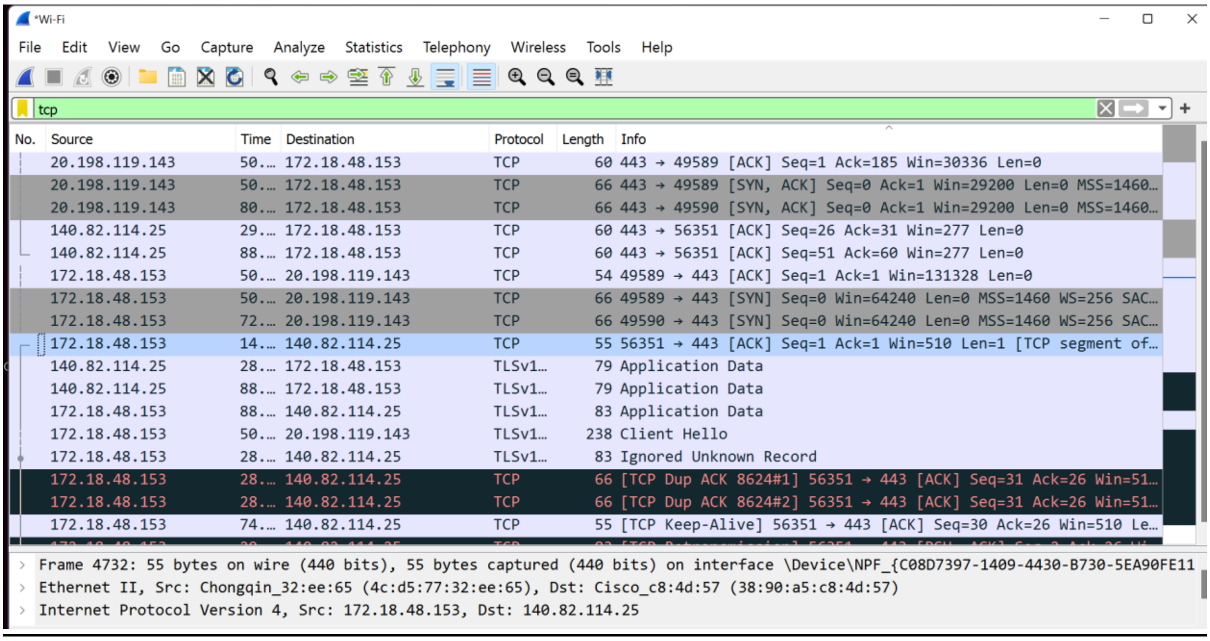
# EX 8: PACKET ANALYZER TOOL

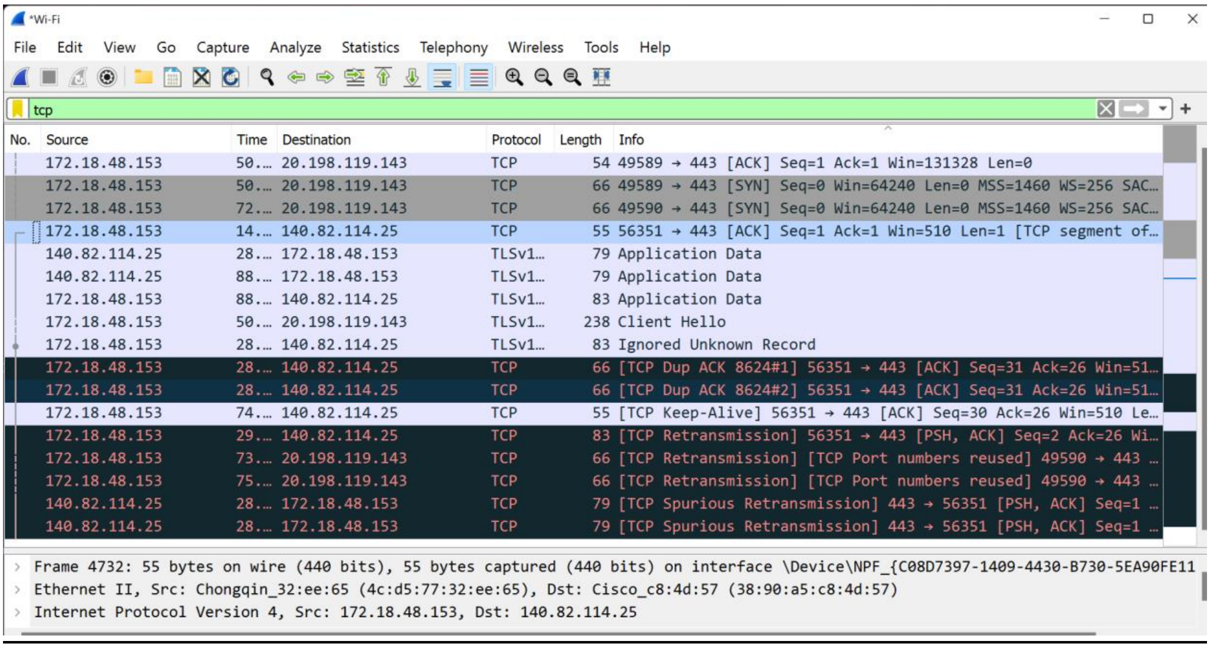
## OUTPUT:



tcp

| No. | Source | Time | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| | 20.198.119.143 | 50… | 172.18.48.153 | TCP | 60 | 443 → 49589 [ACK] Seq=1 Ack=185 Win=30336 Len=0 |
| | 20.198.119.143 | 50… | 172.18.48.153 | TCP | 66 | 443 → 49589 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460… |
| | 20.198.119.143 | 80… | 172.18.48.153 | TCP | 66 | 443 → 49590 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460… |
| | 140.82.114.25 | 29… | 172.18.48.153 | TCP | 60 | 443 → 56351 [ACK] Seq=26 Ack=31 Win=277 Len=0 |
| | 140.82.114.25 | 88… | 172.18.48.153 | TCP | 60 | 443 → 56351 [ACK] Seq=51 Ack=60 Win=277 Len=0 |
| | 172.18.48.153 | 50… | 20.198.119.143 | TCP | 54 | 49589 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| | 172.18.48.153 | 50… | 20.198.119.143 | TCP | 66 | 49589 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC… |
| | 172.18.48.153 | 72… | 20.198.119.143 | TCP | 66 | 49590 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC… |
