden und das Paket wird direkt zugesandt. Ist dies nicht der Fall, schlägt der versendende Host die Ziel-Adresse in seiner Routing-Tabelle nach. Wird er fündig, versendet er das Paket mit der IP-Adresse des Ziels und der MAC-Adresse des Gateways (Routers) als EmpfängerAdressen. Der Router erhält das Paket und leitet es weiter.



Netzwerkskizze

Ziel	Gateway
192.168.20.0/24	192.168.10.250
10.100.0.0/16	10.0.0.1
0.0.0.0/0	192.168.10.1

Routing-Tabelle

Ports

TCP-Datenverkehr

Die Datenübertragung via TCP erfolgt verbindungsorientiert. Zu Beginn einer Übertragung findet zum Verbindungsaufbau der 3-Wege-Handshake statt. Für jedes übermittelte Datenpaket wird eine Quittung zum Absender zurückgesandt. Nicht quittierte Pakete werden erneut versandt. Bei Übertragungsende wird die

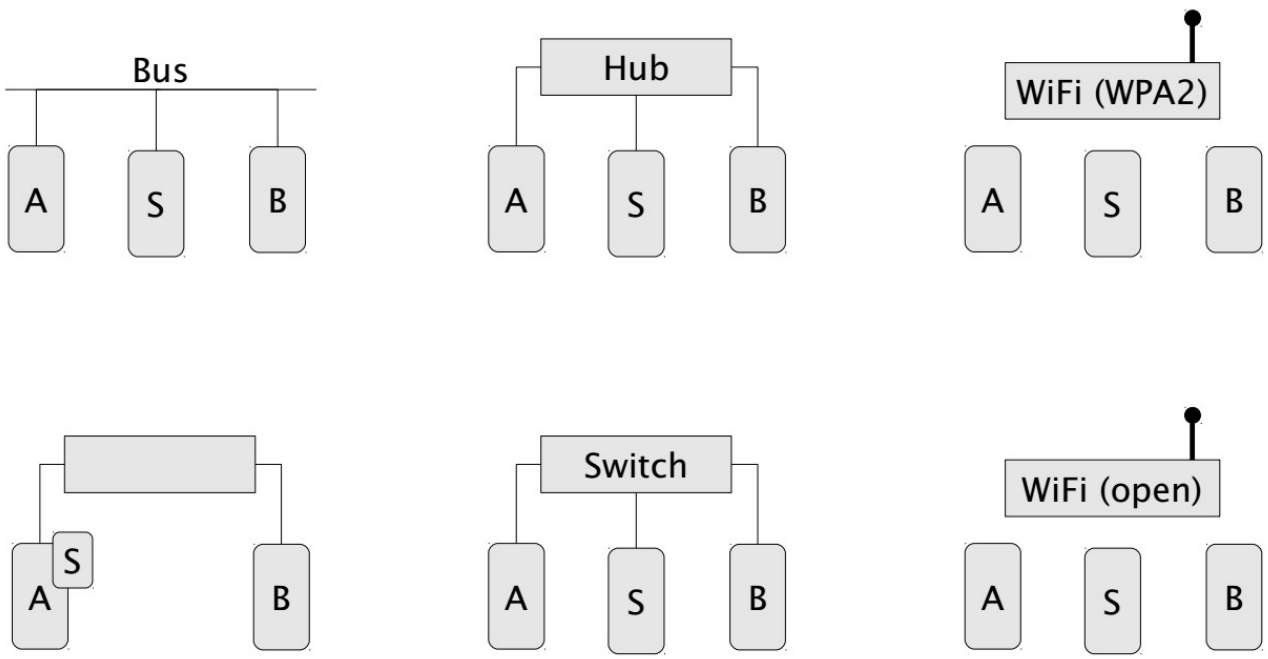
Verbindung ordnungsgemäß beendet.

UDP-Datenverkehr
Die Datenübertragung via UDP erfolgt verbindungslos. Der Empfang von Datenpaketen wird nicht quittiert. Die Pakete enthalten lediglich eine Prüfsumme.

Time To Live
Jedes IP-Paket erhält beim Absender einen Time-To-Live-Wert (TTL), typischerweise 64 oder 128. Erreicht ein Paket einen Router und wird dort weitergereicht, so verringert der Router die TTL um eins. Auf diese Weite soll verhindert werden, dass fehlgeleitete IP-Pakete endlos im Internet kursieren.

Arbeitsweise

Von der Funktionsweise moderner Netzwerke lassen sich einige Bedingungen für die Arbeitsweise von Netzwerksniffern ableiten. Dies beginnt schon bei der Verarbeitung der am Host ankommenden Datenpakete. Abhängig von der Empfängeradresse, an die ein Paket adressiert ist, entscheidet der Host, ob das Paket weiter verarbeitet oder verworfen werden soll.



Sniffer im Netzwerk

Diese Entscheidung wird zwar auf verschiedenen Ebenen mehrfach gestellt, ist aber auf der untersten Ebene besonders entscheidend. Damit die Netzwerkkarte alle Pakete akzeptiert und weiterreicht, die sie empfängt, muss sie in den sogenannten Promiscuous Mode versetzt werden.
Weitere wichtige Aspekte sind die verwendete Netzwerktechnologie und -topologie und die Positionierung des Sniffers im Netzwerk (s.o.).

Mitschnitte gezielt anfertigen

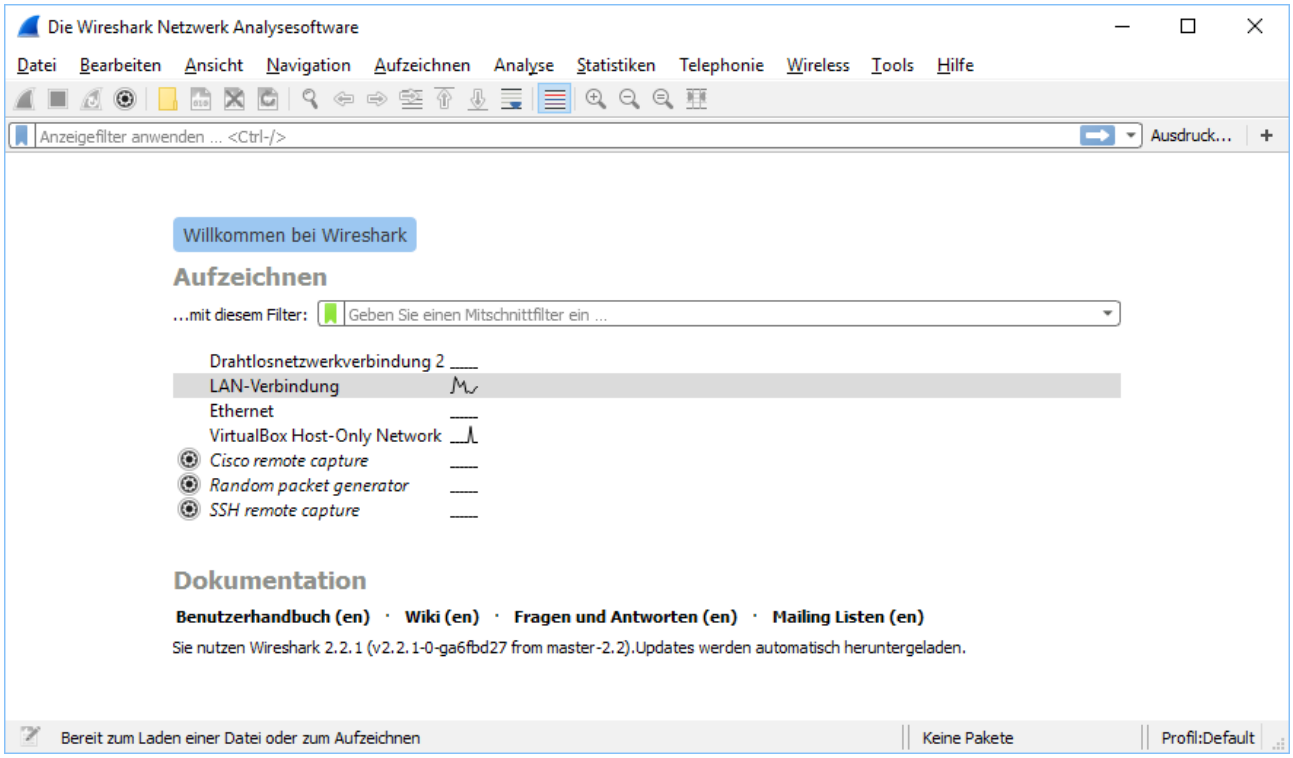
Das Mitschneiden von Netzwerkverkehr erfordert erweiterte Rechte im Betriebssystem. Startet man Wireshark unter Linux als Nutzer root, so wird man mit einer Warnmeldung konfrontiert und manche Erweiterungen werden aus Sicherheitsgründen nicht ausgeführt. Die empfohlene Vorgehensweise besteht deshalb darin, bei der Installation von Wirehsark darauf zu achten, dass man die Option wählt, die es auch anderen Nutzern im System erlaubt, Netzwerkmitschnitte anzufertigen. Anschließend muss der betreffende Nutzer nur der passenden Gruppe (normalerweise „wireshark“) hinzugefügt werden. Dann kann er nach dem nächsten Anmelden Wireshark verwenden.

Startbildschirm

Mit dem Sprung auf die Hauptversion 2 wurde die Startansicht von Wireshark grundlegend überarbeitet. Sie zeigt eine Historie zuletzt geöffneter Mitschnittdateien, ein Schnelleingabefeld für Aufzeichnungsfilter sowie die verfügbaren Aufzeichnungskanäle an. Dazu gehören nicht nur Netzwerk-Interfaces sondern auch USB-Interfaces und weitere Methoden wie z.B. das Mitschneiden auf einem entfernten Host via SSH. Schließt man einen geöffneten Mitschnitt, gelangt man vom Hauptfenster wieder in diese Ansicht zurück.

Zum schnellen und einfachen Start des Sniffing-Vorgangs genügt ein Doppelklick auf das entsprechende Interface. Alternativ kann eine Mitschnittdatei von einem Speichermedium gewählt werden. Wird diese Option gewählt, stehen im Dateidialog noch einige Einstellungen zur Verfügung, z.B. analog zur Funktion des Capture-Filters ein Read-Filter[4] und Einstellungen zur Namensauflösung. Ebenso werden einige Metadaten zur gewählten Mitschnittdatei angezeigt.

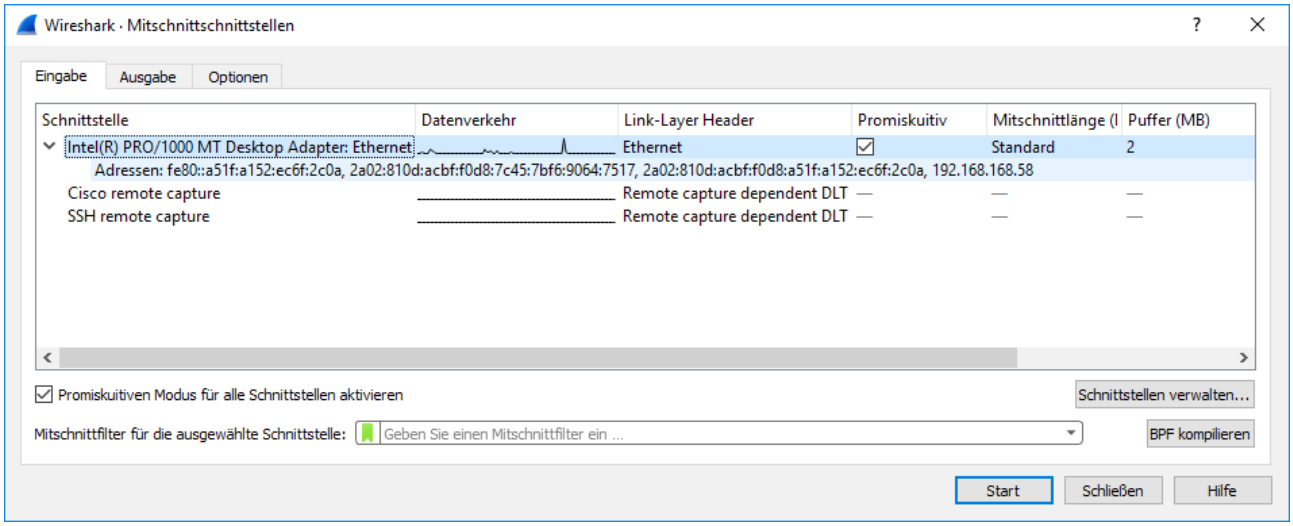
4 Achtung: Die Syntax entspricht dem Display-Filter. Details werden später behandelt.



Startfenster

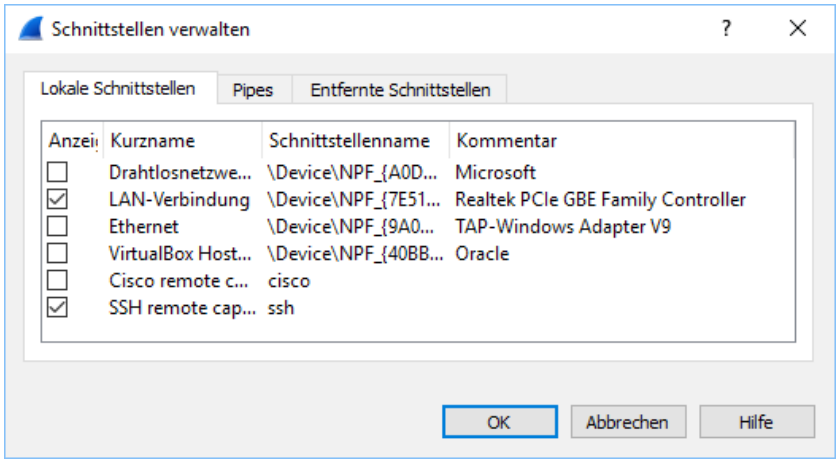
Schnittstellen

Nicht immer reicht ein einfacher Klick auf eine Schnittstelle aus und man benötigt detailliertere Einstellungen. Aus dem Menü „Aufzeichnen“ oder über das Zahnradsymbol in der Werkzeugleiste lässt sich das Dialogfenster für die Mitschnittschnittstellen öffnen.



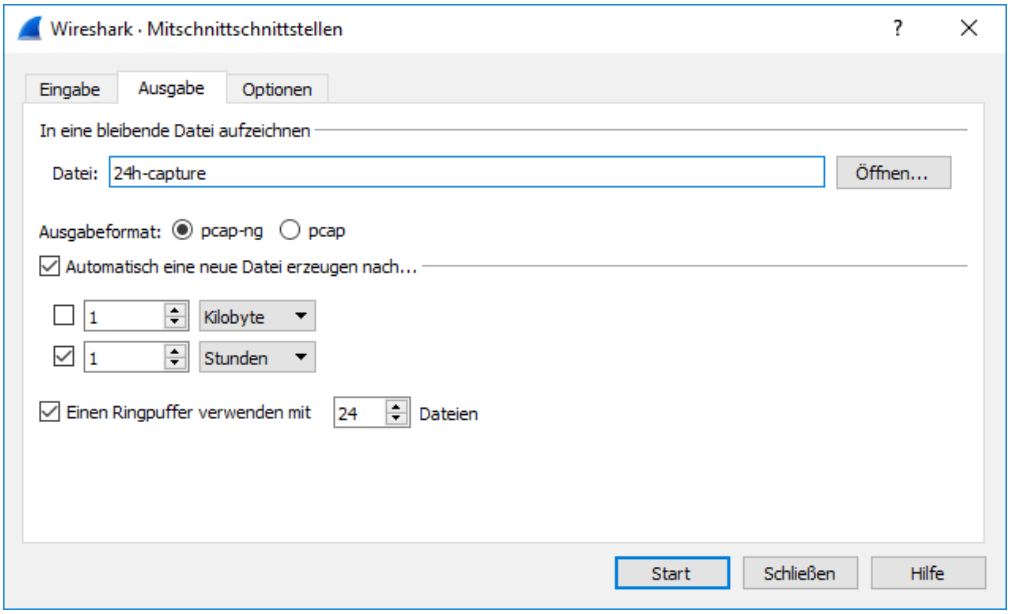
Mitschnittschnittstellen

In diesem Fenster werden alle verfügbaren Schnittstellen angezeigt. Ein Klick auf das Pfeilsymbol neben einer Schnittstelle zeigt die dort konfigurierten Adressen. Dies hilft besonders bei einer größeren Anzahl an Schnittstellen den Überblick zu behalten. Neben der Auswahl der zu verwendenden Schnittstelle, grundlegenden Informationen zu dieser sowie der Eingabe oder Auswahl eines Mitschnittfilters kann im Reiter „Eingabe“ auch die Schnittstellenverwaltung geöffnet werden. Damit lassen sich lokale Schnittstellen, Pipes und entfernte Schnittstellen verwalten. Jedoch ist zu beachten, dass nicht jede Funktionalität für jede Plattform implementiert ist.
Bei einer großen Anzahl lokaler Schnittstellen, wie sie z.B. von VPN-Software oder Virtualisierungslösungen angelegt werden, kann es aus Gründen der Übersichtlichkeit hilfreich sein, solche Schnittstellen auszublenden, solange sie nicht benötigt werden.



