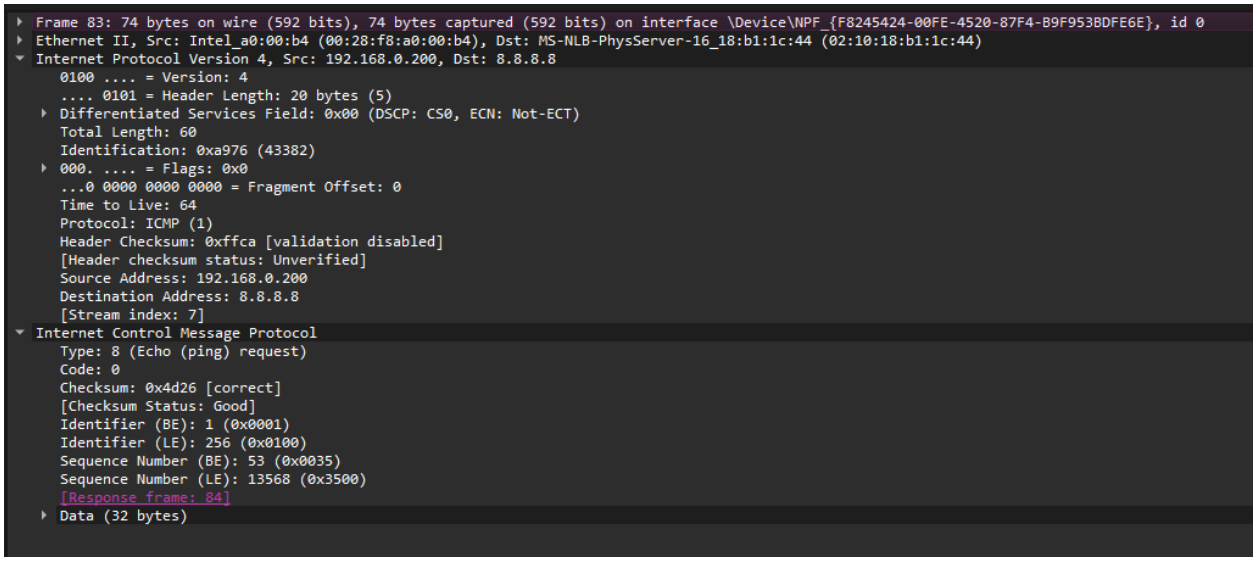
Aufgabe 1: Protokoll-Header

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



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.

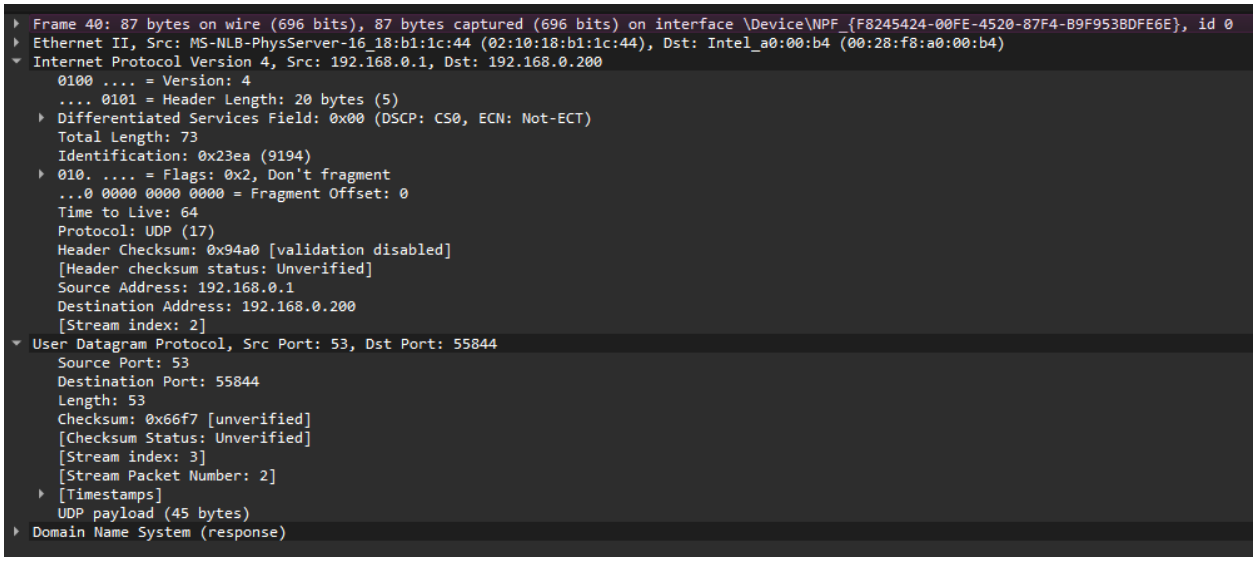
Protocol: ICMP (1)

