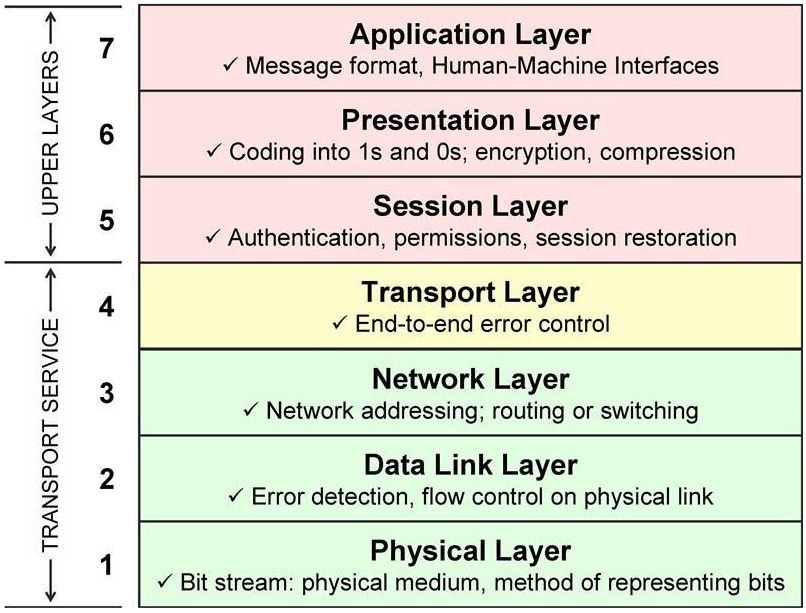
Das OSI-Referenzmodell

Um die Komplexität des Datenaustauschs zu vereinfachen, wurde das OSI-Schichten-Modell in sieben Schichten unterteilt.



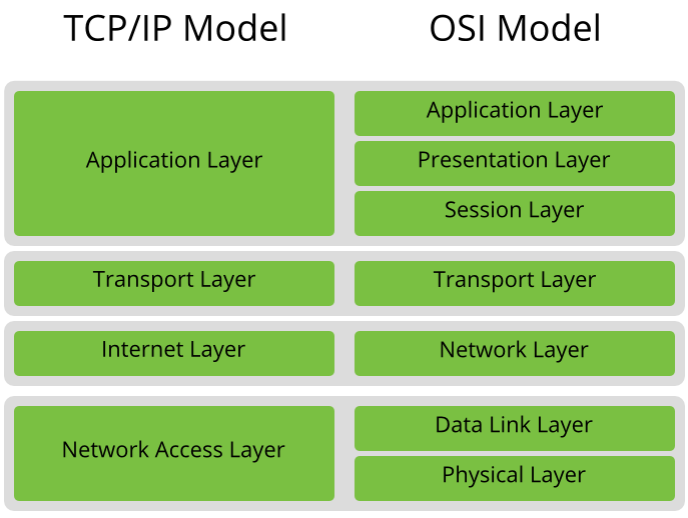
Die Schichten 1 bis 4 gehören zum **Transportsystem**. Die Schichten 5-7 sind **anwendungsorientierte Schichten**. Jede Schicht behandelt eine Anforderung, die für eine funktionierende Kommunikation erfüllt werden muss.

Es gibt einige Eselsbrücken/Informatik-Merksprüche zu den Namen der einzelnen OSI-Schichten z.B. *"**P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way"* (*Physical Layer*, *Data Link Layer* usw.), oder in umgekehrter Reihenfolge: „**A**ll **P**eople **S**eem **t**o **N**eed **D**ata **P**rocessing".

Im Rahmen dieses Kurses interessieren wir uns hauptsächlich für das Transportsystem (Schichten 1-4).

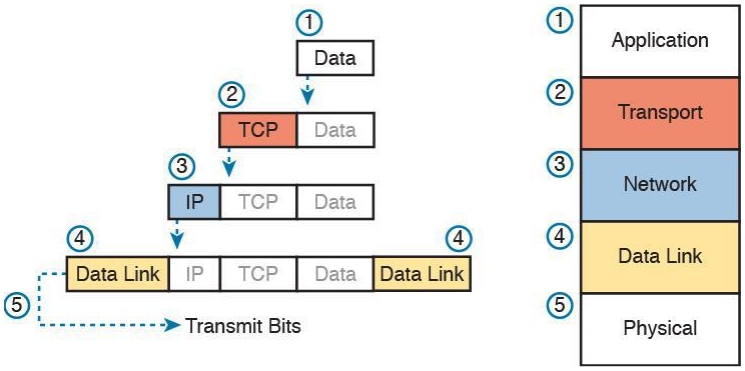
Das TCP/IP - Modell

Das TCP/IP-Modell ist ein weiteres Referenzmodell, benannt nach den beiden primären Protokollen TCP und IP. Es ist zeitlich vor dem OSI-Referenzmodell entstanden, deshalb sind auch die Erfahrungen des TCP/IP-Modells mit in die OSI-Standardisierung eingeflossen. Das TCP/IP-Referenzmodell besteht im Gegensatz zum OSI-Modell aus nur vier Schichten: Application Layer, Transport Layer, Internet Layer, Network Layer.