| | 172.18.48.153 | 14… | 140.82.114.25 | TCP | 55 | 56351 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of… |
| | 140.82.114.25 | 28… | 172.18.48.153 | TLSv1… | 79 | Application Data |
| | 140.82.114.25 | 88… | 172.18.48.153 | TLSv1… | 79 | Application Data |
| | 172.18.48.153 | 88… | 140.82.114.25 | TLSv1… | 83 | Application Data |
| | 172.18.48.153 | 50… | 20.198.119.143 | TLSv1… | 238 | Client Hello |
| | 172.18.48.153 | 28… | 140.82.114.25 | TLSv1… | 83 | Ignored Unknown Record |
| | 172.18.48.153 | 28… | 140.82.114.25 | TCP | 66 | [TCP Dup ACK 8624#1] 56351 → 443 [ACK] Seq=31 Ack=26 Win=51… |
| | 172.18.48.153 | 28… | 140.82.114.25 | TCP | 66 | [TCP Dup ACK 8624#2] 56351 → 443 [ACK] Seq=31 Ack=26 Win=51… |
| | 172.18.48.153 | 74… | 140.82.114.25 | TCP | 55 | [TCP Keep-Alive] 56351 → 443 [ACK] Seq=30 Ack=26 Win=510 Le… |

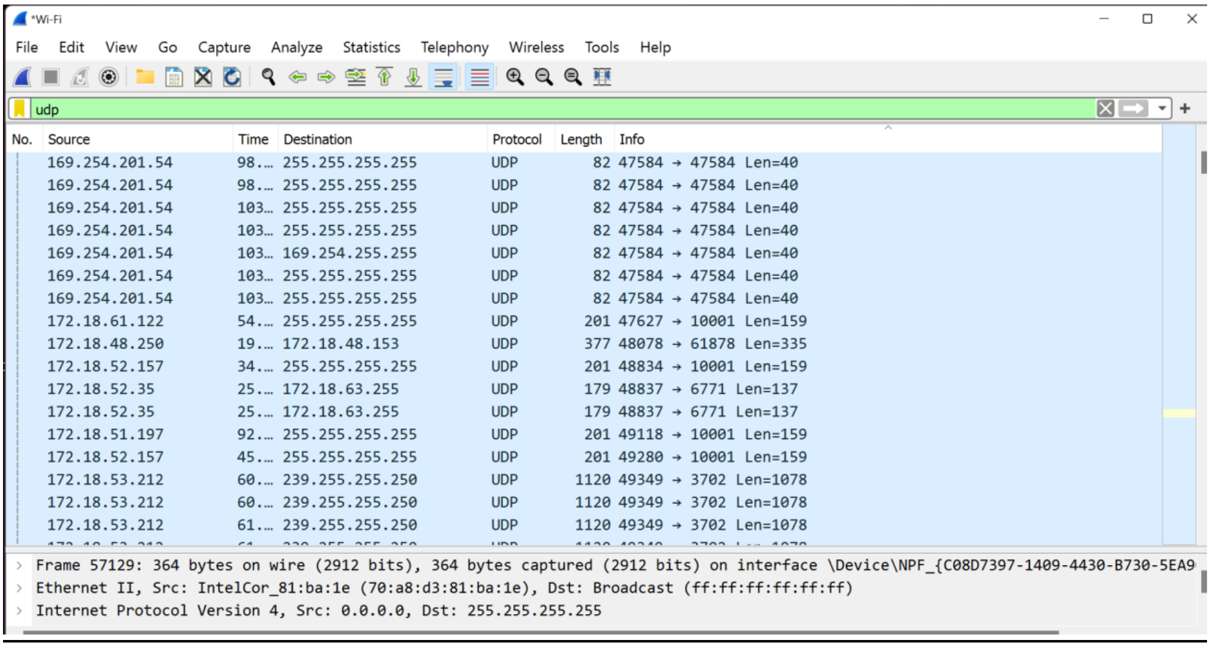
```
> Frame 4732: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90FE11
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: Cisco_c8:4d:57 (38:90:a5:c8:4d:57)