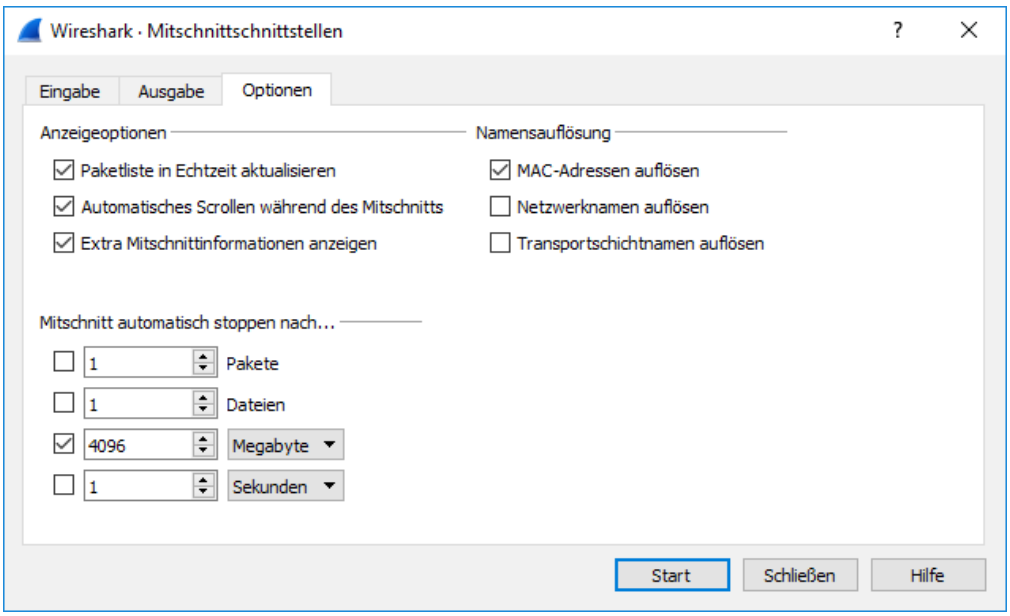
Lokale Schnittstellen verwalten

Im Reiter „Ausgabe“ kann neben dem Ausgabeformat und dem Speicherort für die Ausgabedateien auch eine Regel für den Wechsel der Ausgabedatei festgelegt werden. Abhängig von der Größe oder der Dauer des Mitschnittes, legt Wireshark weitere Mitschnittdateien an, wenn das vorgegebene Limit für die aktuelle Ausgabedatei erreicht ist. Es besteht auch die Möglichkeit einen Ringpuffer zu verwenden, z.B. um einen bestimmten Zeitraum in der Vergangenheit kontinuierlich zu überwachen, etwa die letzten 24 Stunden aufgeteilt in Mitschnitte zu je einer Stunde. Ist die maximale Anzahl der Pufferdateien erreicht, löscht Wireshark die jeweils älteste, sobald eine neuere angelegt werden muss. Wählt der Nutzer sowohl ein Zeit- als auch ein Größenlimit, dann findet der Wechsel statt, sobald das erste der beiden Limits erreicht ist.



Ausgabeoptionen für den Mitschnitt

Der Reiter „Optionen“ bietet neben Anzeigeoptionen und der Namensauflösung für MAC-Adressen, IP-Adressen und Portnamen auch Eingabefelder für eine Abbruchbedingung, bei deren Erreichen der Mitschnitt angehalten werden soll.



Weitere Optionen für den Mitschnitt

Filter

Wireshark verfügt über zwei verschiedene Filtertypen:

- Display-Filter
- Capture-Filter

Display-Filter

Der Display-Filter ist dazu gemacht um die Auswahl der angezeigten Pakete einzuschränken und uninteressante Pakete auszublenden. Letztere werden trotzdem aufgezeichnet, verbrauchen also auch Speicherkapazität und Rechenleistung bei der Verarbeitung. Bei großen Mitschnitten kann die Anwendung eines Display-Filters einige Zeit in Anspruch nehmen.

Capture-Filter

Anders als der Display-Filter, entscheidet der Capture-Filter bereits bei der Aufzeichnung der Pakete, welche aufgezeichnet und welche verworfen werden. Das heißt, er kann nicht einfach bei Bedarf wie der Display-Filter abgewählt werden. Was aufgrund von Filterung nicht mitgeschnitten wurde, ist endgültig verloren. Trotzdem hat der Capture-Filter seine Berechtigung. Er ist vor allem dann notwendig, wenn über einen längeren Zeitraum oder an einem sehr stark frequentierten Netzwerkknoten mitgeschnitten wird. Nur so bleibt das Datenvolumen des Mitschnittes bewältigbar.

Beispiele für gezielte Mitschnitte und Übungen

Führen Sie nun nach Anweisung Ihres Trainers Übungen zum Mitschneiden bei Ping, DNS-Abfragen, HTTP- und HTTPS-Verkehr sowie einem reinen TCP-Verbindungsaufbau mit Putty oder Netcat durch.
Beobachten Sie dabei

- welcher Netzwerkverkehr im Zusammenhang mit den jeweiligen Aufrufen auftritt.
- wie die Ping-Pakete richtig zugeordnet werden können.
- welcher Netzwerkverkehr ggf. nach dem Abgeschlossenen Ladevorgang im Zusammenhang mit der geöffnetet Seite im Hintergrund noch stattfindet.
- was ggf. auch beim Aufruf einer Webseite mittels HTTPS für Sie im Mitschnitt zu sehen ist.

Details zu den Protokollebenen

Details Ethernet

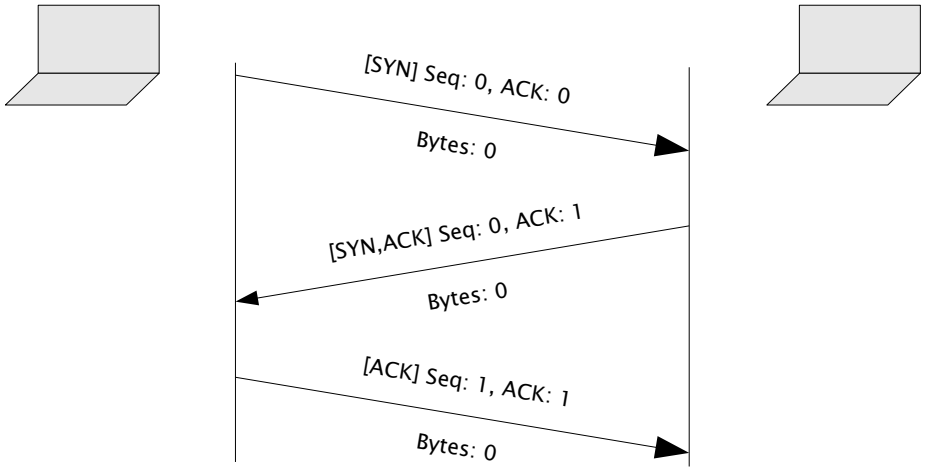
Den Angaben in den Paketdetails kann man im Abschnitt Ethernet die Quelladresse, die Zieladresse und den Typ der enthaltenen Nutzdaten entnehmen. Den Adressen wird wenn möglich anhand der ersten 3 Byte ein Hersteller zugeordnet und die Bits für globally unique/locally administered und unicast/multicast werden ausgewertet.
Falls vorhanden, folgt direkt darunter auch der IEEE 802.1-VLAN-Tag. Wireshark stellt diese Information in einem eigenen Abschnitt dar.

Details IP

Der Dissektion des IP-Headers können neben der IP-Version und der Quell- und Zieladresse auch Längenangaben zu Header und Inhalt entnommen werden, sowie einige Flags und die IP-ID. Außerdem ist hier ebenfalls das auf der nächsten Schicht verwendete Protokoll angegeben (z.B. TCP oder UDP) und die TTL des Pakets. Wireshark versucht zusätzlich weitere Informationen zu den Feldern zu ermitteln, z.B. den geografischen Standort der Hosts.

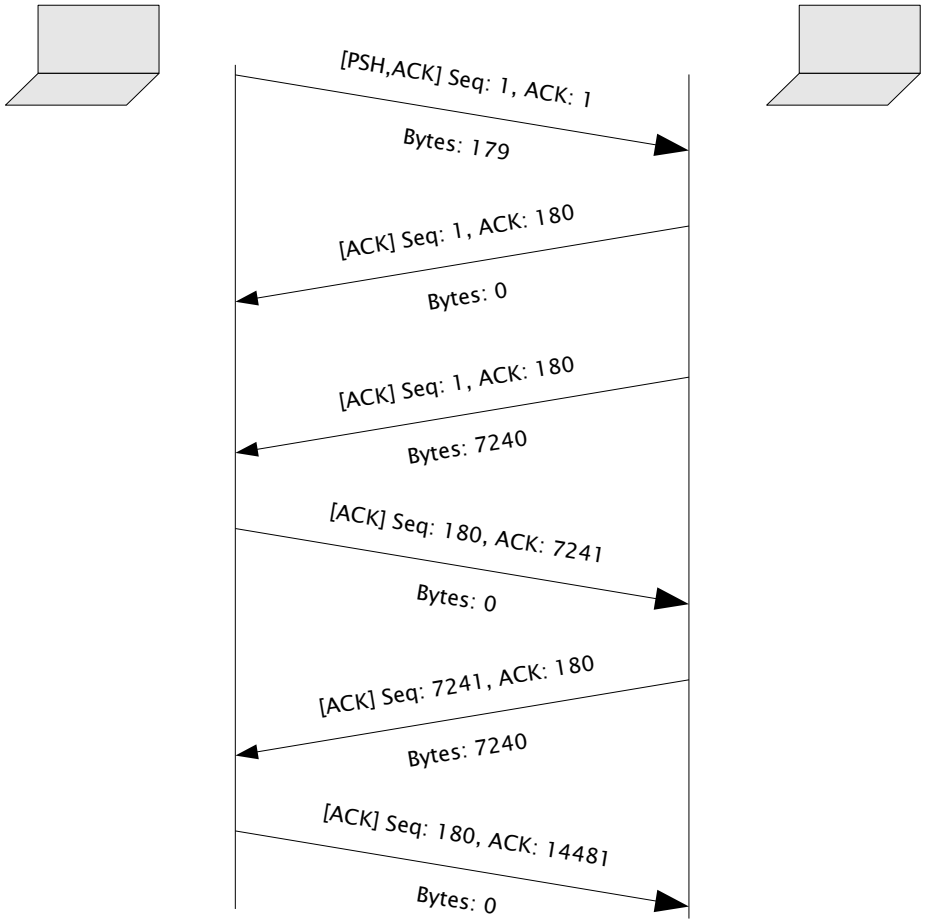
Details TCP

Der Abschnitt für den TCP-Header eines Pakets liefert neben Quell- und Zielport noch weitere Informationen wie Längenangaben, Nummerierungen zur Ablaufkontrolle, Flags, eine Prüfsumme und weitere Optionen wie z.B. Zeitangaben. Wireshark zeigt zudem an, zu welchem TCP-Stream er diese Konversation zählt. Besonders hilfreich ist die Aufbereitung dieser Informationen, die Wireshark vornimmt. Sequenznummer und ACK-Nummer, welche aus Sicherheitsgründen mit einem zufälligen Offset gewählt sein müssen, werden von Wireshark zur besseren Lesbarkeit normalisiert.



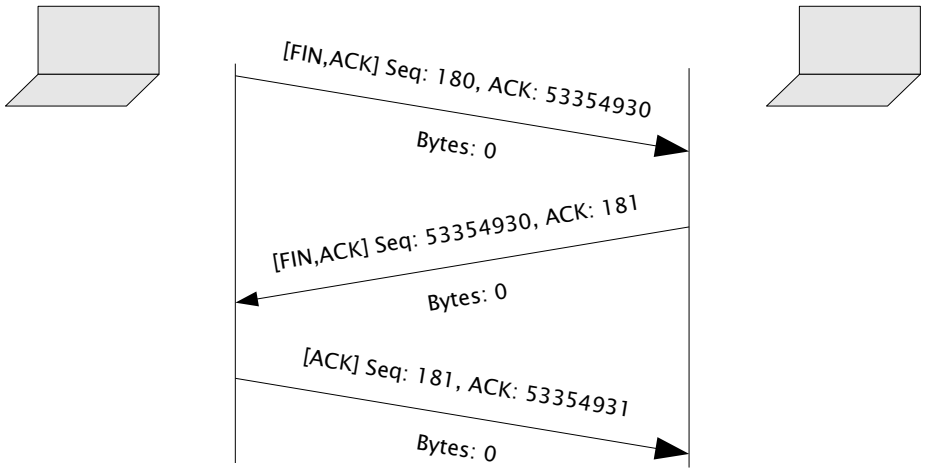
3-Wege-Handshake

Nach erfolgreichem Verbindungsaufbau (sog. 3-Wege-Handshake) Erfolgt die Datenübertragung, jeweils quittiert mit ACK-Paketen. Sequenz- und ACK-Nummer helfen die Pakete in die richtige Reihenfolge zu bringen. Währenddessen werden die Nummern entsprechend der übertragenen Bytes weitergezählt.
Bleiben erwartete Pakete zu lange aus, wird das vorangegangene Paket wiederholt. Wireshark kennzeichnet dies als Wiederholung. In der Auswertung von Sequenznummer und ACK-Nummer verlinkt Wireshark zur einfacheren Handhabung auf das entsprechende Paket und wertet die Laufzeiten (RTT) aus.



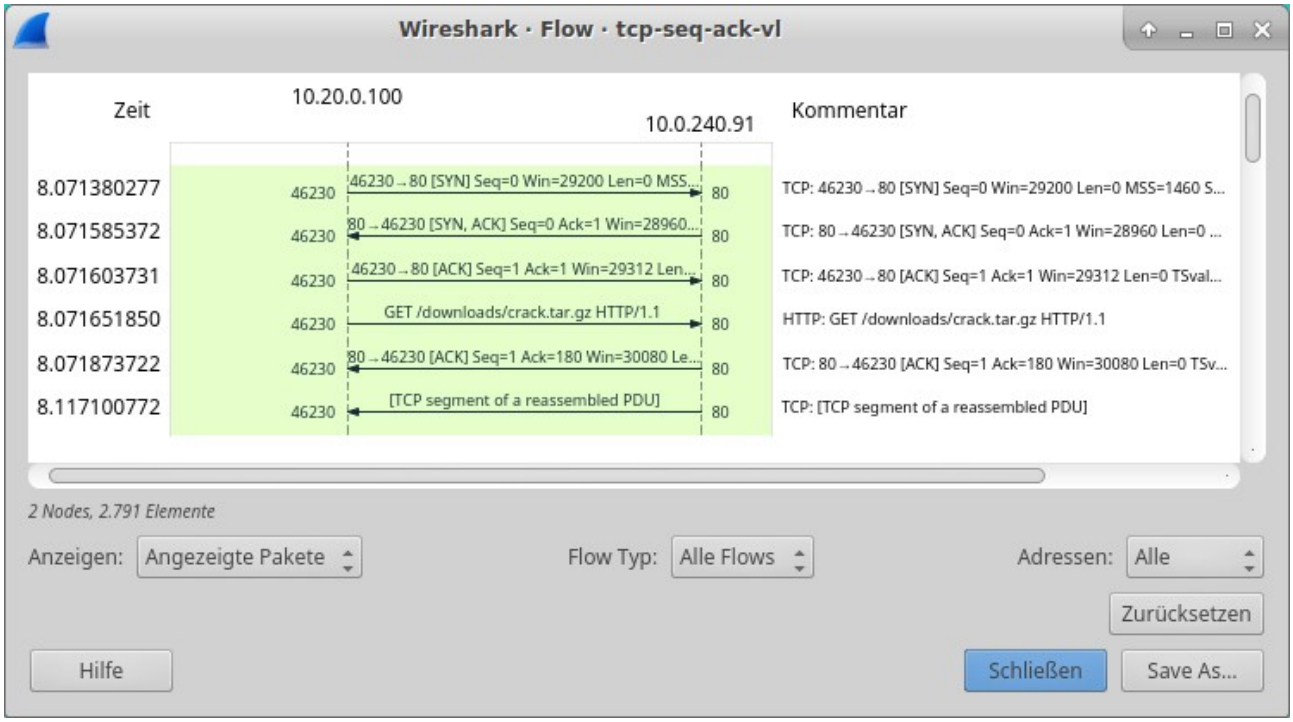
TCP-Sequenz- und ACK-Nummern

Nach Beendigung der Datenübertragung wird die Verbindung ähnlich dem 3-Wege-Handshake auch wieder geordnet abgebaut.