Wenn ein Computer (Host A) Daten an einen anderen Computer (Host B) senden will, müssen die Daten zunächst zu Datenpaketen gepackt werden. Dieser Vorgang wird **Kapselung** genannt. Bei der Kapselung werden Daten vor der Übertragung über das Netz in die benötigten Protokollinformationen eingeschlossen. Zu diesem Zweck wird das Datenpaket, während es die verschiedenen Schichten des OSI-Modells durchläuft, mit Headern, Trailern und weiteren Angaben versehen.

Eine Information kann z. B. in einem LAN abgesendet werden, dann ins Internet weitergeleitet werden und schließlich ihr Ziel in einem anderen entfernten LAN erreichen. Während die Daten die Schichten des OSI-Modells durchlaufen, werden Header und Endmarken hinzugefügt. Um eine zuverlässige Kommunikation über ein Netz zu ermöglichen, müssen zu versendende Daten in Pakete verpackt werden Die obersten drei Schichten (Schichten 5-7) bereiten die Daten für die Übertragung vor, indem sie sie in ein allgemein gebräuchliches Übertragungsformat überführen.



Die **Transportschicht** teilt die Daten in Einheiten leichter zu verarbeitender Größe auf. Diese Einheiten werden als **Segmente** bezeichnet. Außerdem weist sie den Segmenten Segmentnummern zu, um sicherzustellen, dass der empfangende Host die Daten wieder in der richtigen Reihenfolge zusammensetzen kann. Die **Vermittlungsschicht** kapselt das Segment anschließend in einem **Paket**. Schließlich wird das Paket von der Vermittlungsschicht noch mit einer Ziel- und Quellnetzwerkadresse (in der Regel eine IP-Adresse) versehen.

Die **Sicherungsschicht** kapselt das Paket weiter und erstellt einen **Frame**. Dem Frame wird die lokale Quell- und Zieladresse (MAC-Adresse) hinzugefügt. Anschließend überträgt die Sicherungsschicht die binären Bits des Frames über die Medien der Bitübertragungsschicht.

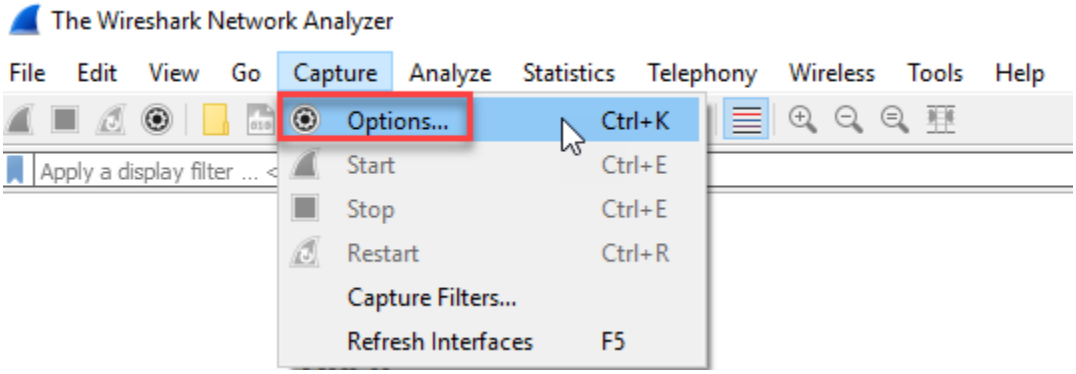
Weitere Infos: https://www.youtube.com/watch?v=TcIV_qc-eOU