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:



Source Port: 53

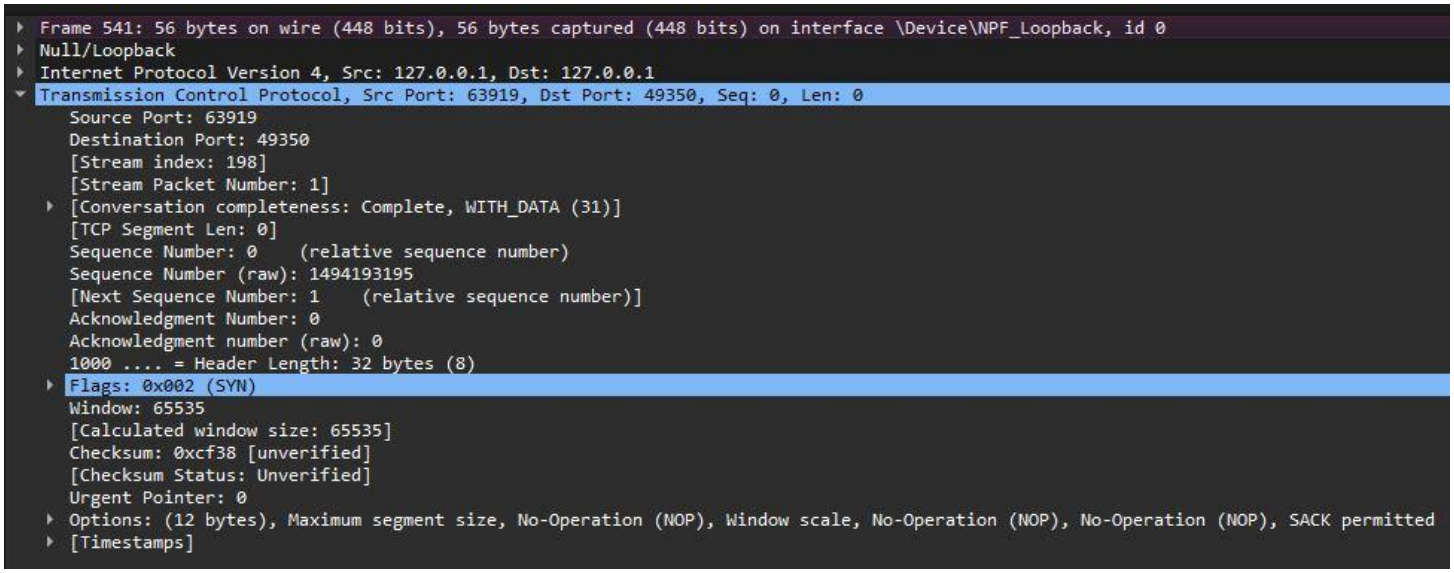
Destination Port: 55844

Length: 53

Checksum: 0x66f7

UDP hat nur 4 Felder im Header.

TCP-Header:



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