> Internet Protocol Version 4, Src: 172.18.48.153, Dst: 140.82.114.25
```



tcp

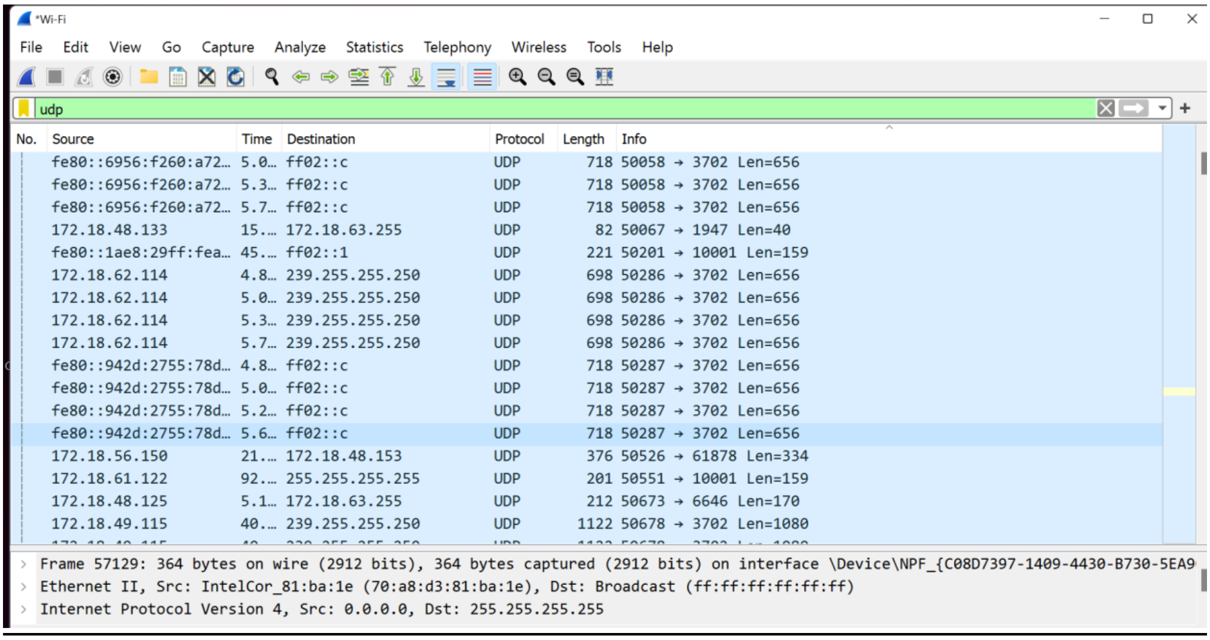
| No. | Source | Time | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| | 172.18.48.153 | 50… | 20.198.119.143 | TCP | 54 | 49589 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| | 172.18.48.153 | 50… | 20.198.119.143 | TCP | 66 | 49589 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC… |
| | 172.18.48.153 | 72… | 20.198.119.143 | TCP | 66 | 49590 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC… |
| | 172.18.48.153 | 14… | 140.82.114.25 | TCP | 55 | 56351 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of… |
| | 140.82.114.25 | 28… | 172.18.48.153 | TLSv1… | 79 | Application Data |
| | 140.82.114.25 | 88… | 172.18.48.153 | TLSv1… | 79 | Application Data |
| | 172.18.48.153 | 88… | 140.82.114.25 | TLSv1… | 83 | Application Data |
| | 172.18.48.153 | 50… | 20.198.119.143 | TLSv1… | 238 | Client Hello |
| | 172.18.48.153 | 28… | 140.82.114.25 | TLSv1… | 83 | Ignored Unknown Record |