TCP-Verbindungsabbau

Im Menü Statistik kann man sich eine ensprechende Auswertung mit Hilfe des Menüpunktes „Flow Graph“ anzeigen lassen.



Flow Graph

Zeitangaben in Wireshark

Ein wichtiger Aspekt bei der Analyse von Netzwerkverkehr ist die Zeit. Dabei gibt es verschiedene Messwerte, die man betrachten kann. Ein grundlegendes Maß ist die Round Trip Time (RTT), also die Zeit, die benötigt wird um ein Paket von einem Host zum Anderen zu schicken und ein Antwortpaket zurück. Hierfür werden meist die ICMP-Pakettypen Echo Request und Echo Reply (ping) verwendet.
Ein weiteres Maß für die Zeit kann die Service Response Time (SRT) sein. Dies ist die Zeit, die ein bestimmter Netzwerkdienst braucht um auf die Anfrage eines Clients zu antworten. Hier fließt neben der reinen Übertragungszeit auch die Rechenzeit auf dem Server mit ein. Wireshark bietet zur Auswertung der SRT im Menü Statistiken den Eintrag „Service Antwortzeit“.

Um das Zeitverhalten im Netzwerk im Bezug auf bestimmte Pakete zu betrachten, kann in der Paketliste über das Kontextmenü eine Zeitreferenz auf ein bestimmtes Paket gesetzt werden. In der Spalte für die verstrichene Zeit werden dann die

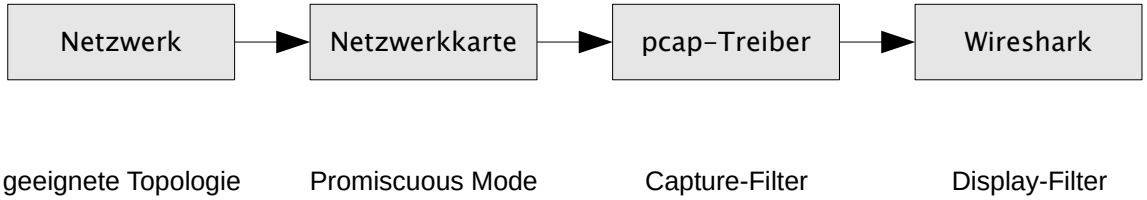
Zeiten für alle folgenden Pakete in Bezug auf das markierte Paket angegeben.

Datenverkehr im Hintergrund

Neben dem Verkehr, der offensichtlich durch Nutzerinteraktion ausgelöst wird, lässt sich mit Wireshark auch beobachten, welcher Informationsaustausch noch auf dem Netzwerk erfolgt. Da gibt es zum einen den Verkehr, der in Begleitung der Nutzerinteraktion entsteht, wie z.B. ARP- und DNS-Auflösung. Weiter kann auch Verkehr beobachtet werden, den Dienste und Programme sowie das Betriebssystem selbst verursacht. Und schließlich zeigt Wireshark auch Verkehr an, der nicht zu direkt an den Host gerichteter Kommunikation gehört, wie z.B. Broad- und Multicasts.

Filter im Detail

Wie bereits angesprochen, wirken die beiden Filter in Wireshark an unterschiedlichen Stellen. Das nachfolgende Bild soll das Zusammenwirken der einzelnen Komponenten verdeutlichen:



Voraussetzungen für die Erfassung von und Filterung von Paketen

Der Display-Filter

Ein Display-Filter[5] wird im dafür vorgesehenen Eingabefeld in Form von logischen Ausdrücken formuliert. Es stehen hierfür verschiedene Operatoren zur Verfügung um Vergleiche anzustellen und Verknüpfungen zu bilden. Die grundlegende Syntax ist:

```
[Negation] Ausdruck [ Verknüpfungsoperator [Negation ] Ausdruck ]
```

Ein Ausdruck selbst besteht dabei immer aus einer linken und einer rechten Seite , die mit einem Operator verknüpft sind, z.B.

```
ip.addr == 10.0.0.4
```

Die Vergleichsoperatoren sind:

Operator	Alternative	Bedeutung
==	eq	gleich
!=	ne	ungleich
>	gt	größer als
<	lt	kleiner als
>=	ge	größer oder gleich
<=	le	kleiner oder gleich
contains		Feld beinhaltet Wert

5 vgl. https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

matches		Feld entspricht Muster[6]
		Feld ist vorhanden

Um Ausdrücke zu verknüpfen oder zu verändern, stehen logische Operatoren zur Verfügung. Komplexe Ausdrücke können geklammert werden.

Operator	Alternative	Bedeutung
&&	and	und
||	or	oder
!	not	nicht
[...]		Teilbereichsoperator (s.u.)
in		Inhaltsoperator (s.u.)

Der Teilbereichsoperator kann in verschiedenen Schreibweisen verwendet werden:

Syntax	Beispiel	Erläuterung
elem[m:n]	udp[10:4] == „SEAR“	vom gewählten Element Offset m, Länge n
elem[m-n]	ip[12-14] == c0:a8:a8	Offset m bis n
elem[:n]	eth.dst[:3] == c8:0e:14	vom Anfang des Elements Länge n
elem[m:]	icmp[8:] contains „abcd“	von Offset m bis Ende des Pakets
elem[m]	icmp[0] == 8	ein bestimmtes Offset-Byte

Die Bereichsangaben können auch kombiniert werden:

```
dns[2-3;17:6] == 01:00:67:6f:6f:67:6c:65
```

Der Inhaltsoperator kann dazu dienen, logische Verknüpfungen verkürzt zu schreiben:

```
tcp.port in {80 443 8080}
```
oder
```
tcp.port == 80 || tcp.port == 443 || tcp.port == 8080
```

Klammerung von Ausdrücken kann die Bedeutung der logischen Verknüpfungen

6 vgl. http://perldoc.perl.org/perlre.html

verändern:

```
(ip.addr == 10.0.0.1 && tcp.dstport == 80) || ip.addr == 10.0.0.55
```

oder

```
ip.addr == 10.0.0.1 && (tcp.dstport == 80 || ip.addr == 10.0.0.55)
```

Caveats

Nicht jeder Operator und Selektor kann an mit jedem Element verwendet werden. Zudem bietet die Verwendung von logischen Verknüpfungen nicht eindeutiger Feldangaben Potenzial für Fehler. Ein Beispiel soll dies verdeutlichen:

Filterausdrücke:

`!(ip.addr == 10.0.0.1)` Fehlen von Gleichheit

oder

`ip.addr != 10.0.0.1` Zutreffen von Ungleichheit

Pakete:

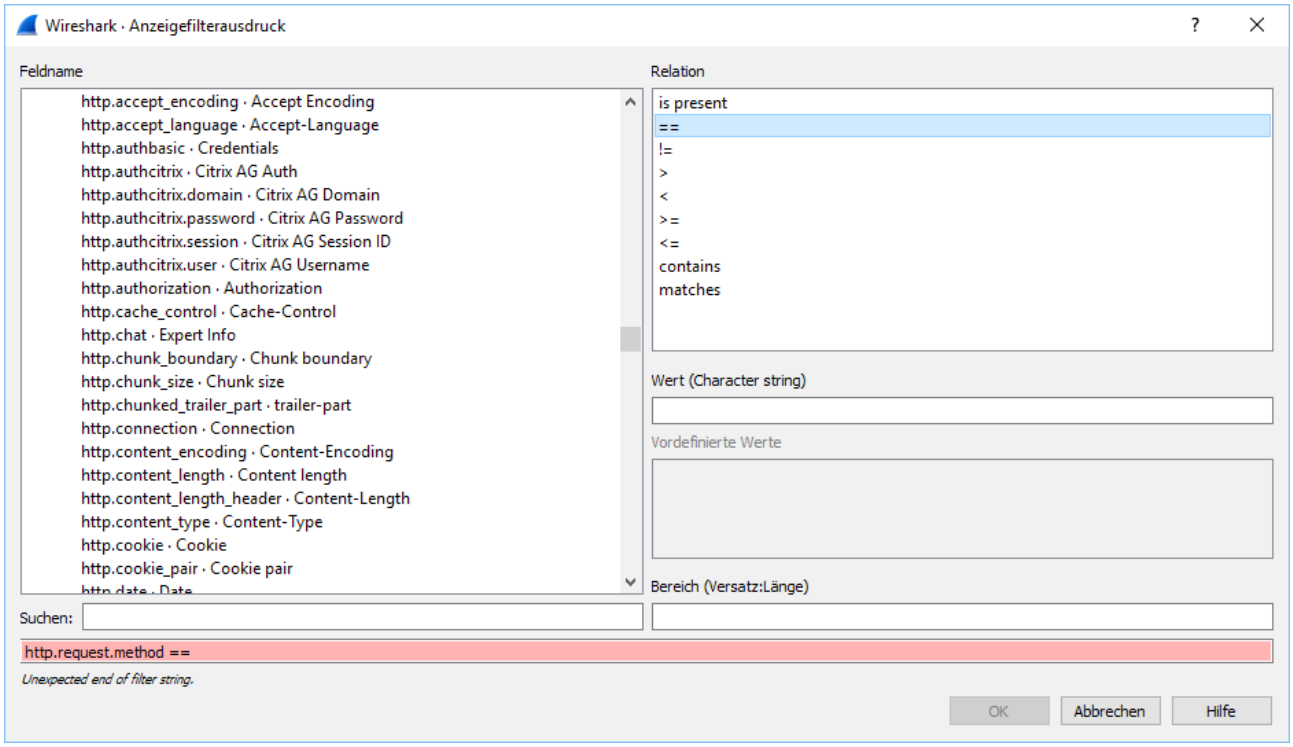
Quelle	Quellport	Ziel	Zielport
10.0.0.55	50000	10.0.0.1	80
10.0.0.1	80	10.0.0.55	80
10.0.0.55	50001	10.0.0.2	25
10.0.0.2	25	10.0.0.55	50001

Die Formulierung der Filterausdrücke muss nicht auswendig aus dem Kopf erfolgen. Wireshark unterstützt den Nutzer dabei. Während der Eingabe bietet Wireshark Autovervollständigungsvorschläge an, so dass der Nutzer nur den gewünschten Ausdruck auszuwählen braucht. Falsche oder korrekte Syntax wird rot oder grün signalisiert.

Ebenfalls sehr bequem lässt sich ein Filter erstellen oder ergänzen, wenn ein passendes Paket zur Verfügung steht. Dann kann der Nutzer in den Paketdetails das Kontextmenü des gewünschten Elements aufrufen und aus verschiedenen Optionen wählen. Er kann einen Filter direkt anwenden oder nur vorbereiten, also ins Eingabefeld schreiben lassen ohne ihn anzuwenden.

Weiter kann er wählen, ob das betreffende Element alleine, und-verknüpft oder oder-verknüpft angegeben werden soll und ob es ein Positiv- oder Negativ-Filter sein soll.

Ist auch das nicht ausreichend, öffnet ein Klick auf die Schaltfläche „Ausdruck“ ein Dialogfenster. Dort kann aus allen Dissektoren das betreffende Feld und die gewünschte Relation gewählt werden.



Dialog Anzeigefilter

Das Eingabefeld für den Anzeigefilter stellt per Dropdown-Auswahl eine Liste der zuletzt verwendeten Filterausdrücke zur Verfügung. Häufig benötigte Filterausdrücke können unter Verwendung der Plus-Schaltfläche abgespeichert werden. Sie erscheinen dann als Schaltfläche neben dem Eingabefeld. Sie lassen sich im zentralen Einstellungsmenü verwalten.

Beim Öffnen einer Mitschnittdatei gibt es eine kleine Besonderheit zu beachten. Dort kann ein Filterausdruck (Read-Filter) angegeben werden, der sich auswirkt wie ein Capture-Filter (d.h. ausgefilterte Pakete werden nicht mit geladen), jedoch die Filter-Syntax des Display-Filters verwendet.

Beispiele

```
eth.addr == f4:6d:04:66:7c:47
```

Zeigt Pakete, bei denen die Quell- oder Ziel-MAC-Adresse der angegebenen entspicht.

```
eth.addr[0:3] == 00:06:5b
```

Zeigt Pakete, bei denen die Quell- oder Ziel-MAC-Adresse die Vendor-ID von Dell aufweist, d.h. bei der die ersten drei Bytes 00:06:5b lauten.

```
eth.type == 0x0800
eth.type == 0x86dd
```

Zeigt Pakete, bei denen der im Ethernet-Header angegebene Inhaltstyp IPv4- bzw. IPv6-Verkehr ist.

```
ipv6
```

Zeigt Pakete bei denen ein IPv6-Header erkannt wurde.

```
ip.dst == 192.168.1.20
```

Zeigt Pakete, bei denen die Ziel-IP 192.168.1.20 lautet.

```
!(ip.addr == 10.0.0.15)
```

Zeigt Pakete, bei denen weder die Quell- noch die Zieladresse 10.0.0.15 lautet.

```
ip.len <= 48
```

Zeigt Pakete, bei denen das Längenfeld im IP-Header kleiner oder gleich 48 angibt, also die Gesamtlänge von IP-Header und IP-Nutzdaten kleiner oder gleich ist.

```
ip.ttl <= 128 && ip.ttl > 126
```

Zeit Pakete von Hosts, die nicht weiter als 2 Hops entfernt sind und vermutlich ein Windows-Betriebssystem nutzen.

```
(ip.ttl <= 64 && ip.ttl > 62) || (ip.ttl <= 255 && ip.ttl > 253)
```

Zeigt Pakete von Hosts, die nicht weiter als 2 Hops entfernt sind und vermutlich kein Windows-Betriebssystem nutzen.

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

Zeigt Pakete, die vermutlich von oder an einen SMTP-Server übertragen wurden.

```
udp[8:3] == 33:01:00
```

Zeigt UDP-Pakete, bei denen die ersten 3 Byte Nutzdaten 0x330100 lauten.

```
udp.dstport == 53
```

Zeigt UDP-Pakete, die an Port 53, vermutlich also an einen DNS-Server gerichtet sind.

```
tcp[13] & 0x04
```

Zeigt Pakete, bei denen das RST-Bit (0x4) gesetzt ist.

```
tcp[13] & 0x10 && tcp[13] & 0x02
tcp[13] & 16 && tcp[13] & 2
```

Zeigt Pakete, bei denen das SYN- und das ACK-Bit gesetzt sind (0x2 und 0x10). Beide Ausdrücke sind gleichwertig.

```
http contains "login" && http contains "admin"
```

Zeigt Pakete, bei denen im HTTP-Anteil die Zeichenfolgen „login“ und „admin“ vorkommen.

```
smtp
```

Zeigt SMTP-Pakete

```
udp && !dns
```

Zeigt alle UDP-Pakete außer den DNS-Paketen.

```
bootp
```

Zeigt DHCP-Pakete.

```
http.request.uri.query.parameter
```

Zeigt HTTP-Pakete, bei denen Requestparameter in der URI enthalten sind.

```
http.request.uri.query.parameter matches "ims="
```

Zeigt HTTP-Pakete, bei denen in den Requestparametern die Zeichenfolge „ims=“

Übungen

Vertiefen Sie Ihr Wissen zu Display-Filtern durch die praktischen Übungen, zu denen Ihr Trainer Sie anleiten wird.

Der Capture-Filter

Die Syntax des Capture-Filters[7] leitet sich aus der libpcap-Bibliothek[8] ab. Man begegnet ihr z.B. auch auf der Kommandozeile bei tcpdump. Sie ist weniger mächtig als die Syntax des Display-Filters.

Ein Filterausdruck entspricht immer der Form

```
[not] primitive [and|or [not] primitive …]
```

wobei ein Primitive eine Kombination aus einem Wert (z.B. Name oder numerischer Wert) mit einem oder mehreren vorangestellten Qualifiern ist. Es gibt drei verschiedene Typen von Qualifiern:

- type (Typ, z.B. host, net, port)
- dir (Direction, Richtung, z.B. src, dst)
- proto (Protokoll, z.B. ether, ip, tcp, udp)

Häufig benötigte Mitschnittfilter können im Menü „Aufzeichnen“ unter dem Menüpunkt „Mitschnittfilter“ in einem Dialogfenster vorbereitet werden, so dass sie bei Beginn der Aufzeichnung nur ausgewählt werden müssen.

