

Aufgabe 1: Protokoll-Header

Ich habe den Befehl ping ausgeführt und ein ICMP Echo Request in Wireshark gefunden. So kann man den IPv4-Header analysieren:

```
▶ Frame 83: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F8245424-00FE-4520-87F4-B9F953BDFE6E}, id 0
▶ Ethernet II, Src: Intel_a0:00:b4 (00:28:f8:a0:00:b4), Dst: MS-NLB-PhysServer-16_18:b1:1c:44 (02:10:18:b1:1c:44)
▼ Internet Protocol Version 4, Src: 192.168.0.200, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 60
        Identification: 0xa976 (43382)
    ▶ 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 64
        Protocol: ICMP (1)
        Header Checksum: 0xffca [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.200
        Destination Address: 8.8.8.8
        [Stream index: 7]
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d26 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 53 (0x0035)
    Sequence Number (LE): 13568 (0x3500)
    [Response frame: 84]
    ▶ Data (32 bytes)
```

Version: 4, also IPv4

Header Length: 20 bytes

Type of Service (Differentiated Services Field): 0x00, d.h. kein spezieller Dienst

Total Length: 60

Identification: 0xa976 (43382). ID für Fragmentierung

Flags: 0x0, d.h. keine Fragmentierung

Fragment Offset: 0

Time to Live: 64. Die maximale Anzahl an Hops. So lange darf das Paket durchlaufen, bevor es verworfen wird.

Protocol: ICMP (1)

Header Checksum: 0xffca. Prüfsumme für Header

Source Address: 192.168.0.200. Die Quell-IP-Adresse ist meine lokale Adresse.

Destination Address: 8.8.8.8. Die Ziel-IP-Adresse ist ein öffentlicher DNS-Server von Google.

UDP-Header:

```
▶ Frame 40: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{F8245424-00FE-4520-87F4-B9F953BDFE6E}, id 0
▶ Ethernet II, Src: MS-NLB-PhysServer-16_18:b1:1c:44 (02:10:18:b1:1c:44), Dst: Intel_a0:00:b4 (00:28:f8:a0:00:b4)
▼ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 73
        Identification: 0x23ea (9194)
    ▶ 010. .... = Flags: 0x2, Don't fragment
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 64
        Protocol: UDP (17)
        Header Checksum: 0x94a0 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.1
        Destination Address: 192.168.0.200
        [Stream index: 2]
▼ User Datagram Protocol, Src Port: 53, Dst Port: 55844
    Source Port: 53
    Destination Port: 55844
    Length: 53
    Checksum: 0x66f7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Stream Packet Number: 2]
    ▶ [Timestamps]
    UDP payload (45 bytes)
▶ Domain Name System (response)
```

Source Port: 53

Destination Port: 55844

Length: 53

Checksum: 0x66f7

UDP hat nur 4 Felder im Header.

TCP-Header:

```

> Frame 541: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 63919, Dst Port: 49350, Seq: 0, Len: 0
  Source Port: 63919
  Destination Port: 49350
  [Stream index: 198]
  [Stream Packet Number: 1]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1494193195
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0xcf38 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  [Timestamps]
```

Source Port: 63919

Destination Port: 49350

Sequence Number: 0

Acknowledgment Number: 0

Flags: 0x002 (SYN). Verbindungsaufbau

Window: 65535

Checksum: 0xcf38

Urgent Pointer: 0

Options: (12 bites), Maximum Segment Size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted