

## Frame einer GET-Anfrage des Clients an einen Webserver (Frame-Nr. 2859)

Mitschnitt für Skrip 2020-09-16.pcapng

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

Anzeigefilter anwenden ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

> Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

> Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

> Internet Protocol Version 6, Src: 2a00:20:5027:139d:58f9:6366:4e40:58cd, Dst: 2a02:26f0:ee00::216:f1a0

> Transmission Control Protocol, Src Port: 50619, Dst Port: 80, Seq: 4981, Ack: 989521, Len: 332

> Hypertext Transfer Protocol

```

0000 f8 c3 9e 11 76 99 34 7d f6 5f a9 9c 86 dd 60 0d  ....v.4}  . . . . .
0010 46 c5 01 60 06 41 2a 00 00 20 50 27 13 9d 58 f9  F...A*..P'..X.
0020 63 66 4e 40 58 cd 2a 02 26 f0 ee 00 00 00 00 00  cfn@X.*. &.....
0030 00 00 02 16 f1 a0 c5 bb 00 50 85 cb d4 73 a8 8b  .....P...s..
0040 b0 85 50 18 10 12 5a 49 00 00 47 45 54 20 2f 70  ..P...ZI ..GET /p
0050 72 2f 66 32 65 37 32 34 63 31 2d 37 34 38 66 2d  r/f2e724 c1-748f-
0060 34 62 34 37 2d 38 66 62 38 2d 38 65 30 64 32 31  4b47-8fb 8-8e0d21
0070 30 65 39 32 30 38 2f 4f 66 66 69 63 65 2f 44 61  0e9208/O ffice/Da
0080 74 61 2f 31 36 2e 30 2e 31 30 33 36 36 2e 32 30  ta/16.0. 10366.20
0090 30 31 36 2f 73 74 72 65 61 6d 2e 78 36 34 2e 78  016/stre am.x64.x
00a0 2d 6e 6f 6e 65 2e 64 61 74 20 48 54 54 50 2f 31  -none.da t HTTP/1
00b0 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  .1..Conn ection:
00c0 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65  Keep-Alive..Acce
00d0 70 74 3a 20 2a 2f 2a 0d 0a 52 61 6e 67 65 3a 20  pt: /*.*. Range:
00e0 62 79 74 65 73 3d 31 35 36 36 35 37 32 35 34 34  bytes=15 66572544
00f0 2d 31 35 36 36 36 33 38 30 37 39 0d 0a 55 73 65  -1566638 079..Use
0100 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f  r-Agent: Microso
0110 66 74 2d 44 65 6c 69 76 65 72 79 2d 4f 70 74 69  ft-Deliv ery-Opti
0120 6d 69 7a 61 74 69 6f 6e 2f 31 30 2e 30 0d 0a 4d  mization /10.0..M
0130 53 2d 43 56 3a 20 6b 53 6d 54 34 4d 34 6b 52 30  S-CV: kS mT4M4kR0
0140 43 57 37 36 38 4a 2e 32 2e 37 2e 31 2e 31 2e 31  CW768J.2 .7.1.1.1
0150 31 35 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67  15..Cont ent-Leng
0160 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 66 66  th: 0..H ost: off
0170 69 63 65 63 64 6e 2e 6d 69 63 72 6f 73 6f 66 74  icecdn.m icrosoft
0180 2e 63 6f 6d 2e 65 64 67 65 73 75 69 74 65 2e 6e  .com.edg esuite.n
0190 65 74 0d 0a 0d 0a  et....

```

Mitschnitt für Skrip 2020-09-16.pcapng

Pakete: 3073 · Angezeigt: 3073 (100.0%)

Profil: Default

Abbildung 1: Zusammensetzung des Frames mit Grundinformationen entsprechend der Funktionsweise des TCP/IP-Referenzmodells

\*WLAN

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

▼ Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

- Interface id: 0 (\Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50})
- Encapsulation type: Ethernet (1)
- Arrival Time: Sep 16, 2020 09:35:31.651114000 Mitteleuropäische Sommerzeit
- [Time shift for this packet: 0.00000000 seconds]
- Epoch Time: 1600241731.651114000 seconds
- [Time delta from previous captured frame: 0.001638000 seconds]
- [Time delta from previous displayed frame: 0.001638000 seconds]
- [Time since reference or first frame: 10.366197000 seconds]
- Frame Number: 2859
- Frame Length: 406 bytes (3248 bits)
- Capture Length: 406 bytes (3248 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]
- Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

```

0000 f8 c3 9e 11 76 99 34 7d f6 5f a9 9c 86 dd 60 0d  ....v.4} ._. ....
0010 46 c5 01 60 06 41 2a 00 00 20 50 27 13 9d 58 f9  F...`A* . P'..X.
0020 63 66 4e 40 58 cd 2a 02 26 f0 ee 00 00 00 00 00  cfn@X.*. &.....
0030 00 00 02 16 f1 a0 c5 bb 00 50 85 cb d4 73 a8 8b  .....P...s...
0040 b0 85 50 18 10 12 5a 49 00 00 47 45 54 20 2f 70  ..P...ZI ..GET /p
0050 72 2f 66 32 65 37 32 34 63 31 2d 37 34 38 66 2d  r/f2e724 c1-748f-
0060 34 62 34 37 2d 38 66 62 38 2d 38 65 30 64 32 31  4b47-8fb 8-8e0d21
0070 30 65 39 32 30 38 2f 4f 66 66 69 63 65 2f 44 61  0e9208/O ffice/Da
0080 74 61 2f 31 36 2e 30 2e 31 30 33 36 36 2e 32 30  ta/16.0. 10366.20
0090 30 31 36 2f 73 74 72 65 61 6d 2e 78 36 34 2e 78  016/stre am.x64.x
00a0 2d 6e 6f 6e 65 2e 64 61 74 20 48 54 54 50 2f 31  -none.da t HTTP/1
00b0 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  .1..Conn ection:
00c0 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65  Keep-Alive..Acce
00d0 70 74 3a 20 2a 2f 2a 0d 0a 52 61 6e 67 65 3a 20  pt: /*.*. Range:

```

Frame (frame), 406 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 2: Wireshark-Informationen zum Mitschnitt des Frames

**\*WLAN**

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

> Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

▼ Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

- > Destination: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)
- > Source: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c)
- Type: IPv6 (0x86dd)

> Internet Protocol Version 6, Src: 2a00:20:5027:139d:58f9:6366:4e40:58cd, Dst: 2a02:26f0:ee00::216:f1a0

```

0000 f8 c3 9e 11 76 99 34 7d f6 5f a9 9c 86 dd 60 0d .....v.4} . . . . .
0010 46 c5 01 60 06 41 2a 00 00 20 50 27 13 9d 58 f9 F...A*...P'..X.
0020 63 66 4e 40 58 cd 2a 02 26 f0 ee 00 00 00 00 00 cfn@X.*. &.....
0030 00 00 02 16 f1 a0 c5 bb 00 50 85 cb d4 73 a8 8b .....P...s..
0040 b0 85 50 18 10 12 5a 49 00 00 47 45 54 20 2f 70 ..P...ZI ..GET /p
0050 72 2f 66 32 65 37 32 34 63 31 2d 37 34 38 66 2d r/f2e724 c1-748f-
0060 34 62 34 37 2d 38 66 62 38 2d 38 65 30 64 32 31 4b47-8fb 8-8e0d21
0070 30 65 39 32 30 38 2f 4f 66 66 69 63 65 2f 44 61 0e9208/O ffice/Da
0080 74 61 2f 31 36 2e 30 2e 31 30 33 36 36 2e 32 30 ta/16.0. 10366.20
0090 30 31 36 2f 73 74 72 65 61 6d 2e 78 36 34 2e 78 016/stre am.x64.x
00a0 2d 6e 6f 6e 65 2e 64 61 74 20 48 54 54 50 2f 31 -none.da t HTTP/1
00b0 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 .1..Conn ection:
00c0 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 Keep-Ali ve...Acce
00d0 70 74 3a 20 2a 2f 2a 0d 0a 52 61 6e 67 65 3a 20 pt: /*.*. Range:
00e0 62 79 74 65 73 3d 31 35 36 36 35 37 32 35 34 34 bytes=15 66572544
00f0 2d 31 35 36 36 36 33 38 30 37 39 0d 0a 55 73 65 -1566638 079...Use
0100 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f r-Agent: Microso
0110 66 74 2d 44 65 6c 69 76 65 72 79 2d 4f 70 74 69 ft-Deliv ery-Opti
0120 6d 69 7a 61 74 69 6f 6e 2f 31 30 2e 30 0d 0a 4d mization /10.0...M
0130 53 2d 43 56 3a 20 6b 53 6d 54 34 4d 34 6b 52 30 S-CV: kS mT4M4kR0
0140 43 57 37 36 38 4a 2e 32 2e 37 2e 31 2e 31 2e 31 CW768J.2 .7.1.1.1
0150 31 35 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 15...Cont ent-Leng
0160 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 66 66 th: 0..H ost: off
0170 69 63 65 63 64 6e 2e 6d 69 63 72 6f 73 6f 66 74 icecdn.m icrosoft
0180 2e 63 6f 6d 2e 65 64 67 65 73 75 69 74 65 2e 6e .com.edg esuite.n
0190 65 74 0d 0a 0d 0a et....
  
```

Ethernet (eth), 14 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) | Profil: Default

Abbildung 3: Ethernet-Header

Wireshark interface showing packet details for an HTTP GET request. The packet list shows three packets, with packet 2859 selected. The packet details pane shows the IP header and TCP header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

Internet Protocol Version 6, Src: 2a00:20:5027:139d:58f9:6366:4e40:58cd, Dst: 2a02:26f0:ee00::216:f1a0

0110 .... = Version: 6

.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 1101 0100 0110 1100 0101 = Flow Label: 0xd46c5

Payload Length: 352

Next Header: TCP (6)

Hop Limit: 65

Source: 2a00:20:5027:139d:58f9:6366:4e40:58cd

Destination: 2a02:26f0:ee00::216:f1a0

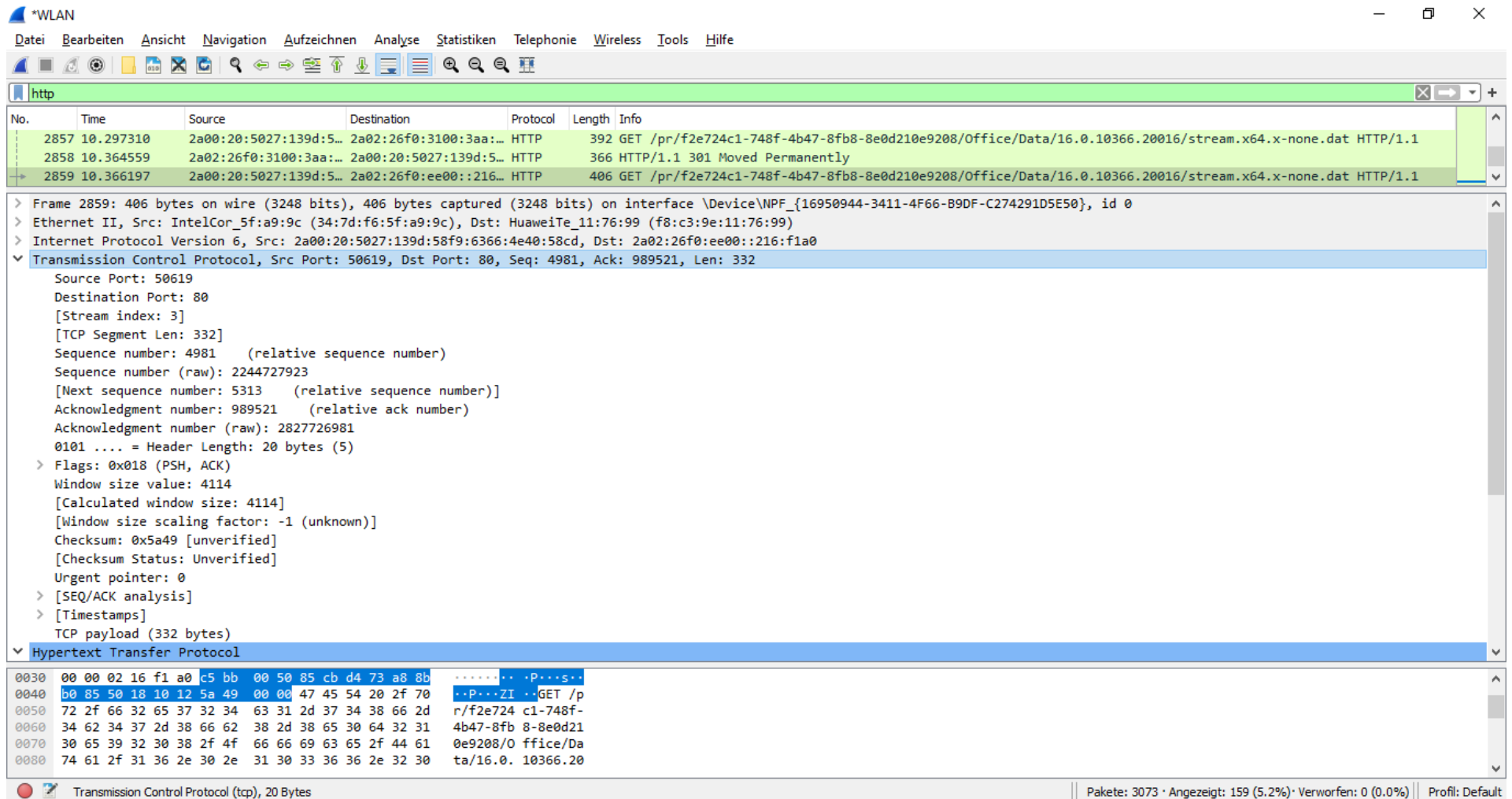
Transmission Control Protocol, Src Port: 50619, Dst Port: 80, Seq: 4981, Ack: 989521, Len: 332

0000 f8 c3 9e 11 76 99 34 7d f6 5f a9 9c 86 dd 60 0d .....v.4} .....  
 0010 46 c5 01 60 06 41 2a 00 00 20 50 27 13 9d 58 f9 F...A\*...P...X..  
 0020 63 66 4e 40 58 cd 2a 02 26 f0 ee 00 00 00 00 00 cFN@X.\*.&.....  
 0030 00 00 02 16 f1 a0 c5 bb 00 50 85 cb d4 73 a8 8b .....P...s..  
 0040 b0 85 50 18 10 12 5a 49 00 00 47 45 54 20 2f 70 ..P...ZI...GET /p  
 0050 72 2f 66 32 65 37 32 34 63 31 2d 37 34 38 66 2d r/f2e724 c1-748f-  
 0060 34 62 34 37 2d 38 66 62 38 2d 38 65 30 64 32 31 4b47-8fb 8-8e0d21  
 0070 30 65 39 32 30 38 2f 4f 66 66 69 63 65 2f 44 61 0e9208/O ffice/Da  
 0080 74 61 2f 31 36 2e 30 2e 31 30 33 36 36 2e 32 30 ta/16.0. 10366.20  
 0090 30 31 36 2f 73 74 72 65 61 6d 2e 78 36 34 2e 78 016/stre am.x64.x  
 00a0 2d 6e 6f 6e 65 2e 64 61 74 20 48 54 54 50 2f 31 -none.da t HTTP/1  
 00b0 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 .1..Conn ection:  
 00c0 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 Keep-Ali ve..Acce  
 00d0 70 74 3a 20 2a 2f 2a 0d 0a 52 61 6e 67 65 3a 20 pt: /\*.\*.Range:  
 00e0 62 79 74 65 73 3d 31 35 36 36 35 37 32 35 34 34 bytes=15 66572544  
 00f0 2d 31 35 36 36 36 33 38 30 37 39 0d 0a 55 73 65 -1566638 079..Use  
 0100 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f r-Agent: Microso  
 0110 66 74 2d 44 65 6c 69 76 65 72 79 2d 4f 70 74 69 ft-Deliv ery-Opti  
 0120 6d 69 7a 61 74 69 6f 6e 2f 31 30 2e 30 0d 0a 4d mization /10.0..M  
 0130 53 2d 43 56 3a 20 6b 53 6d 54 34 4d 34 6b 52 30 S-CV: kS mT4M4kR0  
 0140 43 57 37 36 38 4a 2e 32 2e 37 2e 31 2e 31 2e 31 CW768J.2 .7.1.1.1

Internet Protocol Version 6 (IPv6), 40 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 4: IP-Header



Wireshark interface showing packet details for a TCP-HTTP connection. The packet list shows three HTTP GET requests. The selected packet (2859) is a TCP segment with sequence number 4981, acknowledgment number 989521, and length 332. The packet details pane shows the TCP header and the HTTP payload (GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00:216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

Internet Protocol Version 6, Src: 2a00:20:5027:139d:58f9:6366:4e40:58cd, Dst: 2a02:26f0:ee00:216:f1a0

Transmission Control Protocol, Src Port: 50619, Dst Port: 80, Seq: 4981, Ack: 989521, Len: 332

Source Port: 50619  
Destination Port: 80  
[Stream index: 3]  
[TCP Segment Len: 332]  
Sequence number: 4981 (relative sequence number)  
Sequence number (raw): 2244727923  
[Next sequence number: 5313 (relative sequence number)]  
Acknowledgment number: 989521 (relative ack number)  
Acknowledgment number (raw): 2827726981  
0101 ... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)  
Window size value: 4114  
[Calculated window size: 4114]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x5a49 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0

[SEQ/ACK analysis]  
[Timestamps]  
TCP payload (332 bytes)

Hypertext Transfer Protocol

0030 00 00 02 16 f1 a0 c5 bb 00 50 85 cb d4 73 a8 8b .....P...s..

0040 b0 85 50 18 10 12 5a 49 00 00 47 45 54 20 2f 70 ..P...ZI..GET /p

0050 72 2f 66 32 65 37 32 34 63 31 2d 37 34 38 66 2d r/f2e724 c1-748f-

0060 34 62 34 37 2d 38 66 62 38 2d 38 65 30 64 32 31 4b47-8fb 8-8e0d21

0070 30 65 39 32 30 38 2f 4f 66 66 69 63 65 2f 44 61 0e9208/O ffice/Da

0080 74 61 2f 31 36 2e 30 2e 31 30 33 36 36 2e 32 30 ta/16.0. 10366.20

Transmission Control Protocol (tcp), 20 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 5: TCP-Header

\*WLAN

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

> Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0  
 > Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)  
 > Internet Protocol Version 6, Src: 2a00:20:5027:139d:58f9:6366:4e40:58cd, Dst: 2a02:26f0:ee00::216:f1a0  
 > Transmission Control Protocol, Src Port: 50619, Dst Port: 80, Seq: 4981, Ack: 989521, Len: 332

Hypertext Transfer Protocol

> GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1\r\n  
 Connection: Keep-Alive\r\n  
 Accept: \*/\*\r\n  
 Range: bytes=1566572544-1566638079\r\n  
 User-Agent: Microsoft-Delivery-Optimization/10.0\r\n  
 MS-CV: kSmT4M4kR0CW768J.2.7.1.1.115\r\n  
 > Content-Length: 0\r\n  
 Host: officecdn.microsoft.com.edgesuite.net\r\n  
 \r\n  
[\[Full request URI: http://officecdn.microsoft.com.edgesuite.net/pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat\]](http://officecdn.microsoft.com.edgesuite.net/pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat)  
[\[HTTP request 16/16\]](#)  
[\[Prev request in frame: 2672\]](#)  
[\[Response in frame: 2940\]](#)

0040 b0 85 50 18 10 12 5a 49 00 00 47 45 54 20 2f 70 ..P...ZI..GET /p  
 0050 72 2f 66 32 65 37 32 34 63 31 2d 37 34 38 66 2d r/f2e724 c1-748f-  
 0060 34 62 34 37 2d 38 66 62 38 2d 38 65 30 64 32 31 4b47-8fb 8-8e0d21  
 0070 30 65 39 32 30 38 2f 4f 66 66 69 63 65 2f 44 61 0e9208/O ffice/Da  
 0080 74 61 2f 31 36 2e 30 2e 31 30 33 36 36 2e 32 30 ta/16.0. 10366.20  
 0090 30 31 36 2f 73 74 72 65 61 6d 2e 78 36 34 2e 78 016/stre am.x64.x  
 00a0 2d 6e 6f 6e 65 2e 64 61 74 20 48 54 54 50 2f 31 -none.da t HTTP/1  
 00b0 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 .1..Conn ection:  
 00c0 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 Keep-Ali ve..Acce  
 00d0 70 74 3a 20 2a 2f 2a 0d 0a 52 61 6e 67 65 3a 20 pt: \*/\* ..Range:  
 00e0 62 79 74 65 73 3d 31 35 36 36 35 37 32 35 34 34 bytes=15 66572544  
 00f0 2d 31 35 36 36 36 33 38 30 37 39 0d 0a 55 73 65 -1566638 079..Use  
 0100 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f r-Agent: Microso  
 0110 66 74 2d 44 65 6c 69 76 65 72 79 2d 4f 70 74 69 ft-Deliv ery-Opti

Hypertext Transfer Protocol (http), 332 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 6: HTTP-Header (Anfang in Paketbytes)



\*WLAN

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telefonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2857	10.297310	2a00:20:5027:139d:5...	2a02:26f0:3100:3aa:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2858	10.364559	2a02:26f0:3100:3aa:...	2a00:20:5027:139d:5...	HTTP	366	HTTP/1.1 301 Moved Permanently
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00:216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1

> Frame 2859: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

> Ethernet II, Src: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c), Dst: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

> Internet Protocol Version 6, Src: 2a00:20:5027:139d:58f9:6366:4e40:58cd, Dst: 2a02:26f0:ee00:216:f1a0

> Transmission Control Protocol, Src Port: 50619, Dst Port: 80, Seq: 4981, Ack: 989521, Len: 332

▼ Hypertext Transfer Protocol

> GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1\r\n

Connection: Keep-Alive\r\n

Accept: \*/\*\r\n

Range: bytes=1566572544-1566638079\r\n

User-Agent: Microsoft-Delivery-Optimization/10.0\r\n

MS-CV: kSmT4M4kR0CW768J.2.7.1.1.115\r\n

> Content-Length: 0\r\n

Host: officecdn.microsoft.com.edgesuite.net\r\n

\r\n

[Full request URI: <http://officecdn.microsoft.com.edgesuite.net/pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat>]

[HTTP request 16/16]

[Prev request in frame: 2672]

[Response in frame: 2940]

Offset	Hex	ASCII
00c0	4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65	Keep-Alive..Acce
00d0	70 74 3a 20 2a 2f 2a 0d 0a 52 61 6e 67 65 3a 20	pt: */* .Range:
00e0	62 79 74 65 73 3d 31 35 36 36 35 37 32 35 34 34	bytes=15 66572544
00f0	2d 31 35 36 36 36 33 38 30 37 39 0d 0a 55 73 65	-1566638 079..Use
0100	72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f	r-Agent: Microso
0110	66 74 2d 44 65 6c 69 76 65 72 79 2d 4f 70 74 69	ft-Deliv ery-Opti
0120	6d 69 7a 61 74 69 6f 6e 2f 31 30 2e 30 0d 0a 4d	mization /10.0..M
0130	53 2d 43 56 3a 20 6b 53 6d 54 34 4d 34 6b 52 30	S-CV: kS mT4M4kR0
0140	43 57 37 36 38 4a 2e 32 2e 37 2e 31 2e 31 2e 31	CW768J.2 .7.1.1.1
0150	31 35 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67	15..Cont ent-Leng
0160	74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 6f 66 66	th: 0..H ost: off
0170	69 63 65 63 64 6e 2e 6d 69 63 72 6f 73 6f 66 74	icecdn.m icrosoft
0180	2e 63 6f 6d 2e 65 64 67 65 73 75 69 74 65 2e 6e	.com.edg esuite.n
0190	65 74 0d 0a 0d 0a	et....