Beispiele

```
ether host f4:6d:04:66:7c:47
```

Zeichnet nur Pakete auf, in denen die angegebene MAC-Adresse enthalten ist.

```
ether dst ff:ff:ff:ff:ff:ff
```

Zeichnet nur Broadcast-Pakete auf.

```
dst host 192.168.1.1 and src host 192.168.1.20
```

Zeichnet nur Pakete von 192.168.1.20 an 192.168.1.1 auf.

7 vgl. https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html
8 vgl. http://www.tcpdump.org/manpages/pcap-filter.7.html

`net 173.194`

Zeichnet nur Pakete mit einer IP-Adresse aus dem Google-Netzwerk 173.194.0.0/16 auf.

`dst net 192.168.12.0/22`

Zeichnet nur Pakete mit Ziel 192.168.12.0/22 auf.

`host 10.0.0.15 and not tcp dst port 22`

Zeichnet nur Pakete von oder an 10.0.0.15 auf außer die mit Zielport 22/tcp.

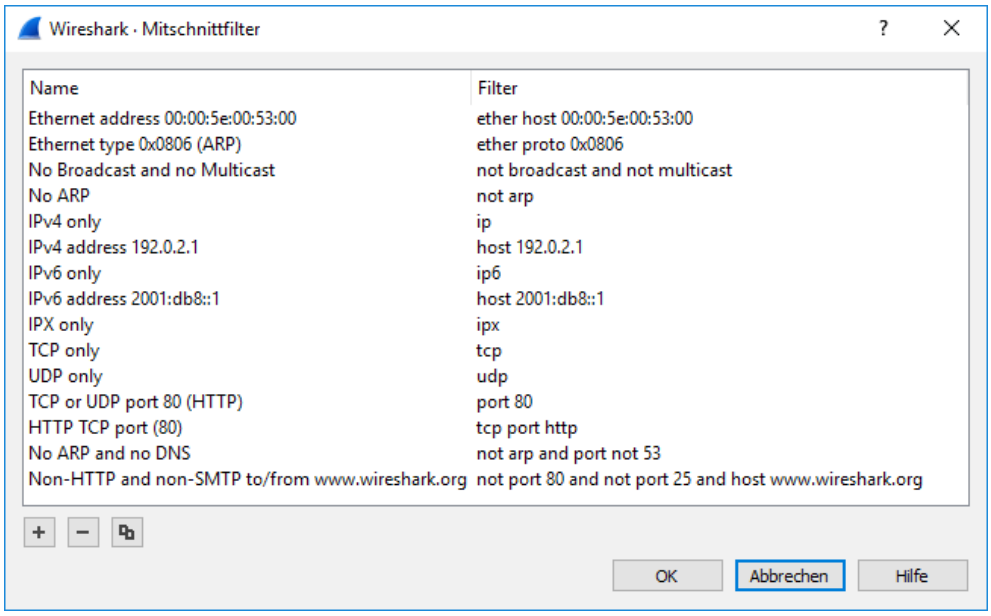
`host 192.168.1.1 and udp dst port 53 or tcp dst port 443`

Zeichnet nur Pakete auf, die die IP-Adresse 192.168.1.1 tragen und an UDP-Port 53 gerichtet sind oder solche, die an TCP-Port 443 gerichtet sind.

`host 192.168.1.1 and (udp dst port 53 or tcp dst port 443)`

Zeichnet nur Pakete auf, die die IP-Adresse 192.168.1.1 tragen und entweder an UDP-Port 53 oder an TCP-Port 443 gerichtet sind.

Über den Menüpunkt „Mitschnittfilter“ im Menü „Aufzeichnen“ können die vorbereiteten Mitschnittfilter verwaltet werden.

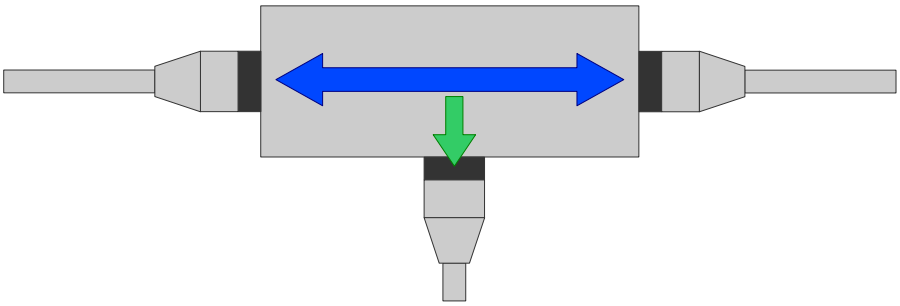


Mitschnittfilter verwalten

Hilfsmittel und Besonderheiten

Mitschneiden mittels TAP

Soll ein Mitschnitt mit Hilfe eines Test Access Ports (TAP) angefertigt werden, muss die bestehende Kabelverbindung an geeigneter Stelle kurzfristig getrennt werden. Ein TAP verfügt üblicherweise über zwei Anschlüsse ihn in eine bestehende Kabelverbindung einzubringen und um einen oder mehrere weitere Anschlüsse, auf denen der gesamte durchgehende Verkehr in Kopie ausgegeben wird. TAPs gibt es sowohl in aktiver als auch passiver Ausführung.



Test Access Port (TAP)

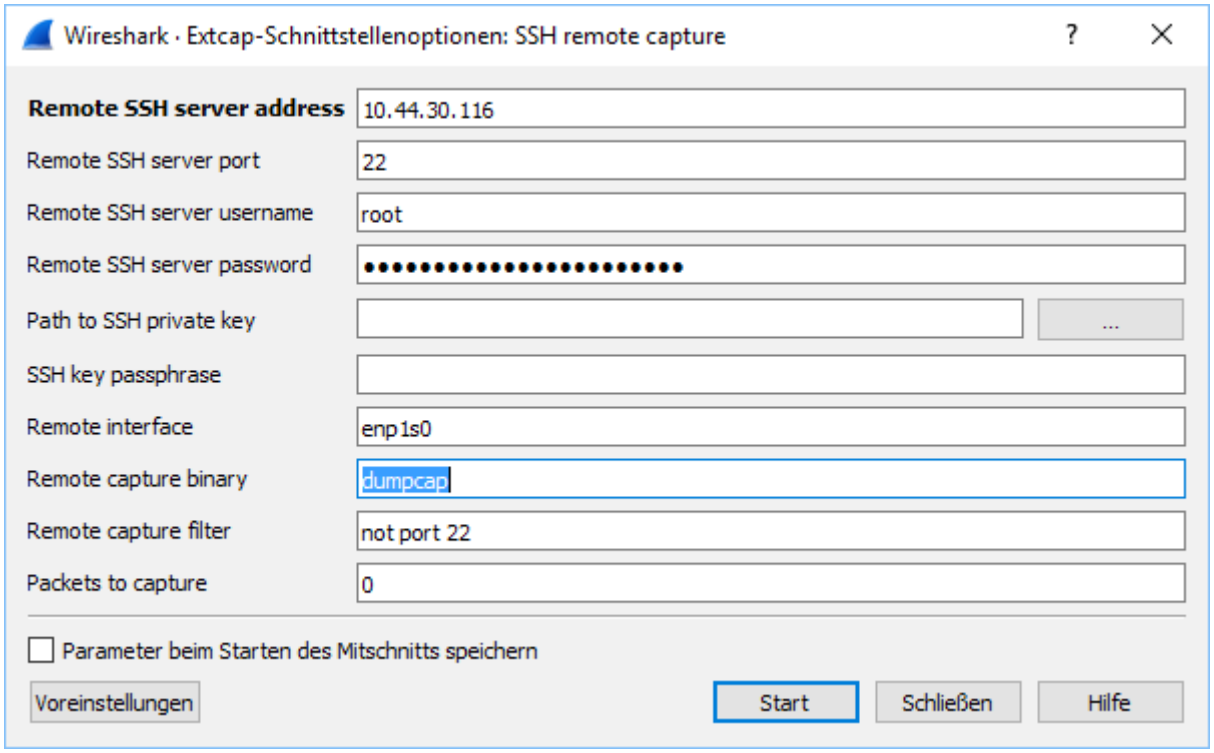
Mitschneiden am Switch

Viele Enterprise-Switches bieten die Möglichkeit, einen unbenutzten Port als Mirroring Port zu konfigurieren. Dabei wird mittels Administratorzugang festgelegt, dass der gesamte ein- und ausgehende Verkehr eines bestimmten Ports in Kopie an einen anderen, unbenutzten Port weitergeleitet wird. An diesen Port kann dann der Netzwerk-Sniffer angeschlossen werden. Diese Methode bietet gegenüber einem TAP den Vorteil, dass eine bestehende Verbindung nicht unterbrochen werden muss.

Mitschneiden mittels SSH

Wurde wie eingangs angegeben die Komponente für das Mitschneiden mittels SSH mitinstalliert, bietet Wireshark in der Auswahl der Interfaces auch die Option „SSH remote capture“ mit an. Dieses Feature vereinfacht die in der Vergangenheit praktizierte Vorgehensweise, bei der ein Mitschnitt unter Verwendung von Pipes und Portweiterleitungen über eine SSH-Verbindung getunnelt wurde erheblich. Es

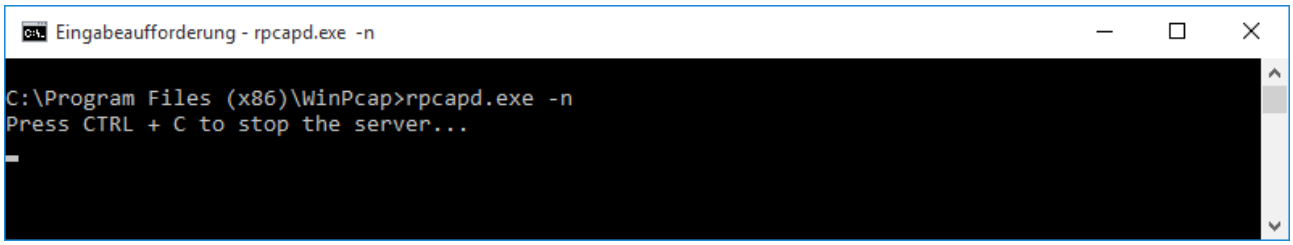
ist lediglich erforderlich, dass auf dem entfernten Host ein geeignetes Kommandozeilenwerkzeug wie tcpdump oder dumpcap installiert ist und der verwendete Benutzer die notwendigen Rechte besitzt.



Dialogfenster: SSH remote capture

Mitschneiden mittels rcapd

Mit dem WinPcap-Treiber wird ein Kommandozeilenwerkzeug namens rpcapd.exe[9], der Remote Packet Capture Daemon, mitgeliefert. Dieser kann auf einem Host ausgeführt werden, auf dem der mitzuschneidende Verkehr anfällt.



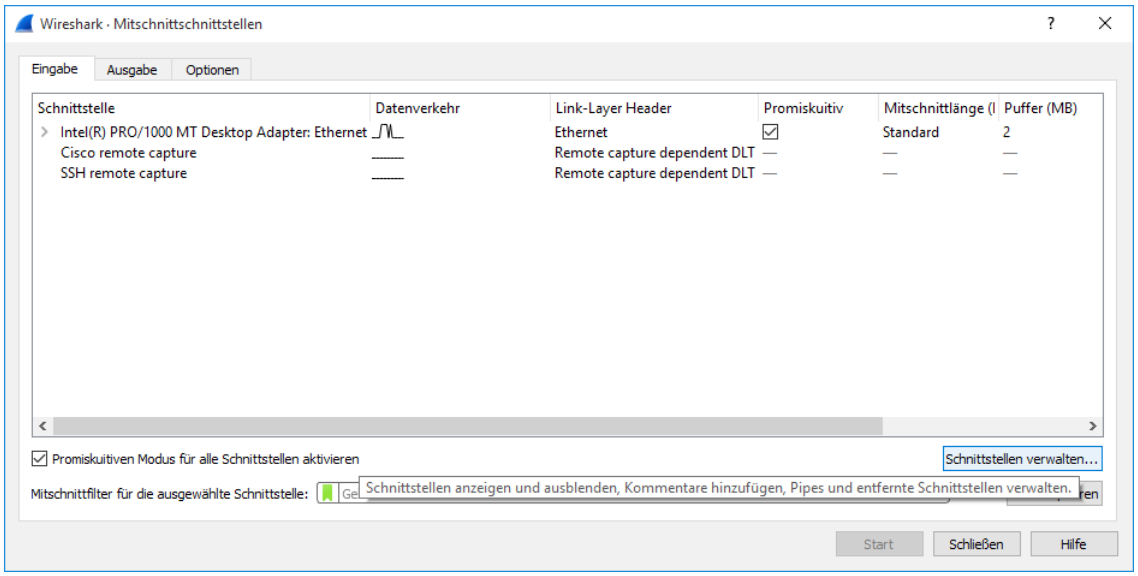
Start des rpcapd auf dem Host, dessen Verkehr mitgeschnitten werden soll

Dort kann er ein Socket zur Verfügung stellen, an dem der Mitschnitt abgegriffen

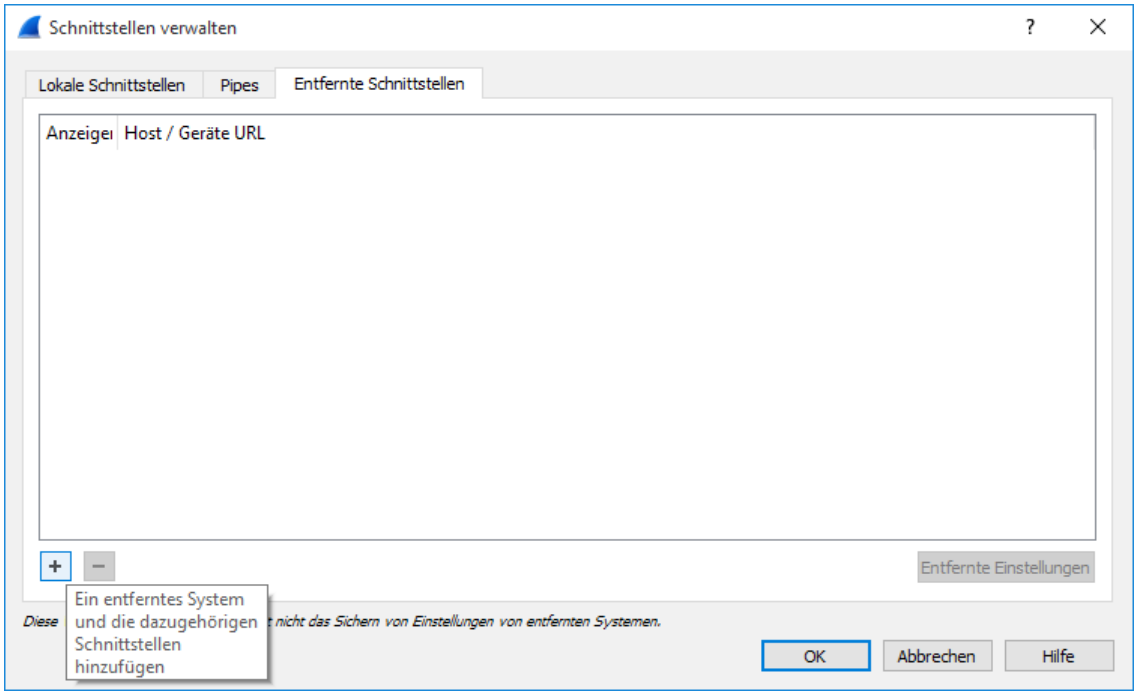
9 vgl. https://www.winpcap.org/docs/docs_40_2/html/group__remote.html

werden kann oder aktiv eine Verbindung aufbauen um den Mitschnitt weiterzuleiten.

Auf einem zweiten Host kann der Daemon als entfernte Schnittstelle eingetragen werden. Dies geschieht in der Schnittstellenverwaltung unter dem Reiter „Entfernte Schnittstellen“.

