Wireshark

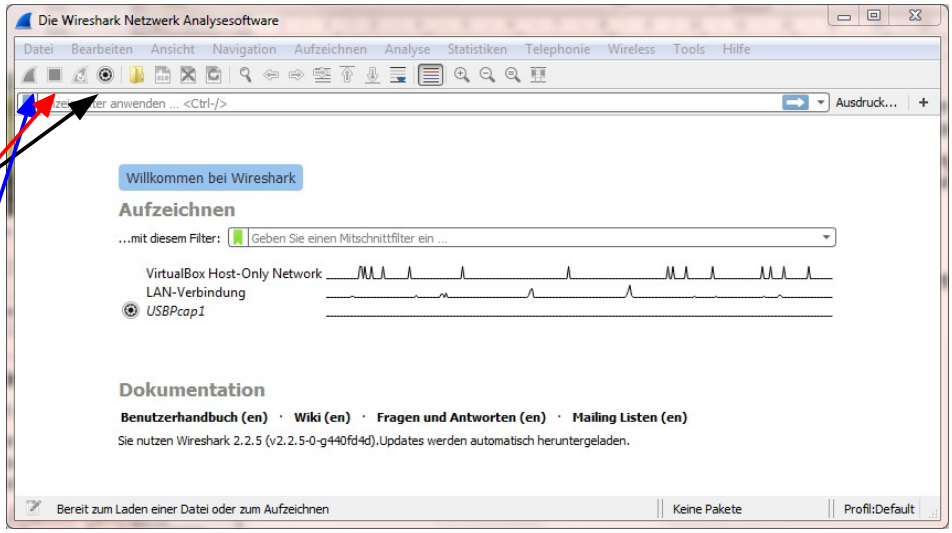
Für die Analyse von Netzwerkkommunikation und die Fehlersuche in Netzwerken kann man sogenannte Sniffer verwenden, die den Netzwerkverkehr einer Netzwerkkarte protokollieren.

Ein bekanntes Open Source-Produkt ist Wireshark[1]. In den nachfolgenden Übungen sollen Sie mit diesem Programm den Netzwerkverkehr auf der Netzzugangsschicht untersuchen.

Zuvor eine kurze Einführung in das Programm!

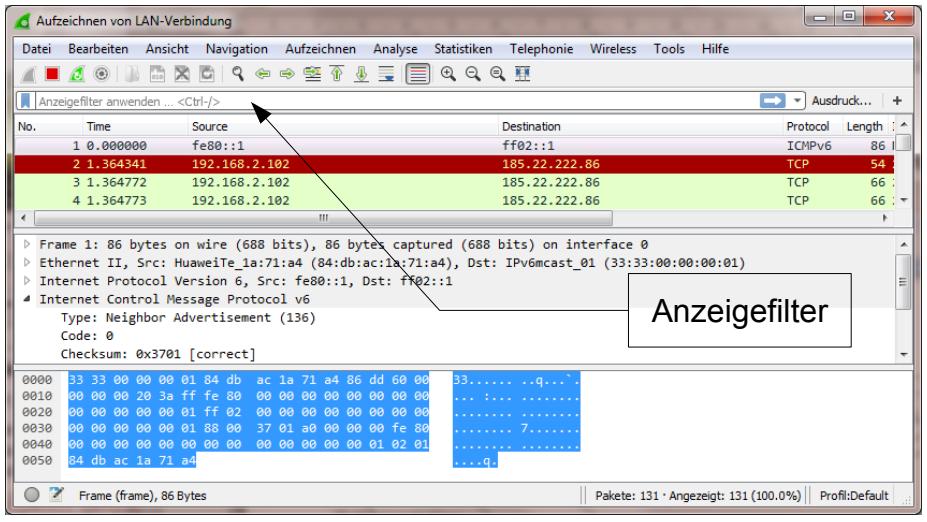
Einführung in Wireshark

In der aktuellen Version[2] präsentiert sich das Programm mit dem folgenden Startbildschirm:



Durch einmaliges Anklicken der „LAN-Verbindung“ wird die betreffende Netzwerkkarte ausgewählt. Durch einen Klick auf das Zahnradsymbol können die Einstellungen verändert werden.

Ein Klick auf die blaue „Haifischflosse“ startet einen Mitschnitt des Datenverkehrs auf dem ausgewählten Netzwerkinterface. Ein Klick auf das dann rot dargestellte Quadrat stoppt den Mitschnitt. Mitschnitte können gespeichert und für eine spätere Analyse wieder geladen werden.



Nach dem Starten eines Mitschnitts wird das Fenster dreigeteilt. Im oberen Drittel werden alle Ethernet-Frames mit einigen Informationen wie Quelle, Ziel, Protokoll etc. dargestellt.