Hypertext Transfer Protocol (http), 332 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 7: HTTP-Header (Ende in Paketbytes)

### Antwort-Frame des Webserver (Frame-Nr. 2940) an den Client auf die Anfrage in Frame 2859

Wireshark interface showing network traffic analysis. The top pane displays a list of frames, with frame 2940 selected. The middle pane shows the details of frame 2940, including interface information, arrival time, and frame length. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2887	10.606517	2a00:20:5027:139d:5...	2a02:26f0:3100:395:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2940	10.647095	2a02:26f0:ee00::216...	2a00:20:5027:139d:5...	HTTP	1194	HTTP/1.1 206 Partial Content

Frame 2940: 1194 bytes on wire (9552 bits), 1194 bytes captured (9552 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

- Interface id: 0 (\Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50})
- Encapsulation type: Ethernet (1)
- Arrival Time: Sep 16, 2020 09:35:31.932012000 Mitteleuropäische Sommerzeit
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1600241731.932012000 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.040578000 seconds]
- [Time since reference or first frame: 10.647095000 seconds]
- Frame Number: 2940
- Frame Length: 1194 bytes (9552 bits)
- Capture Length: 1194 bytes (9552 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ipv6:tcp:http:data]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: HuaweiTe 11:76:99 (f8:c3:9e:11:76:99), Dst: IntelCor 5f:a9:9c (34:7d:f6:5f:a9:9c)

Offset	Hex	ASCII
0000	34 7d f6 5f a9 9c f8 c3 9e 11 76 99 86 dd 60 00	4.....v....
0010	00 00 04 74 06 3c 2a 02 26 f0 ee 00 00 00 00 00	...f.<*. &.....
0020	00 00 02 16 f1 a0 2a 00 00 20 50 27 13 9d 58 f9	.....*..P...X.
0030	63 66 4e 40 58 cd 00 50 c5 bb a8 8c ad d5 85 cb	cfN@X..P.....
0040	d5 bf 50 18 25 21 9e ce 00 00 65 6a 20 c9 8c 88	..P.%!...ej...
0050	71 e0 c5 61 d5 ca db ea 0c 7e bd 59 b9 b2 ce 62	q..a.....~Y...b
0060	0e 8f ff da 95 fd d6 23 be 7d b3 92 1b 6e 25 69	.....#..}...n%i
0070	47 e4 3c 8a ef ec 29 98 2b 7b fb 4d 6b 37 e8 4d	G<...)+{.Mk7.M
0080	0a 11 49 fd 02 42 a4 2e 00 80 77 8e 81 30 a9 bf	..I..B...w..0..
0090	fe 7f 98 b3 8d 8f 02 6e ff 1b 6f 40 c4 e6 b7 a0	.....n..o@...
00a0	0b 50 e4 7f fd 58 64 d3 0b a9 19 95 77 e3 97 00	..P...Xd...w...
00b0	d8 b9 8e c2 56 1a b9 6e 6a 7f f5 9b 60 a3 57 56	....V...n.j....wV

Frame (1194 bytes) Reassembled TCP (65968 bytes)

Frame (frame), 1.194 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 8: Wireshark-Informationen zum Mitschnitt des Frames



\*WLAN

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2887	10.606517	2a00:20:5027:139d:5...	2a02:26f0:3100:395:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2940	10.647095	2a02:26f0:ee00::216...	2a00:20:5027:139d:5...	HTTP	1194	HTTP/1.1 206 Partial Content

> Frame 2940: 1194 bytes on wire (9552 bits), 1194 bytes captured (9552 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

▼ Ethernet II, Src: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99), Dst: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c)

> Destination: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c)

> Source: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99)

Type: IPv6 (0x86dd)

