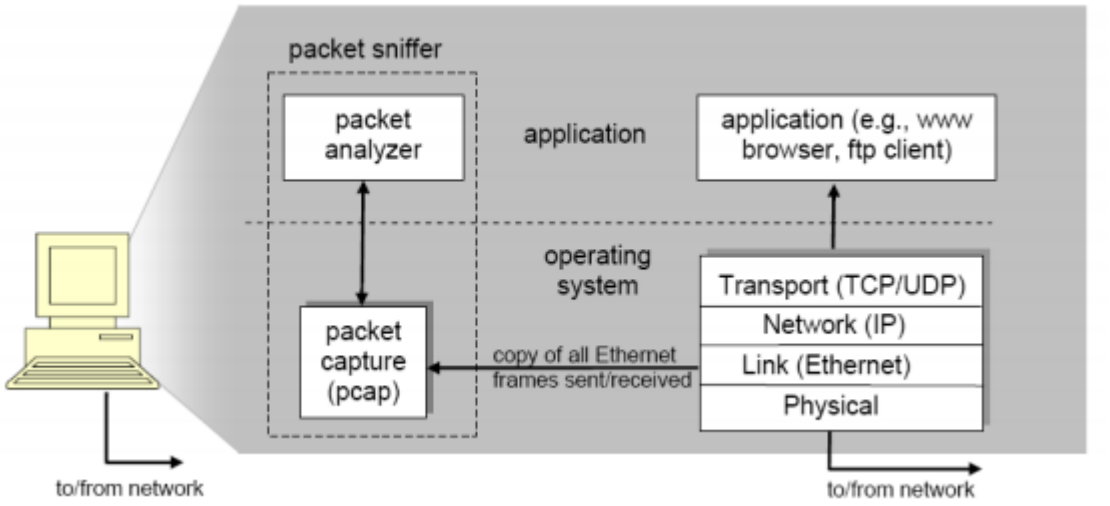
Netzwerkanalyse mit Wireshark

Das Monitoring inklusive der notwendigen Detailanalyse des Datenverkehrs im Netzwerk ist ohne ein leistungsfähiges Analysesystem unmöglich. Eines der **wichtigsten Netzwerktools** für jeden **Administrator** ist **Wireshark** – ein Open Source-Netzwerkanalysator, mit dem Sie alle **Pakete im Netzwerk aufzeichnen** und die Paketinhalte detailliert analysieren.

Packet Sniffer

Das grundlegende Werkzeug für die Beobachtung von Daten zwischen Rechnern wird als **packet sniffer** bezeichnet. Wie der Name schon sagt, **fängt** dieses Werkzeug **empfangene/gesendete Daten** Ihres Rechners **ab**. Ein Sniffer ist immer **passiv**, das heißt er v**erschickt keine Daten**, sondern s**peichert Kopien der Daten** der Kommunikation auf Ihrem Rechner.



Das Bild 1 zeigt die Struktur eines „Sniffers“. Rechts unten im Bild sind die beteiligten Protokolle abgebildet, es werden also Protokolle der Layer 1 bis 4:

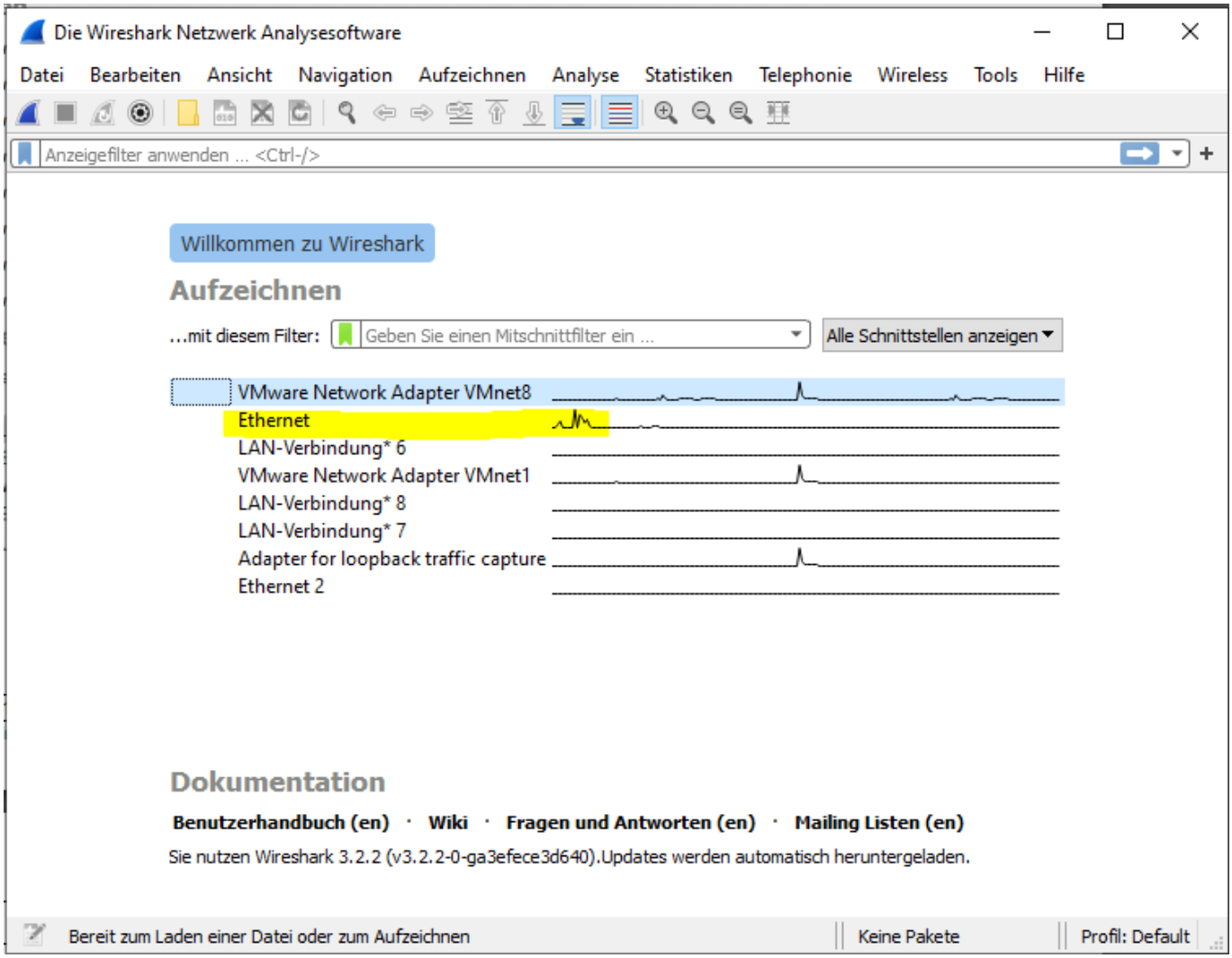
- oben ist die Applikation zu sehen, in unserem Fall ist dies der Webbrowser (Firefox, IE).
- die Blöcke die in den gestrichelten Linien eingerahmt sind gehören zu unserem „Sniffer“.

Am einfachsten lässt sich ein Netzwerk sniffen wenn Hubs als Verbindung der Netzwerkssegmente zwischengeschaltet sind. Bei anderen Verbindungen wie z.B. bei einem Switch bekommt man im Normalfall Probleme den Netzwerkverkehr abzuhören, da der Switch die Daten vom Sender nur an den tatsächlichen Empfänger weiterleitet. Somit würde man nur die eigenen Daten, sowie unwichtigeren Netzwerkverkehr wie z.B. Broadcasts aufzeichnen. Für diesen Fall haben viele Hersteller dieser Komponenten **Switches** bzw. **Router** mit einer **Monitorfunktion** in Ihrem Portfolio. Damit ist es möglich Netzwerkdaten eines gewünschten Ports auf einen anderen zu spiegeln. Auf diesen gespiegelten Port kann man nun direkt zugreifen.