Im mittleren Drittel wird für einen oben ausgewählten Rahmen die detaillierte Information angezeigt. Die Anzeige erfolgt hierarchisch entlang der Schichten im TCP/IP-Modell. Durch Aufklappen können die jeweiligen Detailinformationen betrachtet werden. Im unteren Drittel werden die betreffenden Daten hexadezimal bzw. im ASCII-Code dargestellt. Wählt man im mittleren Drittel eine bestimmte Information aus, wird diese im unteren Drittel farblich hervorgehoben.

1 **http://www.wireshark.org/**

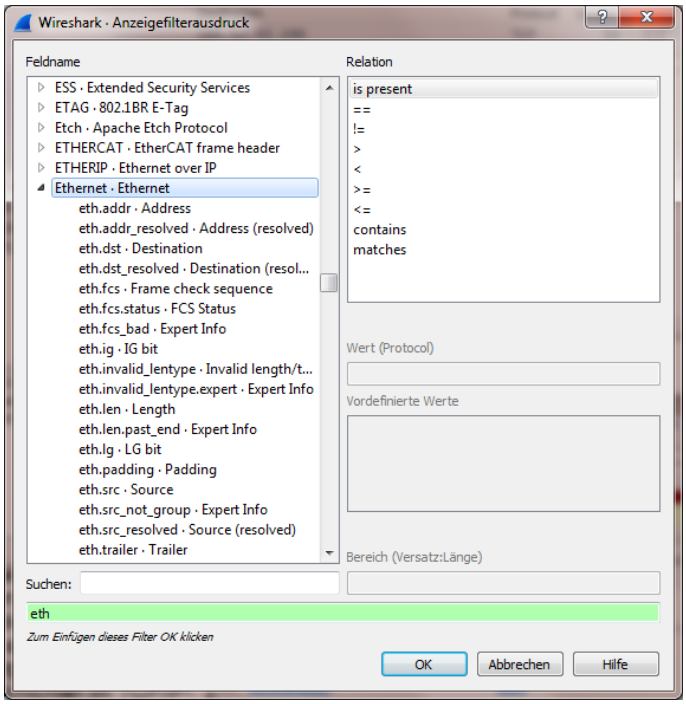
2 Version 2.2.5 am 27. März 2017

Filterung der Daten

Um in der Datenflut den Überblick zu behalten und um lediglich relevante Daten angezeigt zu bekommen, verfügt Wireshark über Anzeigefilter.

Ein Anzeigefilter-Ausdruck kann entweder direkt in der betreffenden Zeile eingetragen oder mittels Dialog zusammen geklickt werden. Das Dialogfenster öffnet man durch die Schaltfläche rechts von der Eingabezeile für Filterausdrücke.

Im Dialogfenster erscheint eine sehr lange Liste von Protokollen, von denen für Protokolleigenschaften bestimmte Vergleichswerte eingetragen werden können. Mehrere Filterausdrücke können durch Logikoperatoren kombiniert werden.



Beispiel

Es sollen nur die Daten angezeigt werden, die mittels der Netzwerkkarte mit der MAC-Adressen **`00-1A-DE-F5-37-2C`** ausgetauscht wurden.

In der Kategorie **Ethernet** kann man nun auswählen, dass die anzuzeigenden Daten diese MAC-Adresse als Quelle oder als Ziel enthalten müssen. Der Filterausdruck wäre also:

`eth.addr == 001ADEF5372C`

Es lässt sich auch leicht nach Protokollen filtern, in dem man den Namen des Protokolls als Filterausdruck verwendet; z.B. zeigt „**`http`**“ lediglich Datenrahmen, in denen HTTP verwendet wird.

Es können auch mehrere Ausdrücke mit Logik-Operatoren verknüpft werden:

Beispiel: **`http && ip.addr==131.169.180.47`**

Übungen

1. Machen Sie sich mit der Bedienoberfläche von Wireshark etwas vertraut. Starten Sie Mitschnitte und sehen Sie sich die dargestellten Daten an. Wählen Sie ein beliebiges Paket im oberen Drittel, schauen Sie, welche Informationen im mittleren und unteren Drittel angezeigt werden.
2. Starten Sie einen neuen Mitschnitt und rufen Sie die Webseite **`http://www.desy.de`** auf. Stoppen Sie anschließend den Mitschnitt. Tragen Sie als Anzeigefilter **`http`** ein.

   Identifizieren Sie die IP von **`www.desy.de`** sowie die Portnummer.
3. Wählen Sie im oberen Drittel eine Zeile mit der Angabe „HTTP“ in der Spalte „Protocol“ aus und öffnen Sie per Rechtsklick das Kontextmenü. Wählen Sie den Eintrag „Folgen“ sowie „HTTP-Stream“. Es öffnet sich nun ein Fenster, in dem Sie den gesamten HTTP-Verkehr lesen können (in rot: Client, in blau: Server)

   Ermitteln Sie den Namen des Webserver-Programms und die genannte Linux-Distribution.