> Internet Protocol Version 6, Src: 2a02:26f0:ee00::216:f1a0, Dst: 2a00:20:5027:139d:58f9:6366:4e40:58cd

```

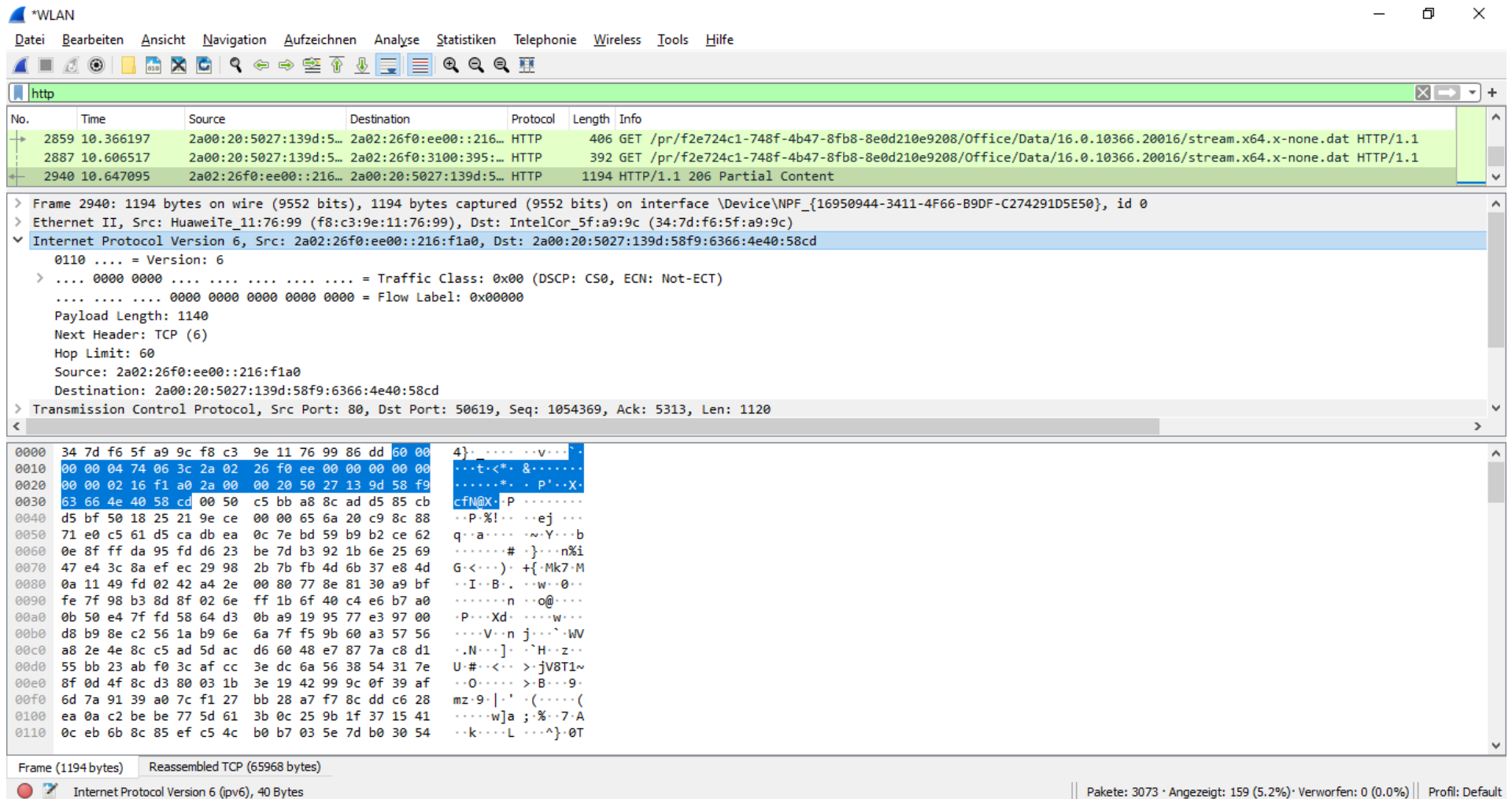
0000 34 7d f6 5f a9 9c f8 c3 9e 11 76 99 86 dd 60 00 4} . . . . .v . . .
0010 00 00 04 74 06 3c 2a 02 26 f0 ee 00 00 00 00 00 . . t . < * . & . . . . .
0020 00 00 02 16 f1 a0 2a 00 00 20 50 27 13 9d 58 f9 . . . . . * . P . . X .
0030 63 66 4e 40 58 cd 00 50 c5 bb a8 8c ad d5 85 cb c f N @ X . P . . . . .
0040 d5 bf 50 18 25 21 9e ce 00 00 65 6a 20 c9 8c 88 . . P . % ! . . . e j . . .
0050 71 e0 c5 61 d5 ca db ea 0c 7e bd 59 b9 b2 ce 62 q . a . . . . ~ . Y . . b
0060 0e 8f ff da 95 fd d6 23 be 7d b3 92 1b 6e 25 69 . . . . . # . } . . n % i
0070 47 e4 3c 8a ef ec 29 98 2b 7b fb 4d 6b 37 e8 4d G . < . . . . + { . Mk 7 . M
0080 0a 11 49 fd 02 42 a4 2e 00 80 77 8e 81 30 a9 bf . . I . B . . . w . 0 . .
0090 fe 7f 98 b3 8d 8f 02 6e ff 1b 6f 40 c4 e6 b7 a0 . . . . . n . . o @ . . .
00a0 0b 50 e4 7f fd 58 64 d3 0b a9 19 95 77 e3 97 00 . P . . X d . . . w . . .
00b0 d8 b9 8e c2 56 1a b9 6e 6a 7f f5 9b 60 a3 57 56 . . . V . . n j . . . w v
00c0 a8 2e 4e 8c c5 ad 5d ac d6 60 48 e7 87 7a c8 d1 . . N . . . . ] . . H . . z . .
00d0 55 bb 23 ab f0 3c af cc 3e dc 6a 56 38 54 31 7e U . # . . < . . > . j V 8 T 1 ~
00e0 8f 0d 4f 8c d3 80 03 1b 3e 19 42 99 9c 0f 39 af . . 0 . . . . . > . B . . . 9 .
00f0 6d 7a 91 39 a0 7c f1 27 bb 28 a7 f7 8c dd c6 28 m z . 9 . | . ' . ( . . . . (
0100 ea 0a c2 be be 77 5d 61 3b 0c 25 9b 1f 37 15 41 . . . . . w ] a . ; . % . . 7 . A
0110 0c eb 6b 8c 85 ef c5 4c b0 b7 03 5e 7d b0 30 54 . . k . . . . L . . . ^ . } . 0 T
0120 96 2a 6a 9a 9d d7 50 65 3e 4f 64 13 40 9a 53 97 . * j . . . P e > 0 d . @ . S .
0130 23 52 c0 c7 f2 57 c7 21 89 04 77 fb 9f cb c5 a7 # R . . . W . ! . . w . . . .
0140 21 00 83 3d 51 86 84 19 00 ec de 9a d5 fd a2 ba ! . . = Q . . . . .
0150 5b be 15 2b e8 29 fe b8 55 34 59 46 8f 8d 58 fb [ . . + . ) . . U 4 Y F . . X .
0160 86 d2 60 bc 64 76 b2 b7 82 96 88 e6 fa 07 74 b2 . . . . d v . . . . . t .
0170 e0 4f c2 f6 e5 a7 fd 9f dd 4c 37 50 7e 67 d1 37 . 0 . . . . . L 7 P ~ g . 7
0180 01 26 d9 f9 86 fb 74 0a 18 94 3b 95 f5 17 c1 f8 . & . . . . t . . ; . . . .
    
```