Einführung in Wireshark

Startet man das Programm, muss man zuerst eine Schnittstelle (z.B.: Ethernet) wählen, die man

abhören möchte:

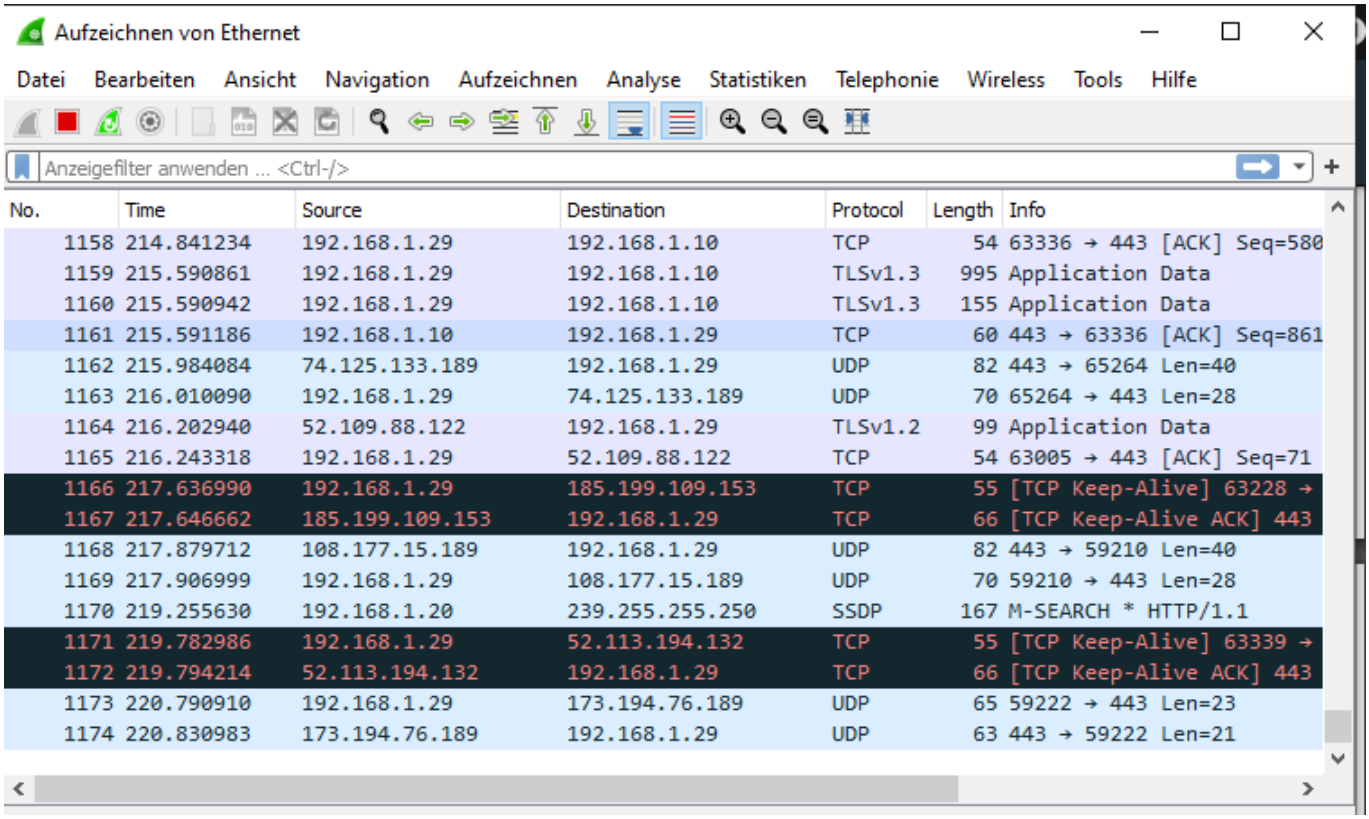


Der Bildschirm, in dem die aufgezeichneten Daten bearbeitet und analysiert werden ist in 3 Bereiche aufgeteilt:

1) Paketliste

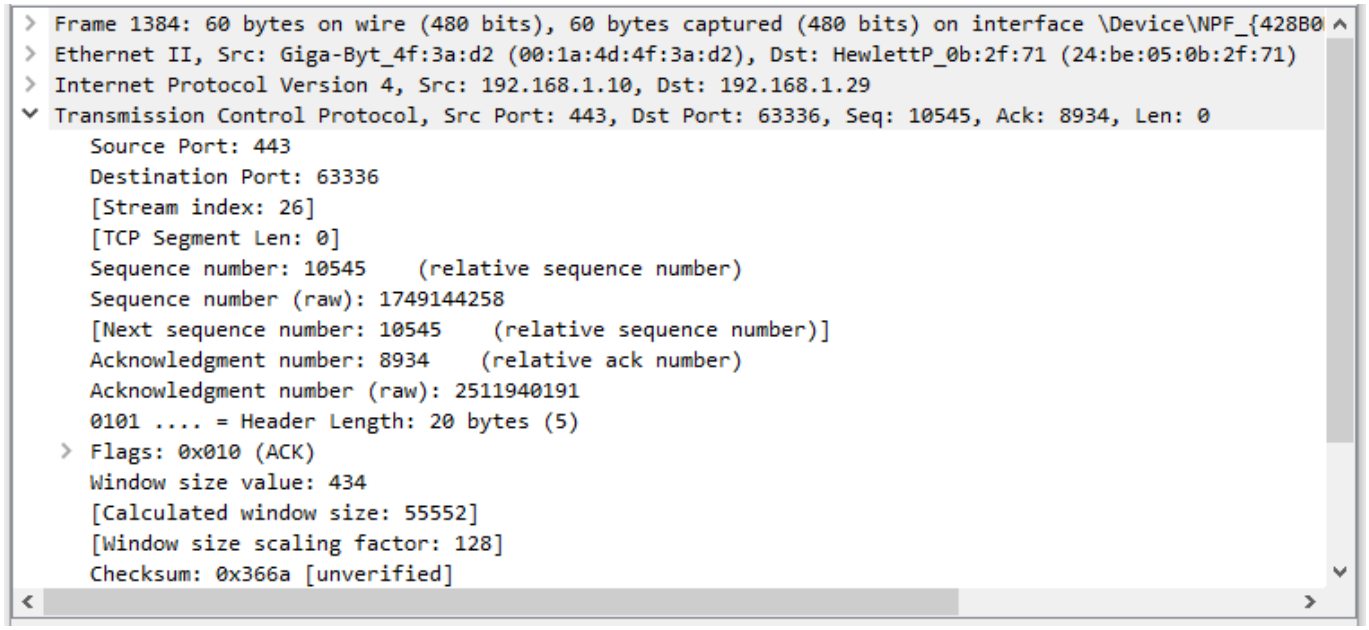
In der Paketliste, sieht man alle aufgezeichneten Frames. Folgende Spalten werden standardmäßig angezeigt:

1. No. = ist eine fortlaufende Nummerierung der Frames 2. Time = zeigt den Zeitabschnitt der Aufzeichnung an 3. Source = zeigt den Absender eines Frames an (meist die IP) 4. Destination = zeigt den Empfänger des Frames an (meist die IP) 5. Protocol = zeigt das verwendete Protokoll des Frame an 6. Info = gibt zusätzliche Informationen zum Frame bekannt



2) Paketdetails

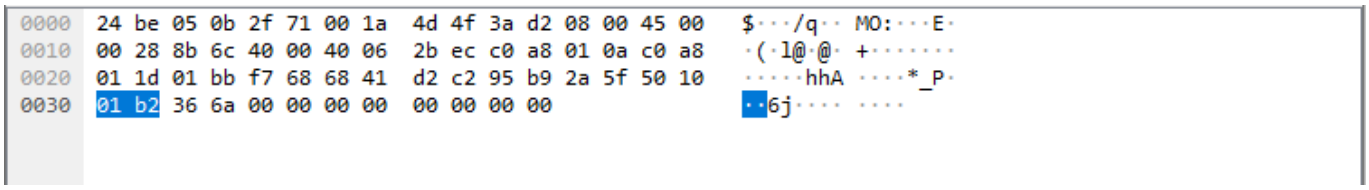
In den Paketdetails werden die OSI-Layer (Schichten) des Datenframes angezeigt. Durch anklicken des Pfeil-Symbols kann der gewählte Layer erweitert werden.