| | 172.18.48.153 | 28… | 140.82.114.25 | TCP | 66 | [TCP Dup ACK 8624#1] 56351 → 443 [ACK] Seq=31 Ack=26 Win=51… |
| | 172.18.48.153 | 28… | 140.82.114.25 | TCP | 66 | [TCP Dup ACK 8624#2] 56351 → 443 [ACK] Seq=31 Ack=26 Win=51… |
| | 172.18.48.153 | 74… | 140.82.114.25 | TCP | 55 | [TCP Keep-Alive] 56351 → 443 [ACK] Seq=30 Ack=26 Win=510 Le… |
| | 172.18.48.153 | 29… | 140.82.114.25 | TCP | 83 | [TCP Retransmission] 56351 → 443 [PSH, ACK] Seq=2 Ack=26 Wi… |
| | 172.18.48.153 | 73… | 20.198.119.143 | TCP | 66 | [TCP Retransmission] [TCP Port numbers reused] 49590 → 443 … |
| | 172.18.48.153 | 75… | 20.198.119.143 | TCP | 66 | [TCP Retransmission] [TCP Port numbers reused] 49590 → 443 … |
| | 140.82.114.25 | 28… | 172.18.48.153 | TCP | 79 | [TCP Spurious Retransmission] 443 → 56351 [PSH, ACK] Seq=1 … |
| | 140.82.114.25 | 28… | 172.18.48.153 | TCP | 79 | [TCP Spurious Retransmission] 443 → 56351 [PSH, ACK] Seq=1 … |

```
> Frame 4732: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90FE11
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: Cisco_c8:4d:57 (38:90:a5:c8:4d:57)