Praktische Übung

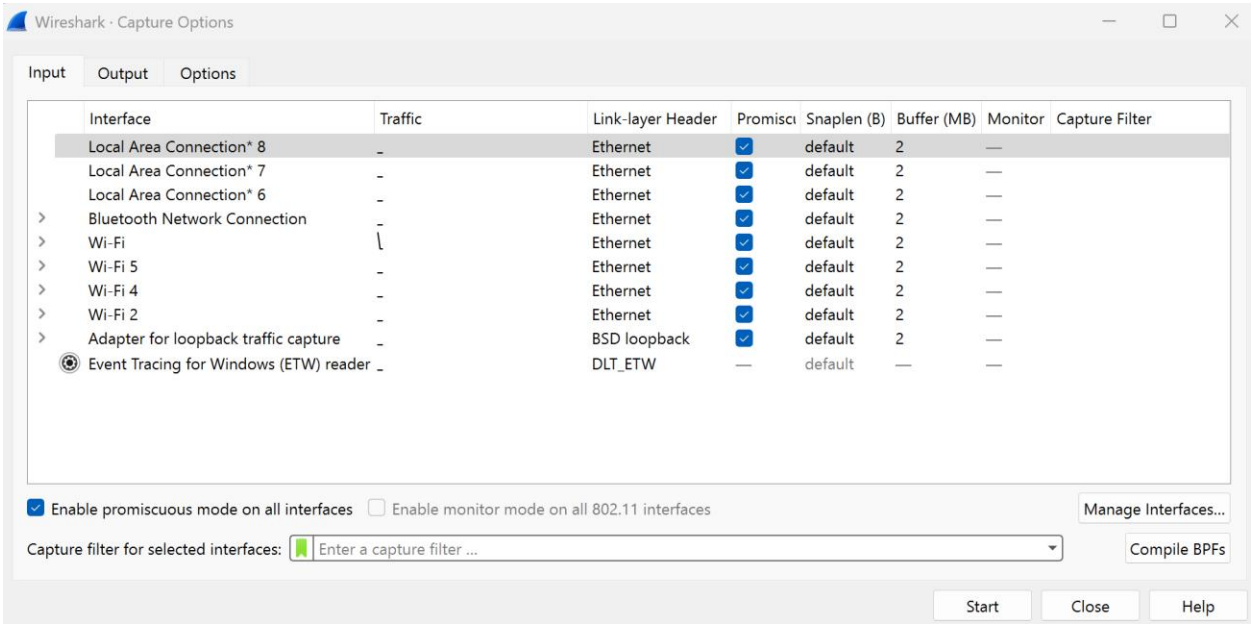
Lade die Software Wireshark herunter.

Wireshark ist ein Werkzeug zur Netzwerküberwachung, das es uns ermöglicht, alle Pakete, die wir auf unserem Computer empfangen oder senden, zu erfassen. Wir können sie uns dann ansehen. Sobald du Wireshark heruntergeladen und installiert hast, wähle im Erfassungsmenü die „**Options**“ aus.

Sobald Sie Wireshark heruntergeladen und installiert haben, wählen Sie im Menü „**Capture**“ die Option „**Options**“.

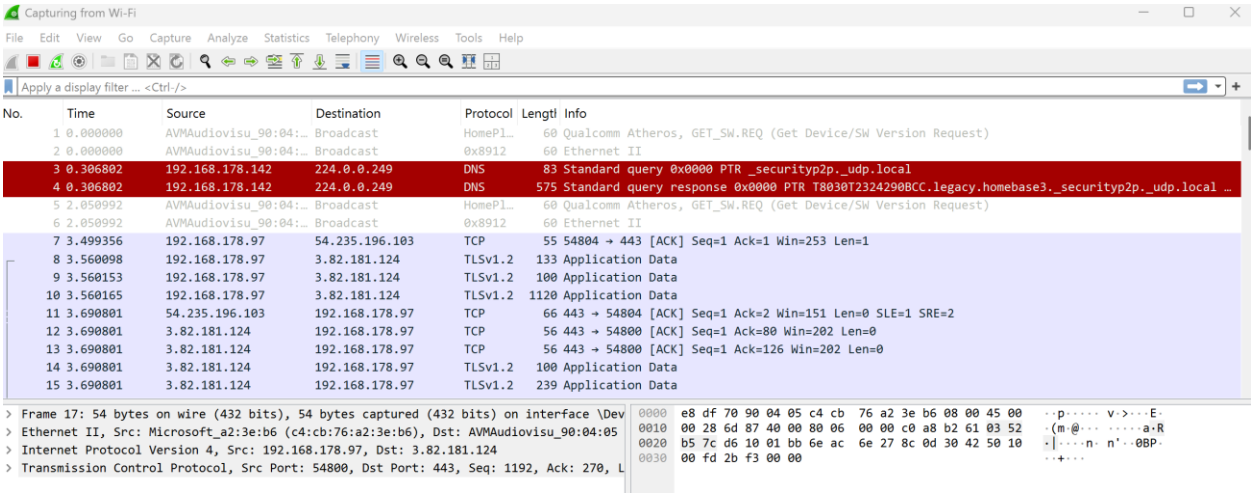


Sie werden nun eine Übersicht über alle Ihre Netzwerkkarten sehen:

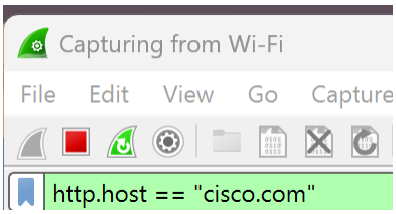


In meinem Fall ist es die Ethernet-Schnittstelle, die ich erfassen möchte. Klicken Sie auf Start, und es werden alle Pakete erfasst, die in diese Schnittstelle ein- und austreten.

Es wird so aussehen:



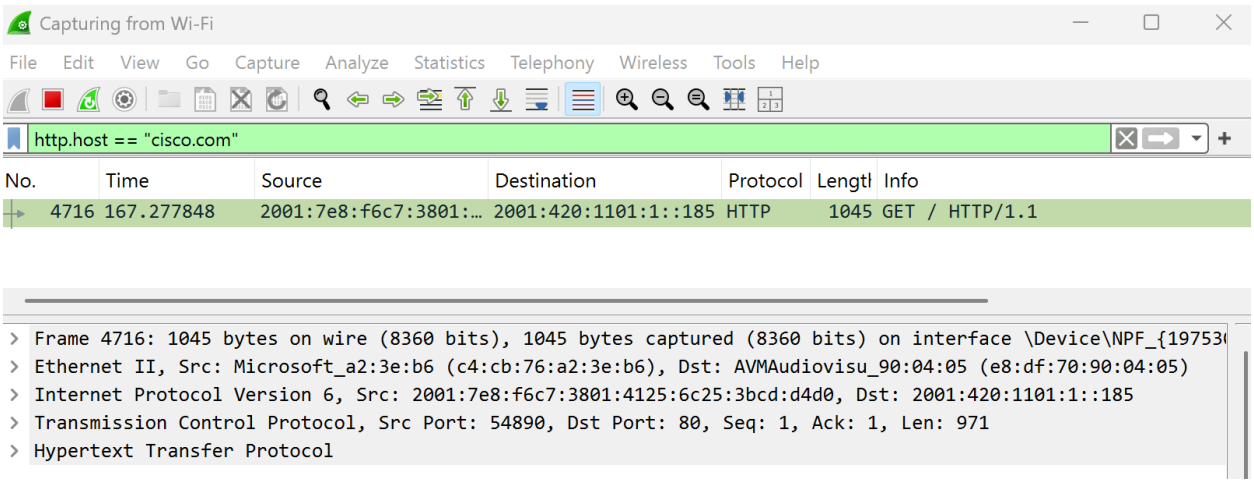
Sie werden viele Dinge sehen, machen Sie sich keine Sorgen darüber, was Sie hier sehen. Wenn Sie mehr über Netzwerke lernen, werden Sie auch mehr über die verschiedenen Netzwerkprotokolle und deren Pakete/Frames erfahren. Wir werden einen einzelnen Frame erfassen und ihn genauer unter die Lupe nehmen. Dazu verwenden wir einen Filter, damit Wireshark nur diesen Verkehr anzeigt:



Geben Sie in der grünen Leiste oben links den folgenden Filter ein.

Öffnen Sie jetzt Ihren Webbrowser und rufen Sie http://cisco.com auf.

Sobald die Webseite geladen ist, werfen Sie einen Blick auf Wireshark:



Ein einzelnes Paket wird mit der Anfrage unseres Browsers angezeigt, um die http://cisco.com Website abzurufen. In der unteren Bildschirmhälfte können wir den Inhalt dieses Frames betrachten.

```
▾ Frame 4716: 1045 bytes on wire (8360 bits), 1045 bytes captured (8360 bits) on interface \Device\NPF_{19753
    Section number: 1
  ▸ Interface id: 0 (\Device\NPF_{19753031-CBD8-4324-BA18-3B831095B28D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 25, 2025 00:07:16.200313000 Romance Standard Time
    UTC Arrival Time: Feb 24, 2025 23:07:16.200313000 UTC
    Epoch Arrival Time: 1740438436.200313000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.149569000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 167.277848000 seconds]
    Frame Number: 4716
    Frame Length: 1045 bytes (8360 bits)
    Capture Length: 1045 bytes (8360 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Wireshark hat die erste Information hinzugefügt. Es zeigt uns, dass wir einen Ethernet-Frame empfangen haben, und gibt zudem die Ankunftszeit an. Hier ist der zweite Teil:

```
▸ Frame 4716: 1045 bytes on wire (8360 bits), 1045 bytes captured (8360 bits) on interface \Device\NPF_{19753
▾ Ethernet II, Src: Microsoft_a2:3e:b6 (c4:cb:76:a2:3e:b6), Dst: AVMAudiovisu_90:04:05 (e8:df:70:90:04:05)
  ▸ Destination: AVMAudiovisu_90:04:05 (e8:df:70:90:04:05)
  ▸ Source: Microsoft_a2:3e:b6 (c4:cb:76:a2:3e:b6)
    Type: IPv6 (0x86dd)
    [Stream index: 2]
▸ Internet Protocol Version 6, Src: 2001:7e8:f6c7:3801:4125:6c25:3bcd:d4d0, Dst: 2001:420:1101:1::185
▸ Transmission Control Protocol, Src Port: 54890, Dst Port: 80, Seq: 1, Ack: 1, Len: 971
▸ Hypertext Transfer Protocol
```

Oben sehen wir die zweite Schicht des OSI-Modells. Das ist der Ethernet-Frame, der die Quell- und Ziel-MAC-Adressen anzeigt. Er gibt auch den Typ an. In diesem Fall enthält unser Ethernet-Frame ein IPv4-Paket. Schauen wir es uns an:

```
▸ Frame 4716: 1045 bytes on wire (8360 bits), 1045 bytes captured (8360 bits) on interface \Device\NPF_{19753
▸ Ethernet II, Src: Microsoft_a2:3e:b6 (c4:cb:76:a2:3e:b6), Dst: AVMAudiovisu_90:04:05 (e8:df:70:90:04:05)
▾ Internet Protocol Version 6, Src: 2001:7e8:f6c7:3801:4125:6c25:3bcd:d4d0, Dst: 2001:420:1101:1::185
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1110 0110 1010 0110 0001 = Flow Label: 0xe6a61
    Payload Length: 991
    Next Header: TCP (6)
    Hop Limit: 255
  ▸ Source Address: 2001:7e8:f6c7:3801:4125:6c25:3bcd:d4d0
  ▸ Destination Address: 2001:420:1101:1::185
    [Stream index: 51]
▸ Transmission Control Protocol, Src Port: 54890, Dst Port: 80, Seq: 1, Ack: 1, Len: 971
▸ Hypertext Transfer Protocol
```

Oben sehen wir das IP-Paket. Dies ist die dritte Schicht des OSI-Modells. Machen Sie sich keine Sorgen um die verschiedenen Felder hier – wir werden sie später behandeln. Zwei Dinge, die Sie oben erkennen können, sind die Quell- und Ziel-IP-Adressen. Lassen Sie uns weitermachen:

```
▾ Transmission Control Protocol, Src Port: 54890, Dst Port: 80, Seq: 1, Ack: 1, Len: 971
    Source Port: 54890
    Destination Port: 80
    [Stream index: 96]
    [Stream Packet Number: 4]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 971]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 677478523
    [Next Sequence Number: 972    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3766771591
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0x4f28 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (971 bytes)
```

Oben sehen wir die vierte Schicht des OSI-Modells. Hier verwenden wir TCP als Transportprotokoll (das wir später detailliert besprechen werden). Nicht zuletzt, die letzte Schicht des OSI-Modells:

```
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: cisco.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatior
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,fr;q=0.8,de;q=0.7\r\n
  ▸ […]Cookie: utag_main=v_id:01953a36ac69001166597bd424340506f001606700978$_sn:1$_se:2$_ss:0$_st:1740440219390$ses_id:
    \r\n
    [Response in frame: 4724]
    [Full request URI: http://cisco.com/]
```

Oben sehen Sie Schicht sieben, die Anwendungsschicht. Beachten Sie, dass hier keine separate Sitzung- oder Darstellungsschicht angezeigt wird. Einige Informationen zum HTTP-Protokoll sind hier zu erkennen. Wir haben eine GET-Anfrage verwendet, um cisco.com abzurufen; als User Agent habe ich Mozilla (Firefox) genutzt.

Fazit

Sie haben nun das OSI-Modell und seine verschiedenen Schichten kennengelernt. Außerdem haben Sie gesehen, wie dies in der Praxis angewendet wird – anhand einer Paketerfassung in Wireshark. In weiteren Lektionen werden Sie feststellen, dass wir Wireshark häufig nutzen, um verschiedene Netzwerkprotokolle und deren innere Funktionsweise zu untersuchen.