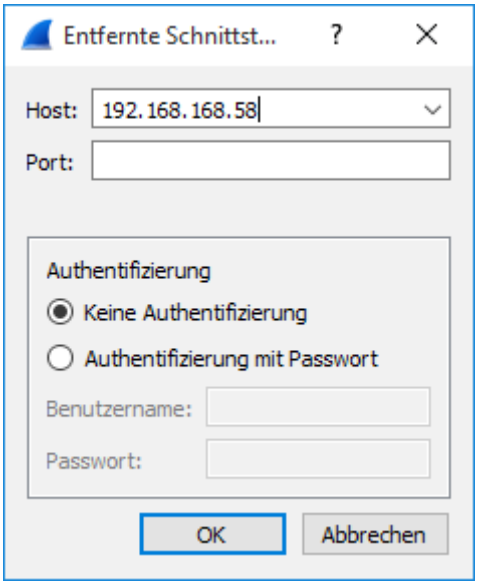


Schnittstellen verwalten



Entfernte Schnittstelle hinzufügen

Um eine Schnittstelle hinzuzufügen, genügt es im einfachsten Fall nur die IP-Adresse anzugeben, unter der der rpcap-Daemon läuft.



IP-Adresse des rpcapd-Hosts angeben

Mitschneiden auf mehreren Interfaces

Ein Mitschnitt muss nicht notwendigerweise auf nur einem einzigen Interface durchgeführt werden. Es können auch mehrere Interfaces für einen Mitschnitt ausgewählt werden, wenn dies für einen bestimmten Anwendungsfall sinnvoll erscheint. Zur besseren Unterscheidung kann eine zusätzliche Spalte in der Paketliste eingefügt werden, die angibt, auf welchem Interface der Frame mitgeschnitten wurde. Der hierfür benötigte Filterausdruck lautet `frame.interface_id` und ist als Feldbezeichnung für die Spalte anzugeben.

Mitschneiden von Wireless LAN

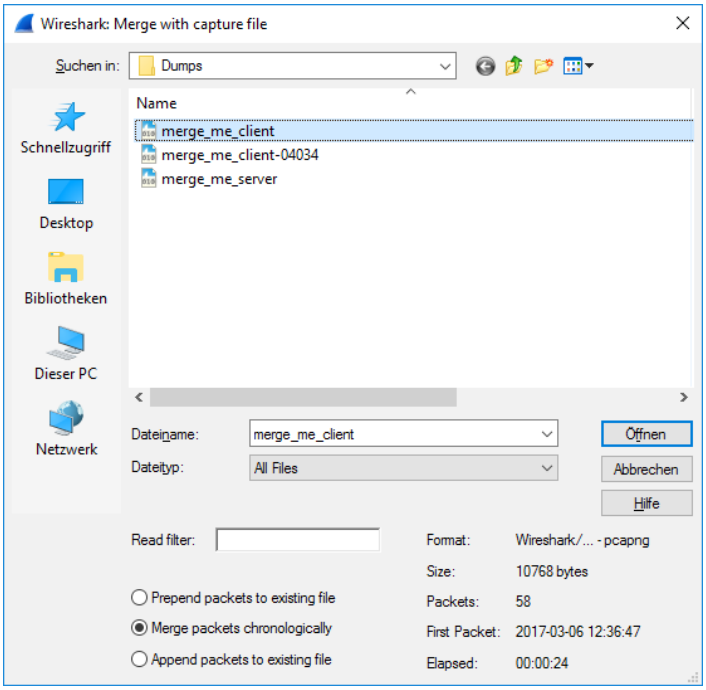
Das Anfertigen von Verkehr auf drahtlosen Schnittstellen kann in zweierlei Weise erfolgen. Zum Einen kann eine solche Schnittstelle einfach für den Mitschnitt ausgewählt werden. Der darüber abgewickelte Verkehr wird dann in der gleichen Weise angezeigt, wie auch auf einer herkömmlichen Ethernet-Schnittstelle. Zum Anderen kann die Netzwerkkarte in den sogenannten Monitor Mode versetzt werden. Zeichnet man dann Netzwerkverkehr auf, so bekommt man auch Frames zu Gesicht, die speziell für die Abwicklung der drahtlosen Verbindung benötigt

werden. Hierzu gehören unter anderem auch Management Frames und Control Frames. Diesen sind auch Angaben zu Kanälen, Signalstärke und Datenraten zu entnehmen. Außerdem können Beacons und Probe Requests und Responses beobachtet werden, ebenso wie Anmeldevorgänge drahtloser Netzwerkteilnehmer am Netzwerk.

Unter Windows ist die Verwendung des Monitor Modes nicht ohne weiteres möglich, da dies vom WinPcap-Treiber nicht unterstützt wird. Es gibt jedoch spezielle Hardware und Treiber namens AirPcap, mit denen derartige Mitschnitte auch unter Windows mögich werden.

Zusammenführen mehrerer Mitschnittdateien

Hat man mehrere Mitschnittdateien erzeugt, entweder aus Platzgründen als aufeinanderfolgende Segmente oder zur besseren Fehlersuche parallel auf mehreren Geräten, kann es notwendig werden, diese zu Analysezwecken zusammenzuführen. Dies ist in Wireshark relativ einfach über das Dateimenü möglich. Hierzu öffnet man zuerst eine der betreffenden Mitschnittdateien. Ab dann ist der Menüpunkt „Zusammenführen“ verfügbar. Dieser öffnet einen Dateiauswahldialog in dem eine weitere Datei ausgewählt und angegeben werden kann, wie die Dateien zusammenzuführen sind.



Dateien zusammenführen

Das verbinden mehrerer aufeinanderfolgender Mitschnittdateien ist grundsätzlich unproblematisch. Etwas schwieriger kann es bei Mitschnitten werden, die zur gleichen Zeit auf unterschiedlichen Geräten erstellt worden sind. Zum Einen ist es hierbei empfehlenswert eine zusätzliche Spalte in der Paketliste anzulegen, welcher entnommen werden kann, von woher das dargestellte Paket stammt, z.B. über den Filterausdruck frame.interface_id. Zum Anderen kann es zu Problemen kommen, wenn die Systemzeit nicht auf allen Geräten exakt gleich eingestellt war. Dann kann es z.B. zu folgender Konstellation kommen:

Nr.	Zeit	Interface	Quelle	Ziel	Info
1	0.010	1 (Server)	Client	Server	Echo Request
2	0.013	1 (Server)	Server	Client	Echo Reply
3	0.505	0 (Client)	Client	Server	Echo Request
4	0.518	0 (Client)	Server	Client	Echo Reply

In diesem Beispiel scheint es, als ginge zuerst auf dem Server ein Ping-Paket vom Client ein und ein Antwortpaket zurück, bevor eine Sekunde später beim Client die gleichen Pakete zu beobachten sind. Dies ist unlogisch, da zuerst das Ping-Paket beim Client ausgehen müsste, dann beim Server ankommen, danach beim Server das Antwortpaket ausgehen und dieses schließlich beim Client ankommen müsste. Die korrekte Reihenfolge der angezeigten Pakete müsste somit 3 1 2 4 lauten. Erklären lässt sich dies dadurch, dass die Systemzeit beim Client in diesem Beispiel um exakt eine halbe Sekunde zu spät ist.

Ist man bei realen Mitschnitten mit diesem Problem konfrontiert, kann man es mit dem Kommandozeilenwerkzeug editcap[10] beheben. Voraussetzung dafür ist, dass man die Zeitdifferenz entweder direkt am System oder anhand der Zuordnung von Paketen in den Mitschnitten ermittelt hat. In diesem Beispiel müsste von den Zeitstempeln im clientseitigen Mitschnitt eine Sekunde abgezogen werden. Der editcap-Aufruf hierfür könnte wie folgt lauten:

```
editcap -t -.5 client.pcapng client_korrigiert_0.5s.pcapng
```

Anschließend verwendet man die neu erzeugte Datei, korrigierte Datei.

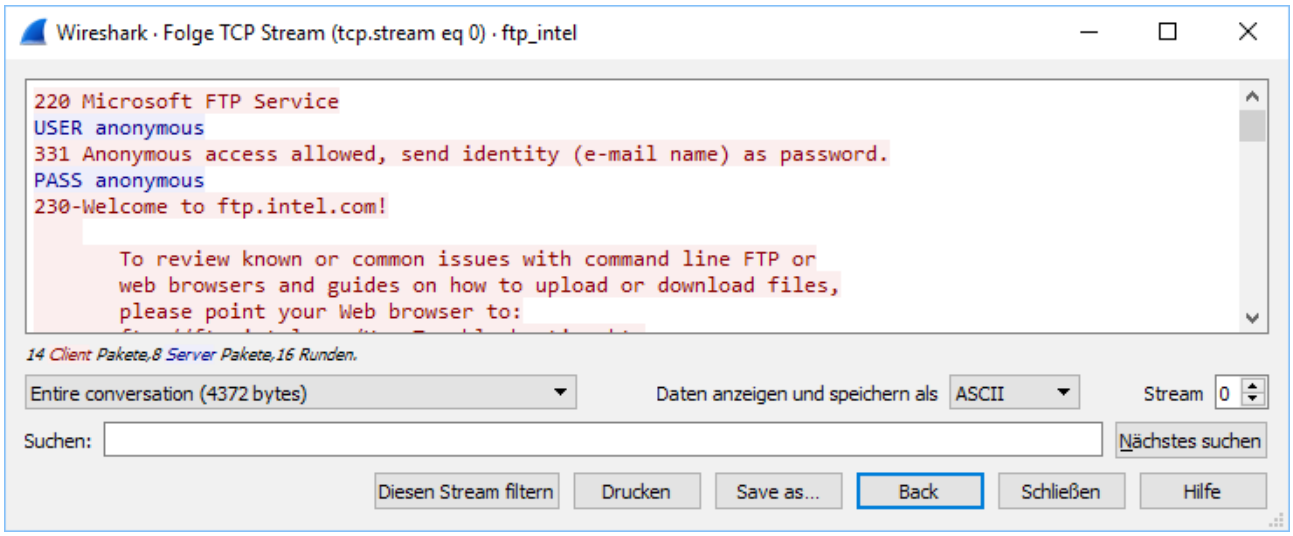
10 vgl. https://www.wireshark.org/docs/man-pages/editcap.html

Analyse von Mitschnitten

Zur Analyse von Mitschnitten bietet Wireshark neben der Filterung verschiedene Hilfsmittel an. Die gebräuchlicheren sollen nachfolgend vorgestellt werden.

Follow Stream

Eines der hilfreichsten Features zur Analyse ist die Fähigkeit den zu einem bestimmten Paket gehörenden Datenstrom aus dem Mitschnitt zu isolieren. Diese Funktion ist über das Kontextmenü des betreffenden Paketes zu erreichen.
Während dieser Menüpunkt anfangs schlicht „Follow TCP Stream“ bezeichnet wurde, unterscheidet Wireshark aktuell verschiedene Arten von Streams. Das Programm ist in der Lage auch netzwerktechnisch gesehen unabhängige Pakete z.B. aus UDP-Konversationen einander zuzuordnen (z.B. DNS-Abfrage und Antwort).
Die Konversation wird in einem eigenen Fenster mit farblicher Unterscheidung zwischen Server und Client dargestellt.



Follow TCP Stream

Wireshark bietet in diesem Fenster auch einige Einstellmöglichkeiten, wie die gefilterte Konversation dargestellt werden soll und bietet auch die Möglichkeit, diesen Stream in eine Datei zu speichern. Zur einfacheren Handhabung kann aus dieser Ansicht heraus direkt auf die nächsten Streams weitergeschaltet werden.

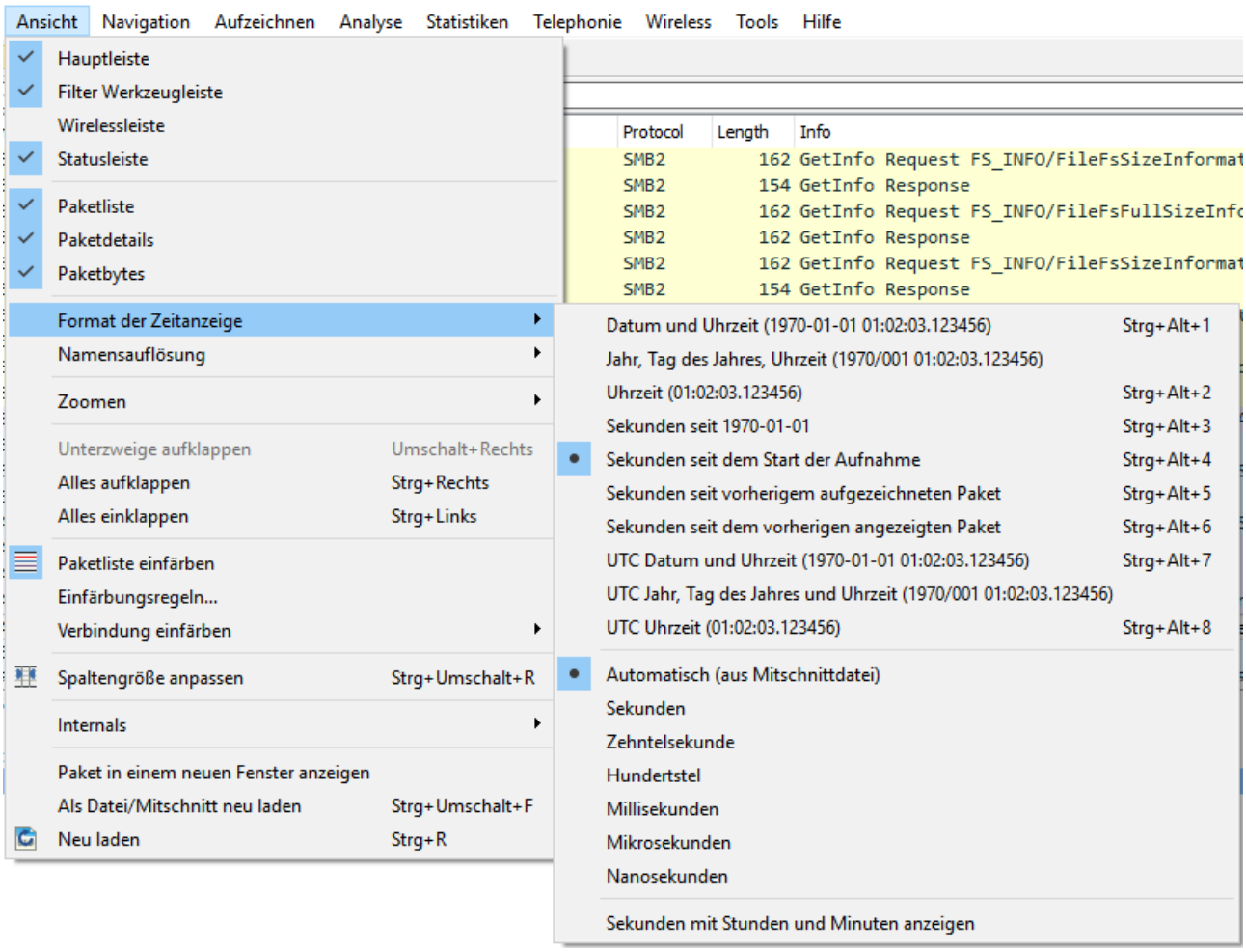
Es ist zu beachten, dass gleichzeitig mit der Filterung des Streams im Hauptfenster ein Display-Filter angewandt wird.

Suchfunktion

Die Suchleiste kann mit der hierfür üblichen Tastenkombination Strg + F geöffnet werden oder aus dem Menü „Bearbeiten“.
Anders als der Anzeigefilter, der alle nicht zutreffenden Pakete ausblendet, ermöglicht es die Suchfunktion, Pakete mit bestimmten Eigenschaften aufzufinden und sie im Verlauf der anderen Pakete zu zeigen. Eine der möglichen Suchvarianten ist trotzdem die Verwendung der Syntax des Display-Filters. Zusätzlich ist es möglich, nach Hexadezimalwerten, Zeichenketten oder regulären Ausdrücken zu suchen. Gefundene Pakete werden hervorgehoben und angezeigt.
In der Streamansicht gibt es eine eigene Suchfunktion, welche nichts mit der globalen Suche zu tun hat.