> Internet Protocol Version 4, Src: 172.18.48.153, Dst: 140.82.114.25
```



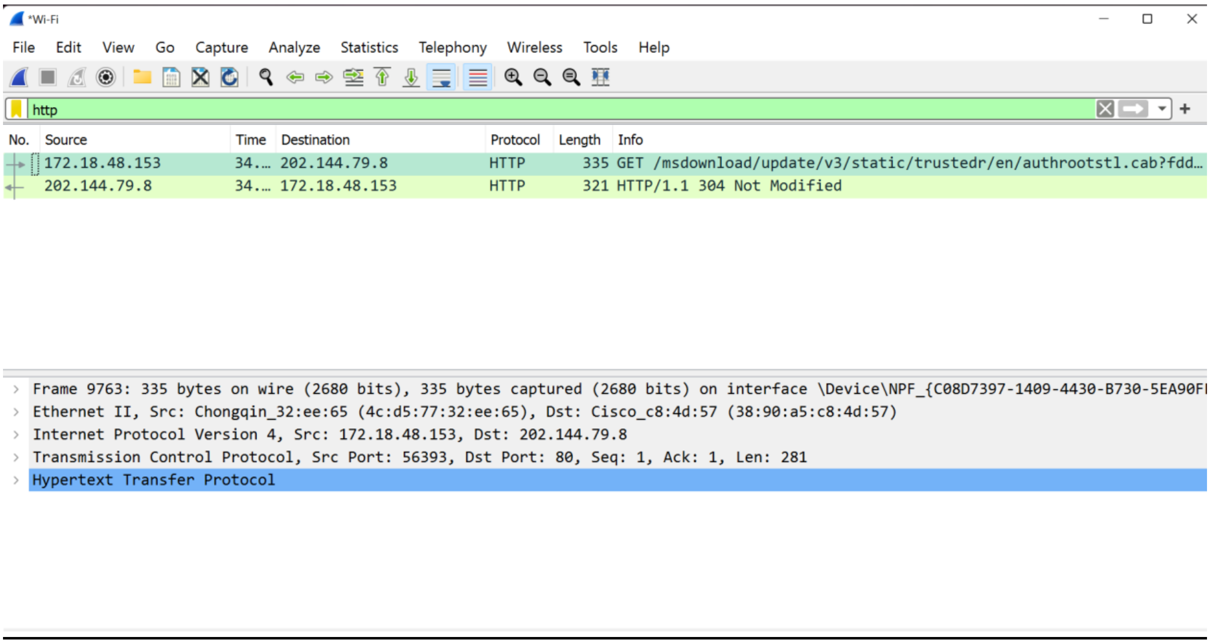
```
No.  Source            Time  Destination      Protocol  Length  Info
     169.254.201.54    98.…  255.255.255.255  UDP         82 47584 → 47584 Len=40
     169.254.201.54    98.…  255.255.255.255  UDP         82 47584 → 47584 Len=40
     169.254.201.54    103…  255.255.255.255  UDP         82 47584 → 47584 Len=40
     169.254.201.54    103…  255.255.255.255  UDP         82 47584 → 47584 Len=40
     169.254.201.54    103…  169.254.255.255  UDP         82 47584 → 47584 Len=40
     169.254.201.54    103…  255.255.255.255  UDP         82 47584 → 47584 Len=40
     169.254.201.54    103…  255.255.255.255  UDP         82 47584 → 47584 Len=40
     172.18.61.122     54.…  255.255.255.255  UDP        201 47627 → 10001 Len=159
     172.18.48.250     19.…  172.18.48.153    UDP        377 48078 → 61878 Len=335
     172.18.52.157     34.…  255.255.255.255  UDP        201 48834 → 10001 Len=159
     172.18.52.35      25.…  172.18.63.255    UDP        179 48837 → 6771 Len=137