Frame (1194 bytes) Reassembled TCP (65968 bytes)

Ethernet (eth), 14 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 9: Ethernet-Header



\*WLAN

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2859	10.366197	2a00:20:5027:139d:5...	2a02:26f0:ee00::216...	HTTP	406	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2887	10.606517	2a00:20:5027:139d:5...	2a02:26f0:3100:395:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2940	10.647095	2a02:26f0:ee00::216...	2a00:20:5027:139d:5...	HTTP	1194	HTTP/1.1 206 Partial Content

> Frame 2940: 1194 bytes on wire (9552 bits), 1194 bytes captured (9552 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

> Ethernet II, Src: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99), Dst: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c)

> Internet Protocol Version 6, Src: 2a02:26f0:ee00::216:f1a0, Dst: 2a00:20:5027:139d:58f9:6366:4e40:58cd

0110 .... = Version: 6

> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 0000 0000 0000 0000 = Flow Label: 0x000000

Payload Length: 1140

Next Header: TCP (6)

Hop Limit: 60

Source: 2a02:26f0:ee00::216:f1a0

Destination: 2a00:20:5027:139d:58f9:6366:4e40:58cd

> Transmission Control Protocol, Src Port: 80, Dst Port: 50619, Seq: 1054369, Ack: 5313, Len: 1120

0000 34 7d f6 5f a9 9c f8 c3 9e 11 76 99 86 dd 60 00 4d} . . . . . v . . . . .

0010 00 00 04 74 06 3c 2a 02 26 f0 ee 00 00 00 00 00 . . . t . < \* . & . . . . .

0020 00 00 02 16 f1 a0 2a 00 00 20 50 27 13 9d 58 f9 . . . . . \* . P ' . . X .

0030 63 66 4e 40 58 cd 00 50 c5 bb a8 8c ad d5 85 cb cfN@X . P . . . . .

0040 d5 bf 50 18 25 21 9e ce 00 00 65 6a 20 c9 8c 88 . . P % ! . . . . . ej . . .

0050 71 e0 c5 61 d5 ca db ea 0c 7e bd 59 b9 b2 ce 62 q . . a . . . . . Y . . . b

0060 0e 8f ff da 95 fd d6 23 be 7d b3 92 1b 6e 25 69 . . . . . # . } . . n % i

0070 47 e4 3c 8a ef ec 29 98 2b 7b fb 4d 6b 37 e8 4d G < . . . . . + { . Mk 7 . M

0080 0a 11 49 fd 02 42 a4 2e 00 80 77 8e 81 30 a9 bf . . I . . B . . . w . . 0 . .

0090 fe 7f 98 b3 8d 8f 02 6e ff 1b 6f 40 c4 e6 b7 a0 . . . . . n . . o @ . . . . .

00a0 0b 50 e4 7f fd 58 64 d3 0b a9 19 95 77 e3 97 00 . P . . . X d . . . . . w . . .

00b0 d8 b9 8e c2 56 1a b9 6e 6a 7f f5 9b 60 a3 57 56 . . . V . . n j . . . . . WV

00c0 a8 2e 4e 8c c5 ad 5d ac d6 60 48 e7 87 7a c8 d1 . . N . . . . . ] . . H . . z . .

00d0 55 bb 23 ab f0 3c af cc 3e dc 6a 56 38 54 31 7e U # . . < . . . . . j V 8 T 1 ~

00e0 8f 0d 4f 8c d3 80 03 1b 3e 19 42 99 9c 0f 39 af . . 0 . . . . . > . B . . . 9 .

00f0 6d 7a 91 39 a0 7c f1 27 bb 28 a7 f7 8c dd c6 28 mz . 9 . | . ' . ( . . . . . (

0100 ea 0a c2 be be 77 5d 61 3b 0c 25 9b 1f 37 15 41 . . . . . w ] a ; % . . 7 . A

0110 0c eb 6b 8c 85 ef c5 4c b0 b7 03 5e 7d b0 30 54 . . k . . . . . L . . . . . ^ } . 0 T

Frame (1194 bytes) Reassembled TCP (65968 bytes)

Internet Protocol Version 6 (IPv6), 40 Bytes

Pakete: 3073 · Angezeigt: 159 (5.2%) · Verworfen: 0 (0.0%) · Profil: Default

Abbildung 10: IP-Header

Mitschnitt für Skrip 2020-09-16.pcapng

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

http

No.	Time	Source	Destination	Protocol	Length	Info
2887	10.606517	2a00:20:5027:139d:5...	2a02:26f0:3100:395:...	HTTP	392	GET /pr/f2e724c1-748f-4b47-8fb8-8e0d210e9208/Office/Data/16.0.10366.20016/stream.x64.x-none.dat HTTP/1.1
2940	10.647095	2a02:26f0:ee00::216...	2a00:20:5027:139d:5...	HTTP	1194	HTTP/1.1 206 Partial Content
2956	10.649216	103.235.47.69	192.168.43.82	HTTP	566	HTTP/1.1 200 OK (application/javascript)

> Frame 2940: 1194 bytes on wire (9552 bits), 1194 bytes captured (9552 bits) on interface \Device\NPF\_{16950944-3411-4F66-B9DF-C274291D5E50}, id 0

> Ethernet II, Src: HuaweiTe\_11:76:99 (f8:c3:9e:11:76:99), Dst: IntelCor\_5f:a9:9c (34:7d:f6:5f:a9:9c)