Zeitangaben

Wireshark speichert bei der Aufzeichnung die Zeitstempel im Unix-Zeitformat (Seit 01.01.1970) ab. Bei der Anzeige eines Mitschnittes wird für eine absolute Zeitangabe die Zeitzone des anzeigenden Systems verwendet. Dies ist ggf. bei der Überschreitung von Zeitzonengrenzen zu beachten.
Oftmals sind die zeitlichen Zusammenhänge der Kommunikation im Netzwerk interessant. Hier bietet Wireshark mehrere Möglichkeiten, wie die Zeit in der entsprechenden Spalte der Paketliste dargestellt werden soll. Über die Bearbeitungsfunktion im Kontextmenü oder über das Menü „Ansicht“ können Anpassungen vorgenommen werden. Letzteres ist quasi das festgelegte Standardformat und bestimmt auch die Anzeige, wenn für das Spaltenformat „Time (format as specified)“ ausgewählt wurde.
So lässt sich nicht nur die absolute Zeit oder die verstrichene Zeit seit Beginn der Aufzeichnung anzeigen. Es ist auch möglich, bestimmte Pakete als Zeitreferenz zu setzen, so dass die verstrichene Zeit seit dem gewählten Paket angezeigt wird. Auch die Zeitdifferenz zum vorangegangenen Paket kann gewählt werden. Dies ist hilfreich, wenn das Antwortzeitverhalten betrachtet wird oder nach Pausen in der Kommunikation gesucht wird.



Auswahl des Formats zur Anzeige von Zeitangaben

Experteninfo

Einen anderen Überblick über den Mitschnitt liefert die sogenannte Experteninfo. Sie ist über das Leuchtensymbol links in der Statusleiste zu erreichen und wird in einem eigenen Fenster angezeigt. Dort sind nach Schweregrad (Fehler, Warnung, etc.) gestaffelt Ereignisse aufgelistet, die eine Besonderheit im Netzwerkverkehr darstellen, wie z.B. fehlerhafte bzw. von Wireshark nicht interpretierbare Pakete, Übertragungsfehler, Wiederholungen und ähnliches.

Gerade bei der Fehlersuche kann diese Ansicht schnell erste Anhaltspunkte liefern.

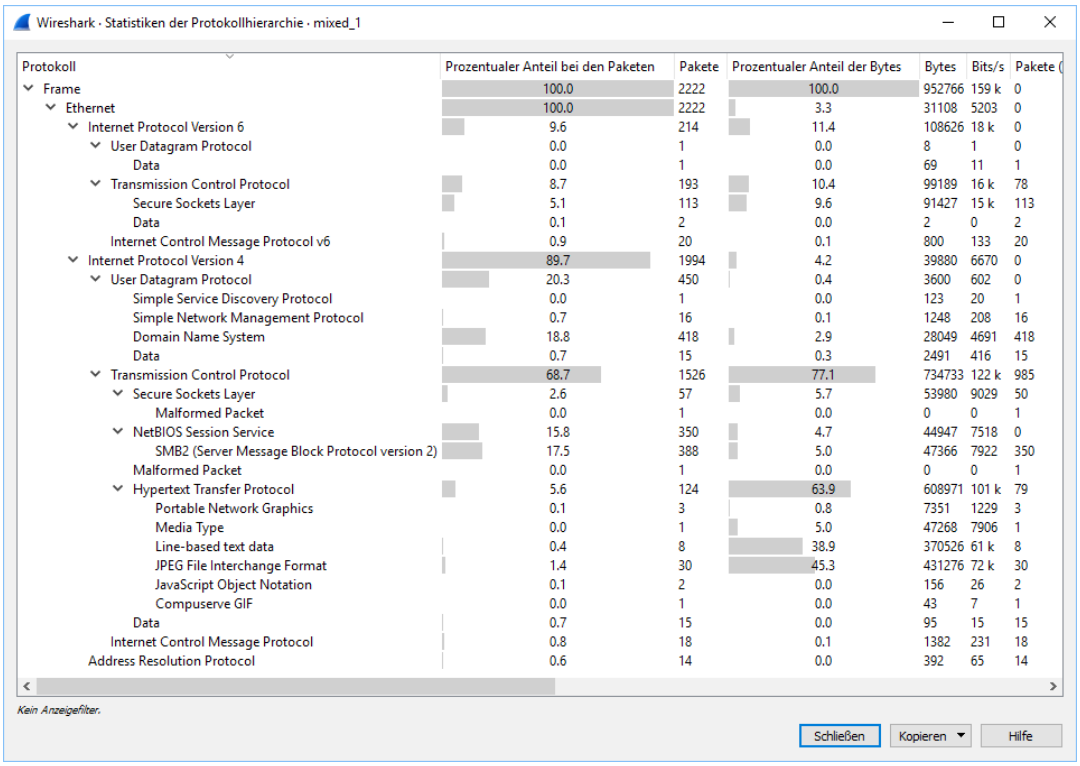
Statistiken

Einen etwas größeren Bereich von Auswertungen erhält man über das Menü „Statistiken“. Hier sind mehrere Menüpunkte hervorzuheben:
Eigenschaften der Mitschnittdatei

Hier erhält der Nutzer einen groben Überblick über die Metadaten des Mitschnitts. Zeitumfang, Paketanzahl, Speicherort sowie aufzeichnende Software und verwendetes Netzwerk-Interfaces sind nur einige der bereitgestellten Informationen.

Protokollhierarchie

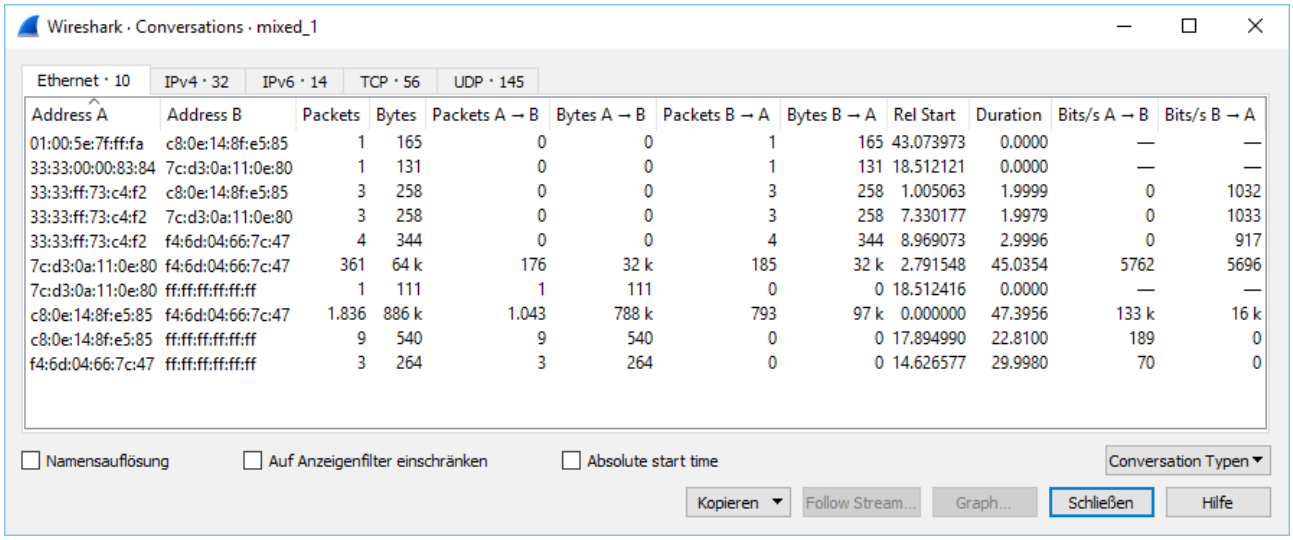
In diesem Dialogfenster erhält der Nutzer einen Überblick über die prozentuale Verteilung der Pakete oder Daten auf verschiedene Protokolle. Dies liefert zum einen einen grundlegenden Überblick, welche Arten von Netzwerkverkehr überhaupt aufgezeichnet wurden, zum anderen lassen sich unter Umständen Auffälligkeiten hinsichtlich der Häufigkeit mancher Protokolle erkennen. Hierfür sind natürlich Referenzwerte nötig.



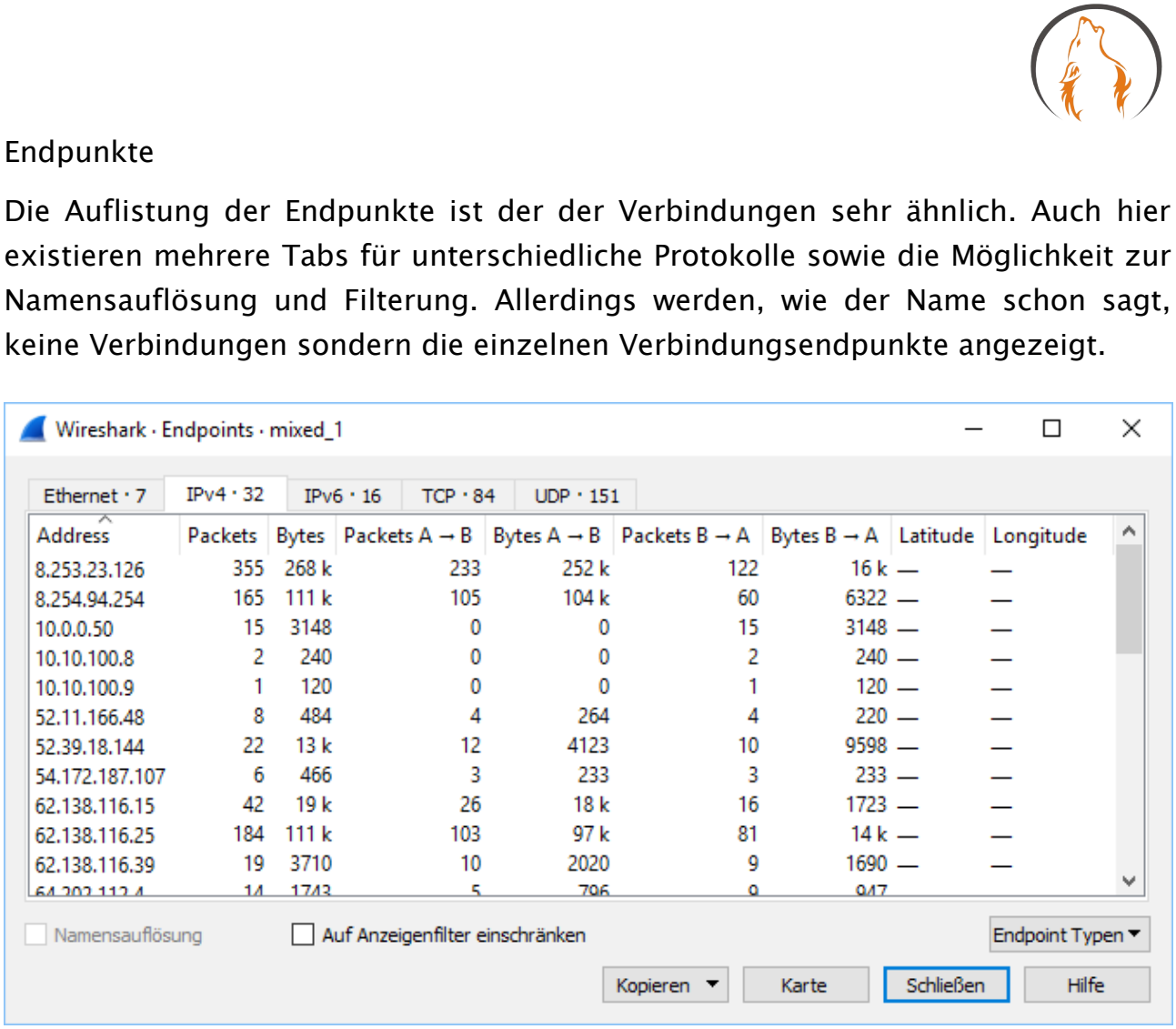
Protokollhierarchie

Verbindungen

Das Dialogfenster Verbindungen listet die im Mitschnitt identifizierten Verbindungen zwischen zwei Kommunikationsendpunkten auf. Es kommen hierbei die Schichten aus dem TCP/IP-Modell zum Tragen, denn es werden Tabs für verschiedene Protokolle unterschiedlichen Ebenen angeboten. Der Aufruf einer Webseite wird sich z.B. sowohl als TCP- als auch als IP-Verbindung identifizieren lassen, ggf. sogar als Ethernet-Verbindung.
Das Dialogfenster bietet zudem die Möglichkeit eine Namensauflösung durchzuführen und eine gewählte Verbindung als Anzeigefilter zu aktivieren.



Verbindungen



Endpunkte

Die Auflistung der Endpunkte ist der der Verbindungen sehr ähnlich. Auch hier existieren mehrere Tabs für unterschiedliche Protokolle sowie die Möglichkeit zur Namensauflösung und Filterung. Allerdings werden, wie der Name schon sagt, keine Verbindungen sondern die einzelnen Verbindungsendpunkte angezeigt.

Endpunkte

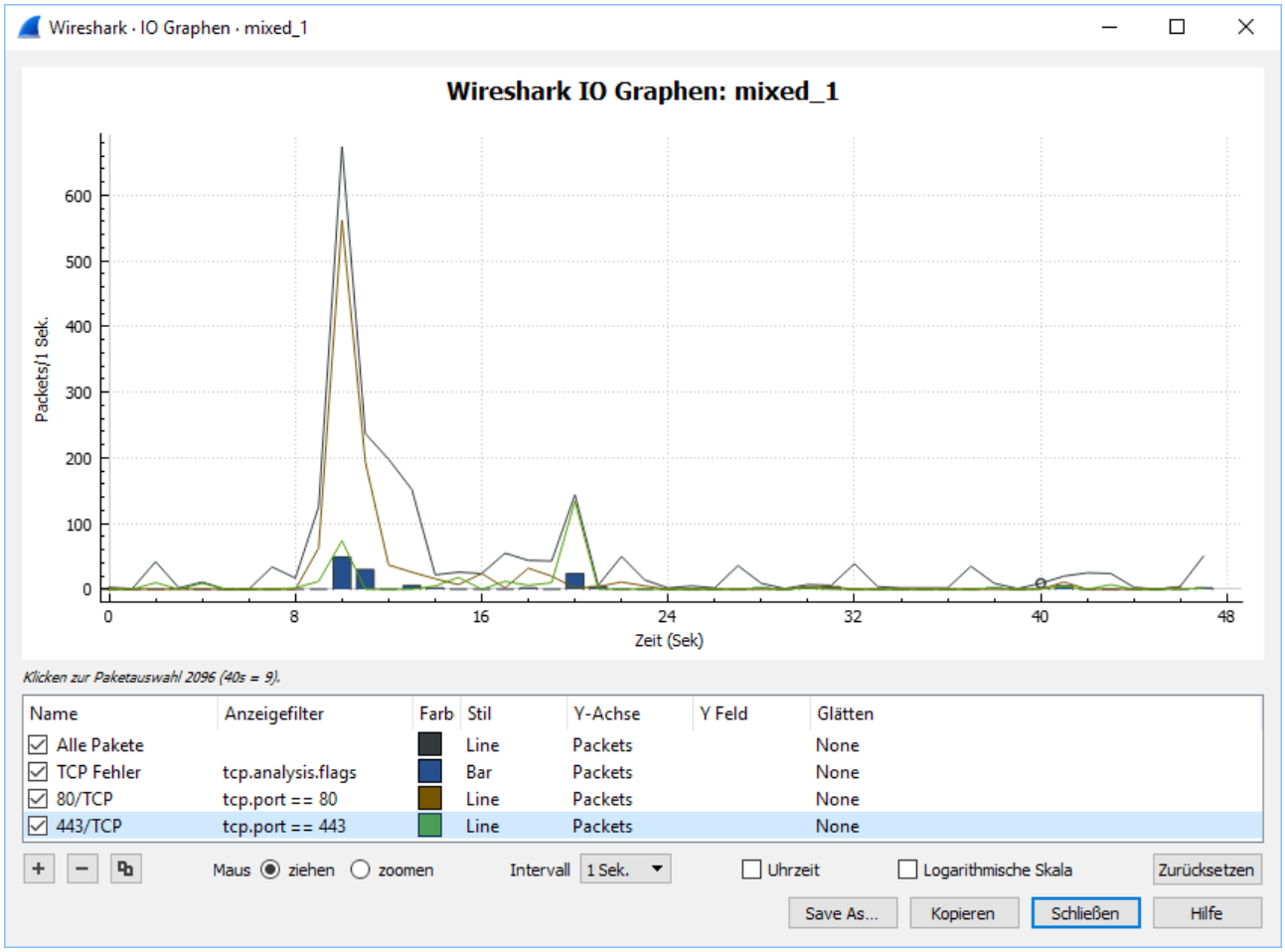
Diese Ansicht kann z.B. hilfreich sein um auffällig gesprächige Endpunkte im Netzwerk ausfindig zu machen.

Paketlängen

Dieses Dialogfenster zeigt schlicht eine anteilige Auswertung der aufgezeichneten Pakete anhand ihrer Größe. Diese Aufteilung ist im globalen Einstellungsmenü konfigurierbar.