Natürlich variieren die Protokolldetails von Protokoll zu Protokoll. Nur die ersten 2 Schichten sind immer vorhanden.

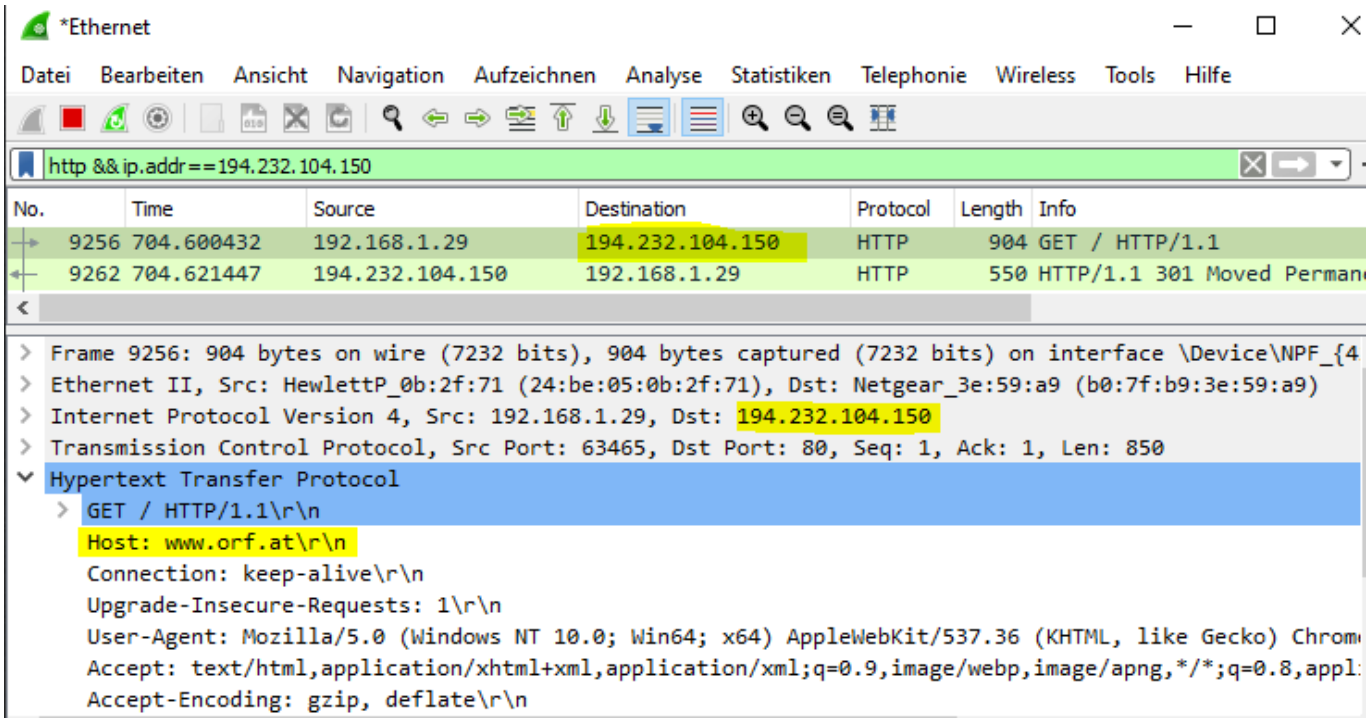
3) Paketdaten (Hexadezimal)

Hier sind die Daten einmal im Hexadezimalsystem (links) und nebendran im Klartext (rechts) bzw. in entschlüsselter Form angezeigt.



Filter

Nachdem praktisch ständig Netzwerkpakete gesendet und empfangen werden, ist es wichtig, dass es Möglichkeit gibt, um den Netzwerktraffic zu filtern. In dem in der Abbildung gezeigten Textfeld können beliebige Filter eingestellt werden.



Im obigen Beispiel wurden nur http-Pakete mit der IP-Adresse 194.232.104.150 angezeigt. Wie man in der Abbildung erkennen kann, ist/war dies die IP-Adresse der Internetseite www.orf.at. Da http natürlich das TCP-Protokoll, IP-Protokoll & Ethernet-Protokoll nutzt, werden auch diese Daten angezeigt.