> Internet Protocol Version 6, Src: 2a02:26f0:ee00::216:f1a0, Dst: 2a00:20:5027:139d:58f9:6366:4e40:58cd

> Transmission Control Protocol, Src Port: 80, Dst Port: 50619, Seq: 1054369, Ack: 5313, Len: 1120

Source Port: 80  
Destination Port: 50619  
[Stream index: 3]  
[TCP Segment Len: 1120]  
Sequence number: 1054369 (relative sequence number)  
Sequence number (raw): 2827791829  
[Next sequence number: 1055489 (relative sequence number)]  
Acknowledgment number: 5313 (relative ack number)  
Acknowledgment number (raw): 2244728255  
0101 ... = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)  
Window size value: 9505  
[Calculated window size: 9505]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x9ece [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0

> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (1120 bytes)  
TCP segment data (1120 bytes)

0030 63 66 4e 40 58 cd 00 50 c5 bb a8 8c ad d5 85 cb cfn@X:P .....  
0040 d5 bf 50 18 25 21 9e ce 00 00 65 6a 20 c9 8c 88 ..P.%!..ej ...  
0050 71 e0 c5 61 d5 ca db ea 0c 7e bd 59 b9 b2 ce 62 q..a....~.Y...b  
0060 0e 8f ff da 95 fd d6 23 be 7d b3 92 1b 6e 25 69 .....#..}...n%1

Frame (1194 bytes) Reassembled TCP (65968 bytes)

Transmission Control Protocol (tcp), 20 Bytes

Pakete: 3073 · Angezeigt: 159 (5,2%) Profil: Default

Abbildung 11: TCP-Header

**Abbildung 12: zusätzliche TCP-Informationen (zusammengesetzte TCP-Segmente)**

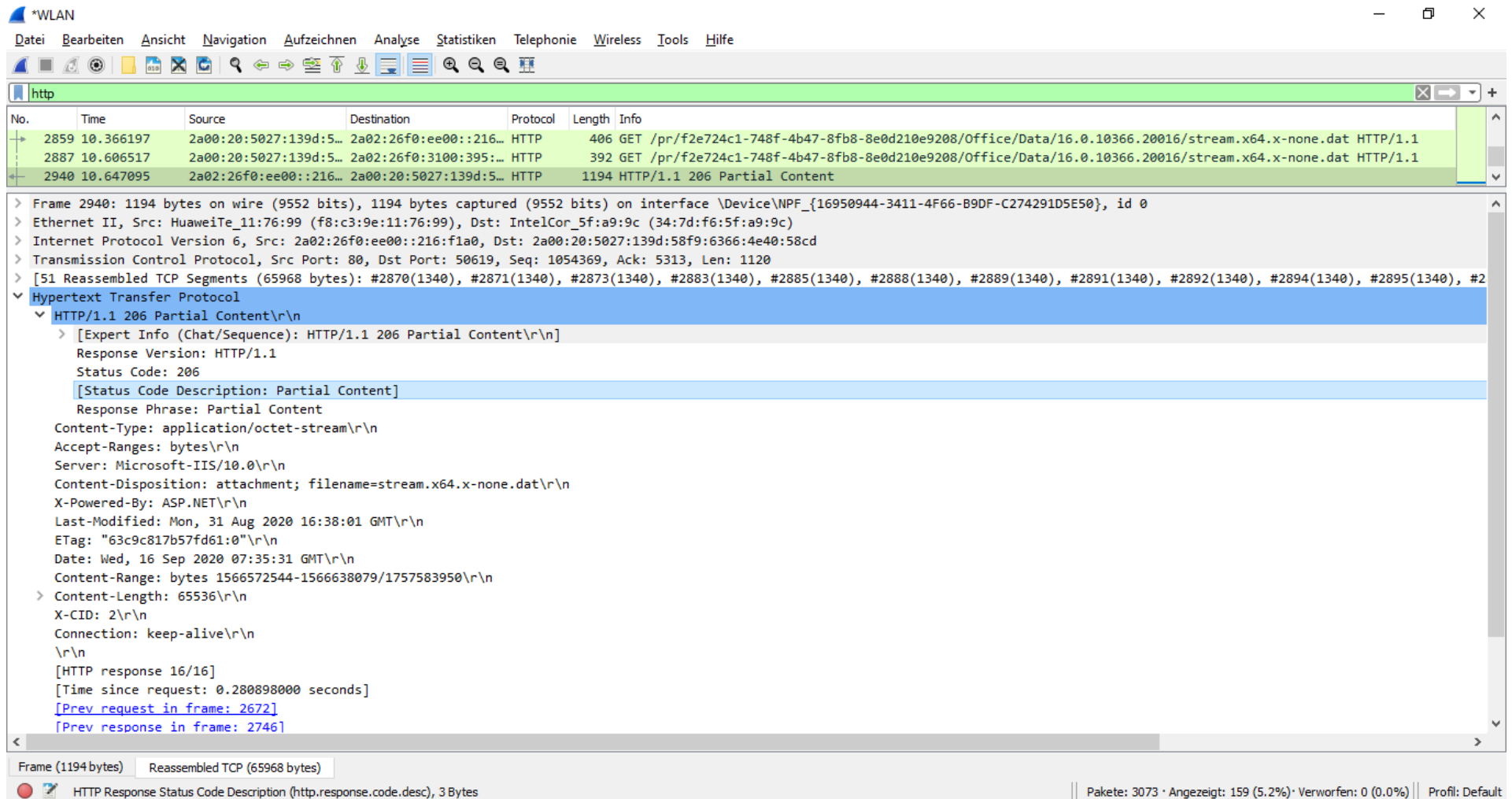


Abbildung 13: Teil 1 HTTP-Header: vollständiger HTTP-Header in Paketdetails (Paketbytes nicht sichtbar)



**Abbildung 14: Teil 2 HTTP-Header: letzter Teil des HTTP-Headers in Paketbytes mit Payload darunter**