I/O Graph

In manchen Fällen kann es hilfreich sein, verschiedene Aspekte des Mitschnittes zu visualisieren und miteinander zu vergleichen. Anomalien oder Zusammenhänge lassen sich hierdurch oft schneller erkennen. Hierfür ist das Dialogfenster I/O Graph geeignet.

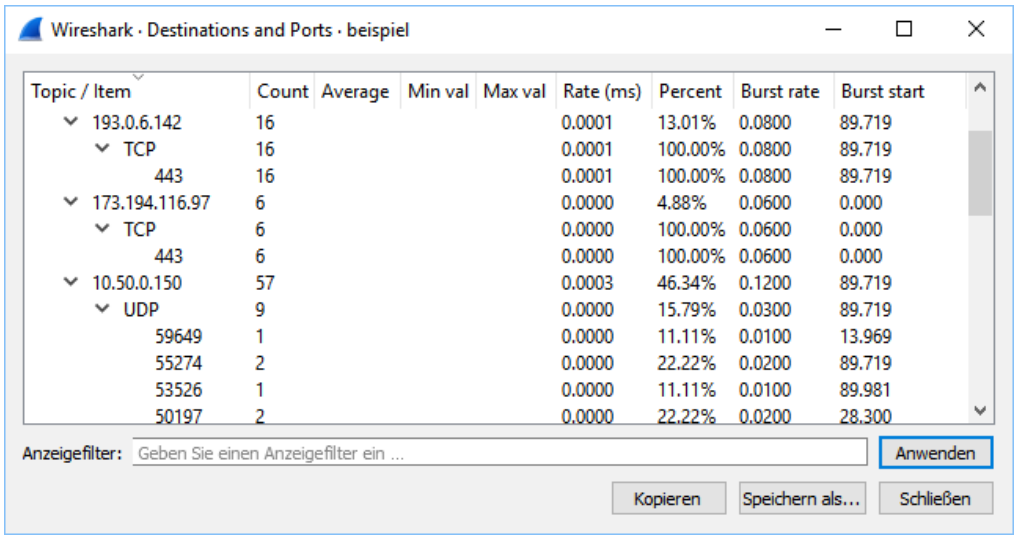


IO Graph

Um diese Funktion sinnvoll einzusetzen, ist es notwendig, eigene Graphen anzulegen. Dies geschieht im Wesentlichen über die Eingabe eines Display-Filterausdrucks. Zusätzlich können einige Anzeigeoptionen festgelegt werden.
Wurden in der grafischen Darstellung interessante Punkte identifiziert, ist es über das Kontextmenü möglich, die zugehörigen Pakete in der Paketliste anzusteuern. Ebenso bietet das Kontextmenü noch weitere Navigations- und Darstellungsoptionen.

IPv4-/IPv6-Statistiken

Die beiden Menüeinträge IPv4- und IPv6-Statistiken bieten noch weitere Sichtweisen auf den Mitschnitt ähnlich den Verbindungs- und Endpunktstatistiken. Am ehesten dürfte die Ansicht „Destinations and Ports“ von Nutzen sein, da sie die bereits kennengelernten Sichten um eine Gruppierung der verwendeten Ports zu den beteiligten Kommunikationspartnern ergänzt.



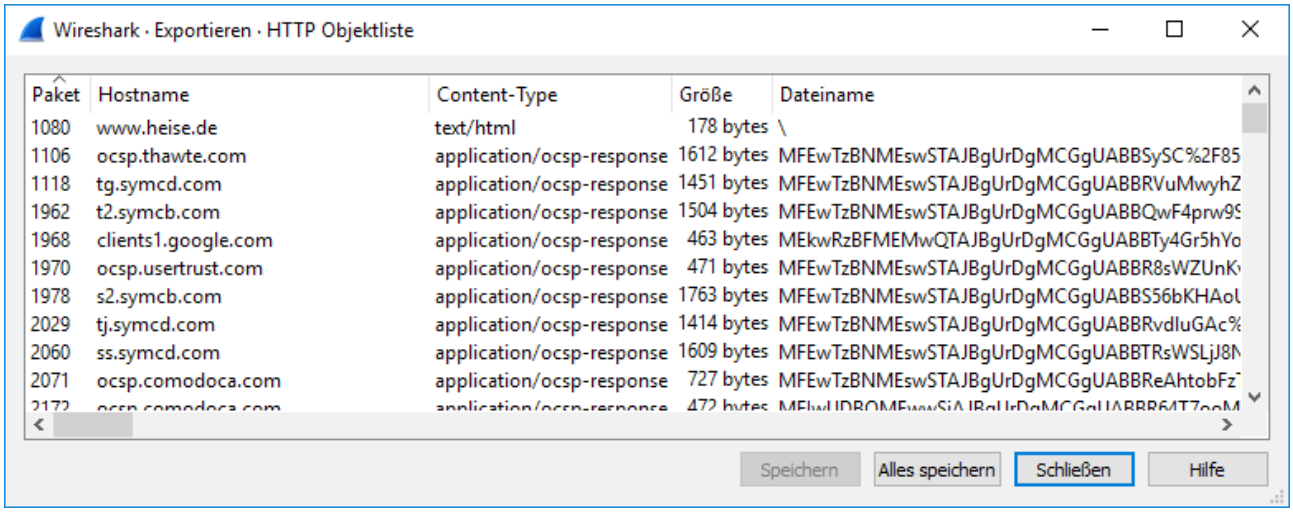
IPv4-Statistiken: Destinations and Ports

Protokolleinstellungen

Das Kontextmenü beinhaltet einen Eintrag „Protokolleinstellungen“. Dessen Unterpunkte variieren stark in Abhängigkeit davon, wo das Kontextmenü aufgerufen wurde. So gibt es große Unterschiede, ob man in der Paketliste klickt und welche Art von Verkehr man angeklickt hat oder ob man das Kontextmenü in der Detailansicht aufruft und dort wiederum für welche Elemente einer bestimmten Schicht.

Objekte exportieren

Für ausgewählte Protokolle bietet Wireshark die Option in der Kommunikation enthaltene Objekte zu exportieren. Derzeit ist dies für DICOM[11], HTTP, SMB und TFTP verfügbar. Um diese Funktion nutzen zu können, muss der Mitschnitt bereits angehalten worden sein.



HTTP-Objekte aus einem Mitschnitt exportieren

Es können sowohl ausgewählte Objekte einzeln exportiert werden als auch alle erkannten Objekte. Dabei ist darauf zu achten, dass ein geeigneter Speicherort gewählt wird, am besten in einem neuen, leeren Ordner.

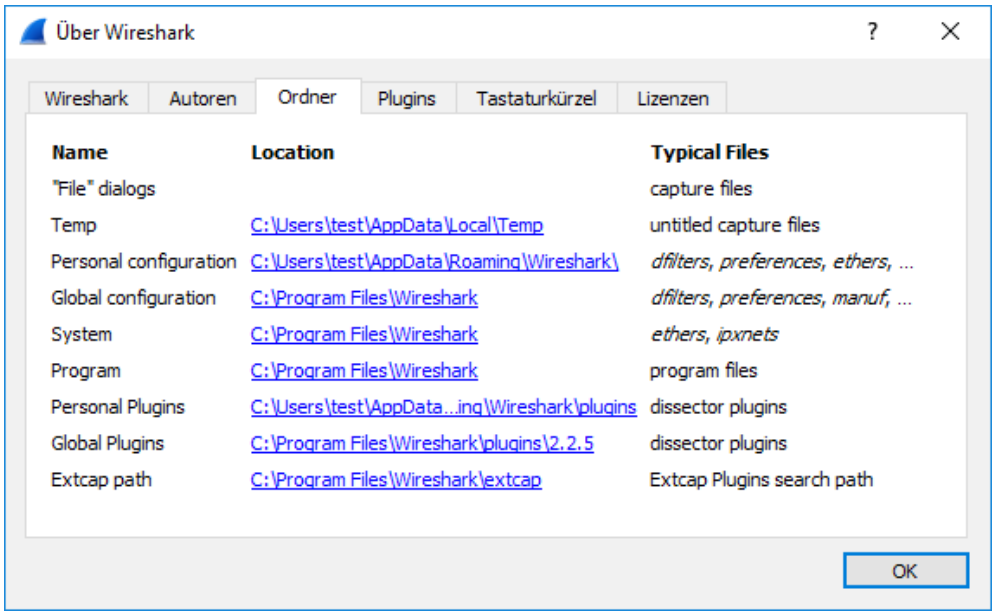
11 Digital Imaging and Communications in Medicine

Anpassen der Arbeitsumgebung

Profile

Wireshark lässt sich in hohem Maß an die vielfältigen Erfordernisse des Nutzers anpassen. Unterschiedliche Einsatzszenarien können ebenso unterschiedliche Darstellungen und Anpassungen erfordern. Hierzu stehen in Wireshark Profile zur Verfügung.
Das aktuell gewählte Profil wird in der Statusleiste ganz rechts unten angezeigt. Hierüber kann auch auf andere Profile umgeschaltet (Linksklick) oder die Verwaltung der Profile geöffnet werden (Rechtsklick). Alternativ ist das zugehörige Dialogfenster auch über die Menüleiste erreichbar.
Jede Veränderung von Einstellungen wie z.B. die Anordnung von Fenstern und Spalten sowie Farbeinstellungen u.v.m. wird automatisch im aktuell aktiven Profil hinterlegt.

Ein wenig versteckt ist das Dialogfenster zur Verwaltung der Pfade in Wireshark im Menü „Hilfe“ unter dem Menüpunkt „Über Wireshark“ zu finden. Dem Reiter Ordner sind veschieden Pfade zu entnehmen, unter anderem auch der Speicherort der Profildateien. Kopiert man das entsprechende Verzeichnis, kann man recht einfach Profile kopieren oder sichern.



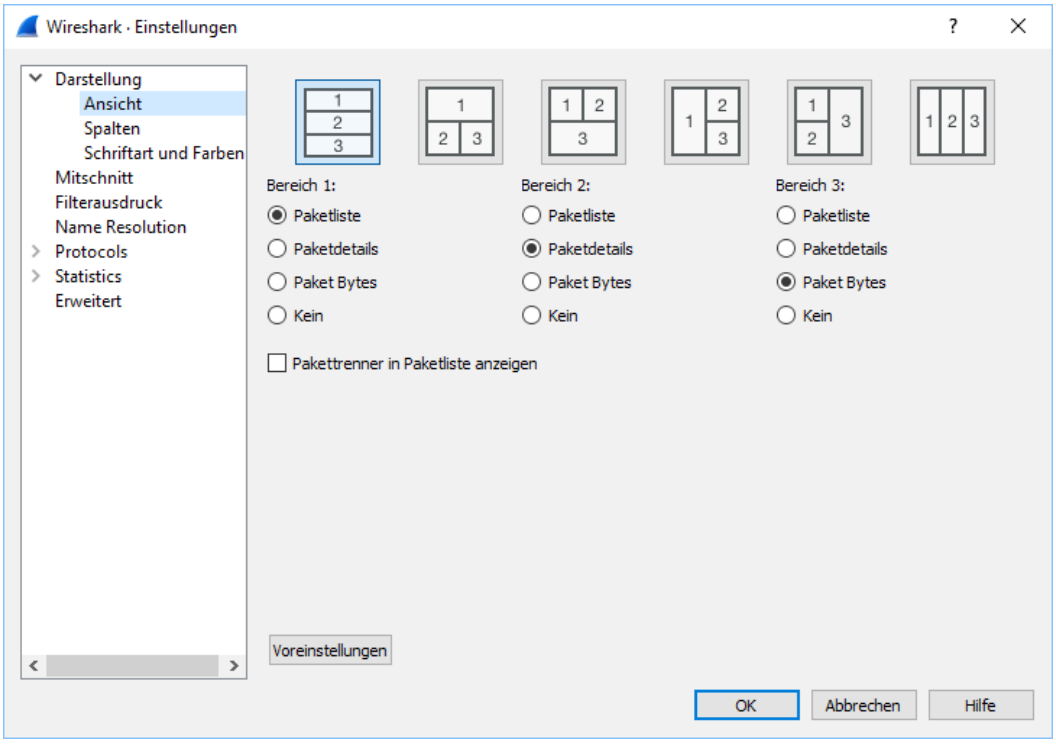
Über Wireshark: Pfade

Einstellungen

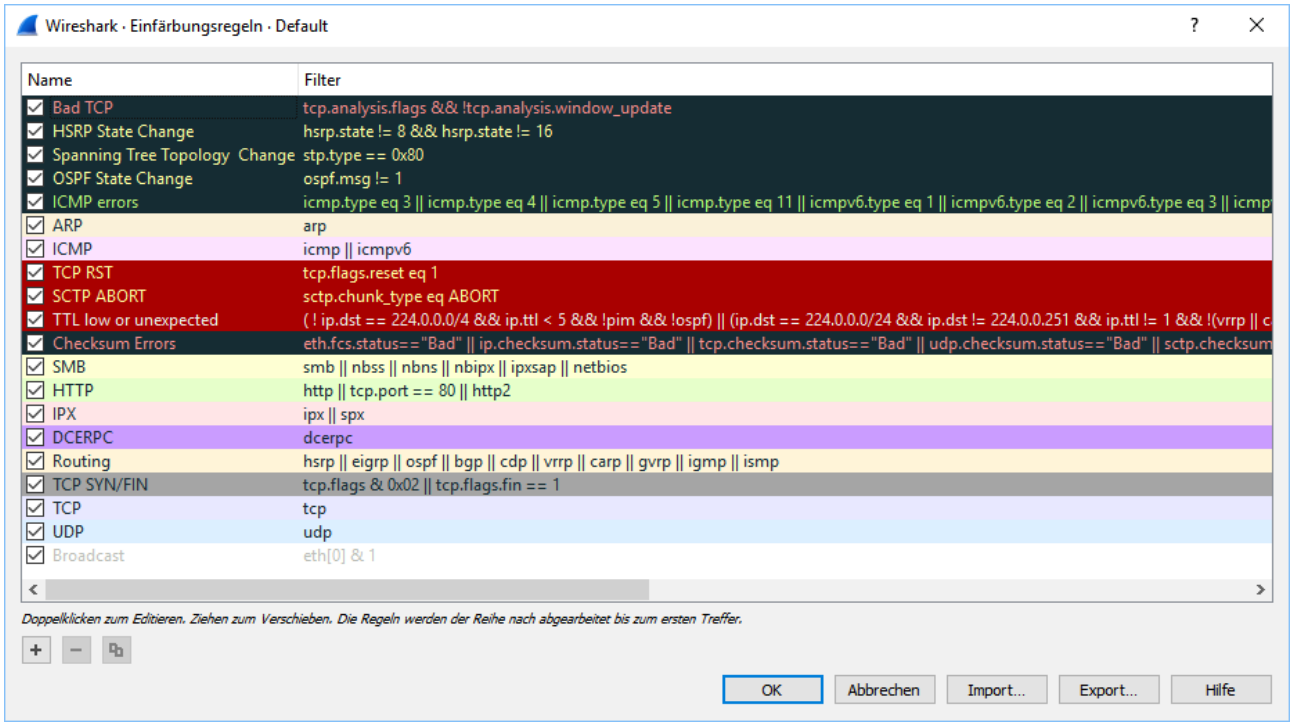
Die allgemeinen Einstellungen für Wireshark findet man zentral im Menü „Bearbeiten“. Es sei auch erwähnt, dass einige weitere Informationen zu globalen Einstellungen Im Menü „Hilfe“ unter dem Menüpunkt „Über Wireshark“ in den dort vorhandenen Tabs zu finden sind. Hierzu gehören z.b. Ordnereinstellungen, vorhandene Plugins und Tastaturkürzel.

Darstellung

Der Einstellungsbereich „Darstellung“ gibt dem Nutzer die Möglichkeit das Erscheinungsbild von Wireshark den jeweiligen Erfordernissen anzupassen. Dies geht von der allgemeinen Aufteilung der Fenster über anzuzeigende Spalten bis hin zur farblichen Aufbereitung der Fensterinhalte.
Neben den Farbeinstellunge in diesem Menü bietet das Ansichtmenü weitere Möglichkeiten zur farblichen Kennzeichnung. Zum Einen lassen sich ausgewählte Verbindungen zur besseren Unterscheidung farblich Kennzeichnen (Menüpunkt: Verbindung einfärben). Zum Anderen können die Einfärbungsregeln, die Wireshark in der Paketliste anwendet, beliebig angepasst werden. Der zugehörige Dialog ist über den Menüpunkt „Einfärbungsregeln“ zu erreichen.



Einstellungen Darstellung



Einfärbungsregeln

Mitschnitte

Im Bereich „Mitschnitt“ lassen sich einige Voreinstellungen für die Aufzeichnung machen.

Filterausdruck

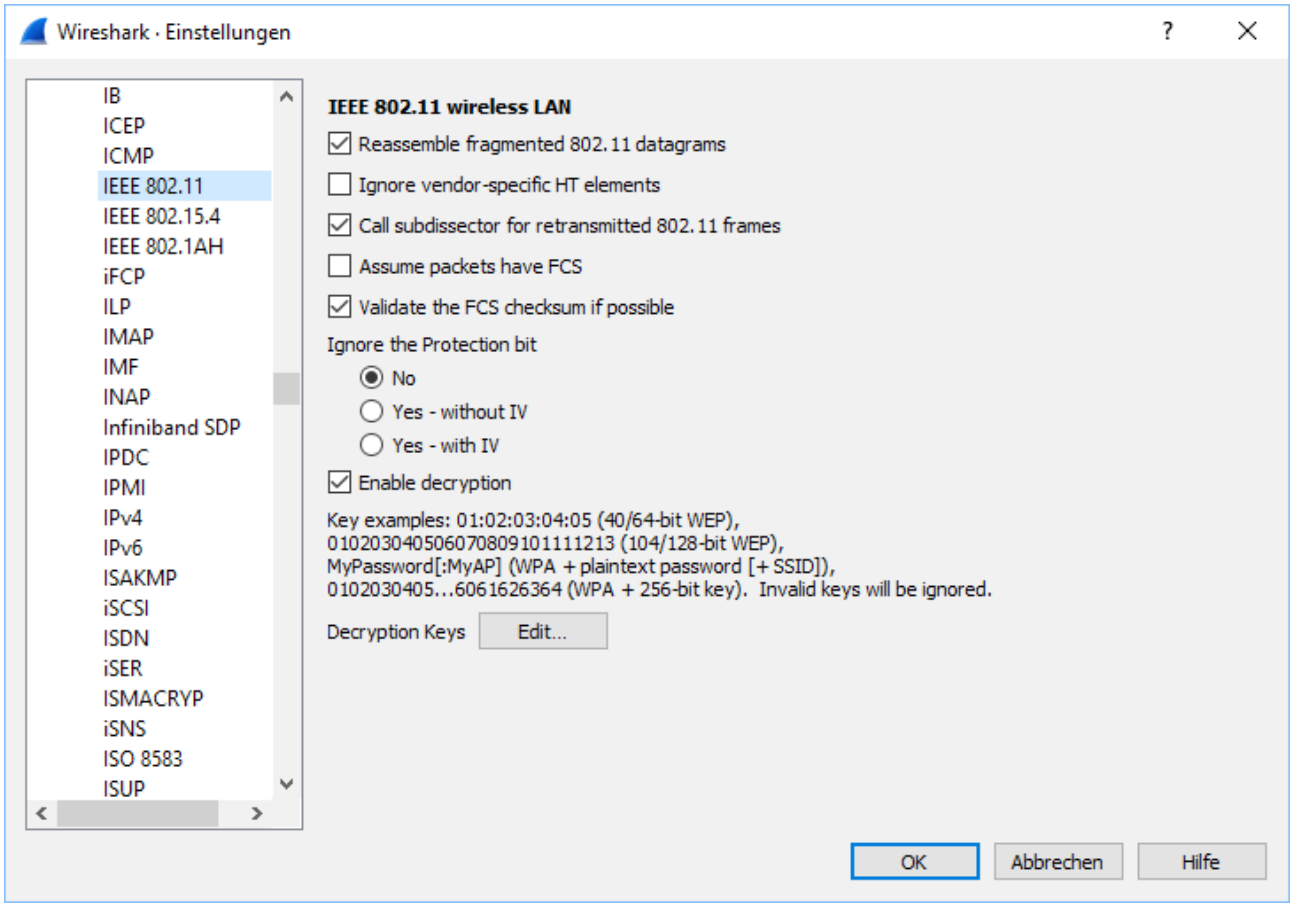
Der Abschnitt „Filterausdruck“ dient dazu die gespeicherten Display-Filter zu verwalten. Hier können Filter angelegt und gelöscht werden und es lässt sich einstellen, welche der vorhandenen Filter gerade aktiviert, also in der Filterleiste verfügbar sein sollen.

Namensauflösungen

Im Abschnitt „Namensauflösungen“ kann festgelegt werden, welche Werte in Namen übersetzt werden sollen. Hierzu gehört z.B. die Auflösung von MAC-Adressen zu Herstellern oder von IP-Adressen zu DNS-Namen.

Protokollebenen

Im Abschnitt „Protocols“ können zu allen Protokollen, zu denen Dissektoren vorhanden sind, jeweils zutreffende Einstellungen vorgenommen werden. So können z.B. für die Analyse von HTTPS- und WLAN-Verkehr bekannte



Einstellungen Protocols

Statistiken

Der Dialog „Statistics“ erlaubt Einstellungen für die statistische Auswertung des aufgezeichneten Verkehrs.

Erweitert

Der Abschnitt „Erweitert“ bietet direkten Zugriff auf zahlreiche Einstellungsparameter ohne Eingabeformular. Einstellungen, die nicht mehr der Standardeinstellung entsprechen, sind hervorgehoben.

Fehlersuche

Versuchen Sie am Anfang grundlegende Fehler auszuschließen. Achten Sie zum Beispiel auf DHCP-Requests, welche eventuell unbeantwortet bleiben. Analysieren Sie unbeantwortete oder unbefriedigend beantwortete ARP- und DNS-Anfragen.
Bei korrekt funktionierendem DHCP sehen Sie im Normalfall vier zueinander gehörende Pakete, mit denen einem Client die notwendigen Informationen zugeteilt werden. Diese sind

- DHCP-Discover
  Der Client versucht einen DHCP-Server ausfindig zu machen
- DHCP-Offer
  Ein DHCP-Server antwortet dem Client und bietet ihm eine Konfiguration an
- DHCP-Request
  Der Client geht auf das Angebot des Servers ein und fordert die Konfigurationsinformationen an
- DHCP-Ack
  Der Server teilt dem Client die Konfiguration zu

Achten Sie bei der ARP-Auflösung ob Anfragen beantwortet werden (In der Regel gibt es zu jeder Anfrage im Erfolgsfall eine Response.), unbeantwortet bleiben oder ob nicht sinnvolle oder auffällige ARP-Pakete im Mitschnitt zu finden sind.
Tauchen DHCP-Offers oder ARP-Responses auf, die nicht zu Ihrer Netzwerkkonfiguration passen, sollten Sie diesen nachgehen.

IP

Bei der Fehlersuche auf IP-Basis stellt sich zuerst die Frage, ob die Übertragung der Informationen vollständig ist. Hierfür zeigt Ihnen Wireshark in der IP-Dissektion die Felder Identification und Fragment offset an. Mit diesen Informationen können Sie nachvollziehen, ob alle Pakete vorhanden sind und sich korrekt zusammensetzen lassen. Hierbei kann es hilfreich sein, diese Information über das Kontextmenü als Spalte einblenden zu lassen.
Zudem können Sie, wenn eine Verbindungsaufnahme gar nicht zustande kommt, anhand der versendeten Pakete Konfigurationsfehlern auf die Spur kommen. Ist beispielsweise die Subnetzmaske falsch vergeben, oder das falsche Gateway

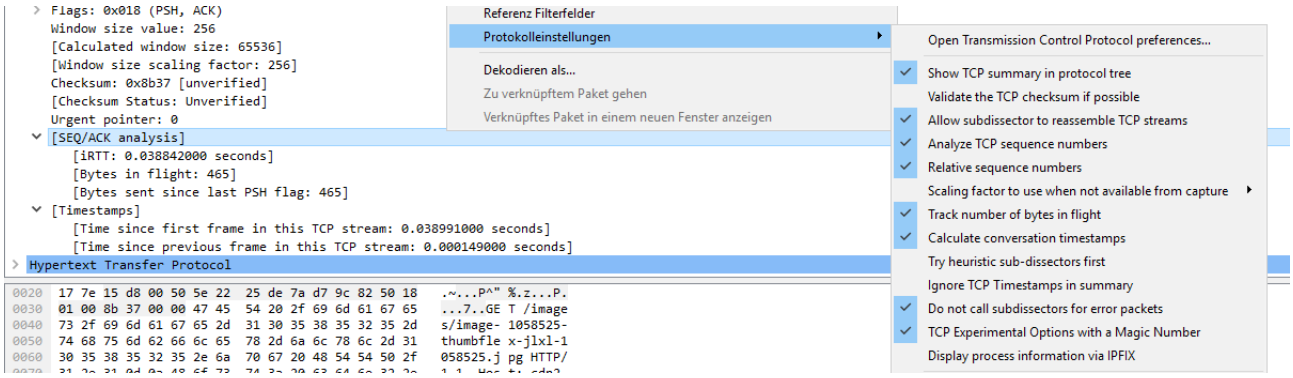
eingestellt, lässt sich dies mit Wireshark schnell erkennen. Auch fehlerhafte Routing-Einträge können unter Umständen detektiert werden. Achten Sie dabei auch auf ICMP-Redirects.

TCP

Auf auf TCP-Ebene können Probleme erkennbar sein, die die ursächlich für eine nicht funktionierende Verbindung sind. Achten Sie z.B. auf unbeantwortete SYN-Pakete, welche auf gescheiterte Verbindungsversuche hinweisen, beispielsweise mit folgendem Filter:

```
tcp.flags == 0x02 && tcp.analysis.retransmission
```

Ist die Kommunikation ungewöhnlich langsam oder ergeben sich immer wieder lange Wartezeiten, kann es hilfreich sein von Wireshark die Zeitverhältnisse zwischen den Paketen berechnen zu lassen. Im Kontextmenü zu dem Bereich SEQ/ACK analysis in der TCP-Dissektion, kann diese Berechnung aktiviert werden.



Zeitstempel im TCP-Datenverkehr

Zur besseren Übersicht kann es sinnvoll sein einige Informationen wie z.B. Stream Index, Sequenznummer, nächste Sequenznummer, ACK-Nummer, Fenstergröße, Bytes, RTT oder auch die soeben berechneten Zeitangaben in der Paketliste als zusätzliche Spalten anzeigen zu lassen. Für einige Protokolle sind zusätzliche Zeitangaben verfügbar, wie z.B. `http.time`, `dns.time` oder `tcp.time_delta`. Bei der Arbeit mit speziellen zusätzlichen Spalten ist die Verwendung eines gesonderten Profils angebracht.

Zeigt Wireshark in der Paketliste Pakete mit roter Schrift auf schwarzem Grund mit der Information „Previous Packet not captured“, so hat er festgestellt, dass ein Paket nicht die nächste zu erwartende Sequenznummer aufweist und schließt daraus, dass er Pakete verpasst hat. Erfolgt darauf keine erneute Übertragung durch den Absender und wird die Kommunikation fortgesetzt, hat der Empfänger das Paket wahrscheinlich erhalten, Wireshark jedoch nicht.

HTTP

Die Ursache für Verbindungsprobleme können auch auf Applikationsprotokoll-ebene begründet sein. Mit seinen zahlreichen Dissektoren kann Wireshark auch hier gute Dienste bei der Fehlersuche leisten. Beispielsweise kann bei Problemen mit HTTP-Datenverkehr die Auswertung der Protokollinformationen Aufschluss geben. Der Filter

```
http.response.code != 200
```

liefert z.B. alle Pakete, die kein OK erhalten haben. Die Filter

```
http.response.code >= 500
http.response.code <500 && http.response.code >= 400
```

liefern alle Pakete zurück, bei denen ein Serverfehler bzw. ein Problem auf der Clientseite aufgetreten ist. Für manche Protokolle, so auch für HTTP, gibt es im Statistiken-Menü weitere Auswerteoptionen. So kann man sich darüber z.B. alle mitgeschnittenen Requests in einer Übersicht anzeigen lassen.

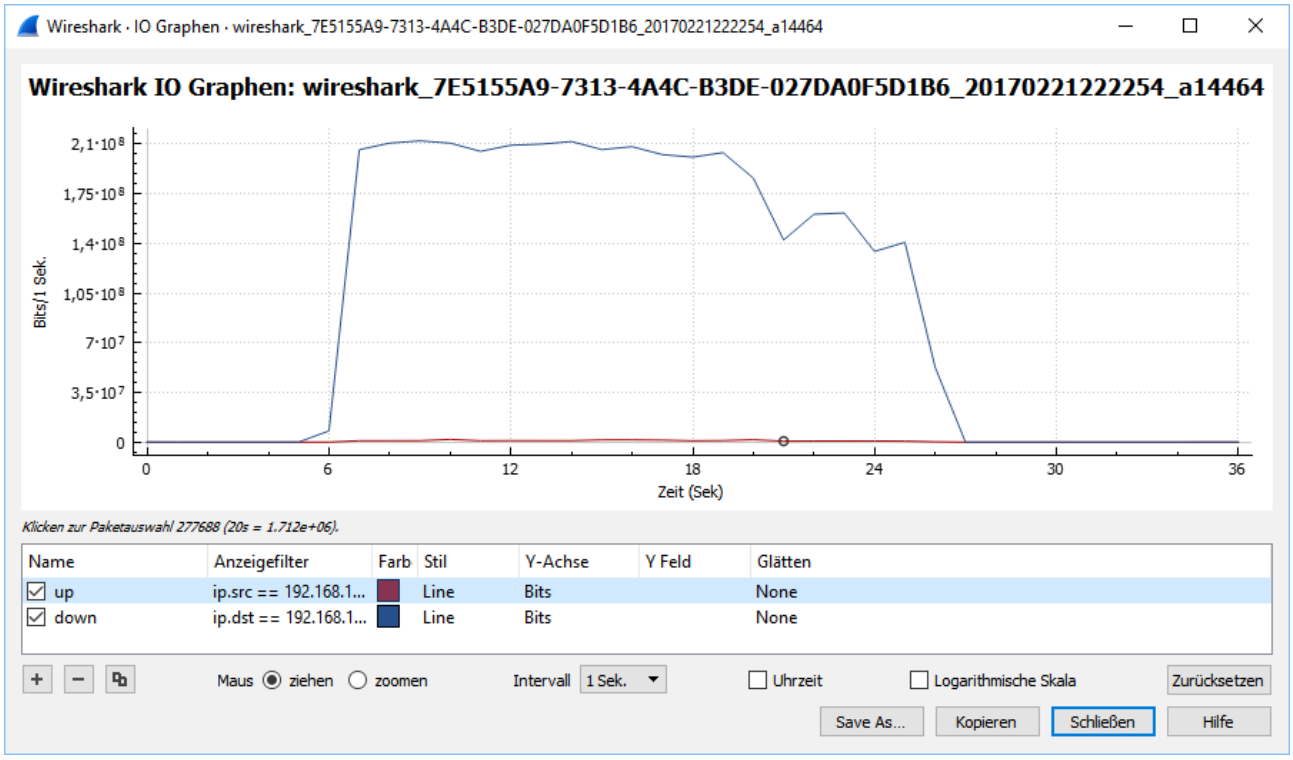
Protokollauflösung

Interpretiert Wireshark den Inhalt von Paketen fälschlicherweise mit einem Dissektor, der nicht zum enthaltenen Protokoll passt, besteht die Möglichkeit, diesen abzuschalten. Im Menü „Analyse“ befindet sich der entsprechende Eintrag.
Dieses Verhalten lässt sich auch beeinflussen über das Kontextmenü. Mit dem Eintrag „Dekodieren als“ kann man bestimmte Paketeigenschaften als Indikator verwenden, um bei deren Zutreffen einen anderen Dissektor zu wählen. So kann man z.B. festlegen, dass Pakete, die an den UDP-Port 53 gerichtet sind, nicht mehr anhand des DNS-Protokolls interpretiert werden sollen, sondern anhand

etwas anderem.

Bandbreitenengpässe

Um Bandbreitenengpässe erkennen zu können, kann es hilfreich sein, eine Auswertung mit Hilfe des I/O-Graphen durchzuführen. Hierzu wählt man einen geeigneten Filterausdruck, ein Interval von einer Sekunde und die Einheit Bits als Maß. Dadurch erreicht man eine Darstellung des ausgewählten Verkehrs in Bit pro Sekunde über den angezeigten Zeitverlauf. Im unten abgebildeten Beispiel wird bei einem Download die maximale Bandbreite von 200 MBit/s erreicht.



Sättigung der Downloadbandbreite bei 200 MBit/s