     172.18.52.35      25.…  172.18.63.255    UDP        179 48837 → 6771 Len=137
     172.18.51.197     92.…  255.255.255.255  UDP        201 49118 → 10001 Len=159
     172.18.52.157     45.…  255.255.255.255  UDP        201 49280 → 10001 Len=159
     172.18.53.212     60.…  239.255.255.250  UDP       1120 49349 → 3702 Len=1078
     172.18.53.212     60.…  239.255.255.250  UDP       1120 49349 → 3702 Len=1078
     172.18.53.212     61.…  239.255.255.250  UDP       1120 49349 → 3702 Len=1078
```

```
> Frame 57129: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA9
> Ethernet II, Src: IntelCor_81:ba:1e (70:a8:d3:81:ba:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```



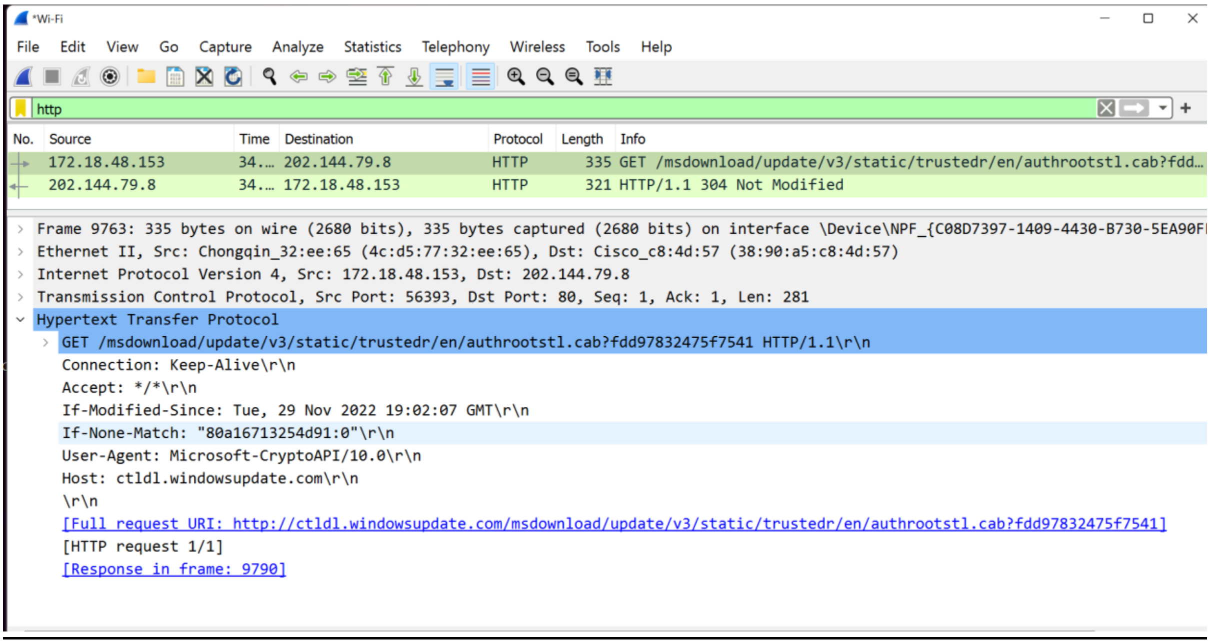
```
No.  Source                 Time  Destination      Protocol  Length  Info
     fe80::6956:f260:a72…   5.0…  ff02::c          UDP        718 50058 → 3702 Len=656
     fe80::6956:f260:a72…   5.3…  ff02::c          UDP        718 50058 → 3702 Len=656
     fe80::6956:f260:a72…   5.7…  ff02::c          UDP        718 50058 → 3702 Len=656
     172.18.48.133          15.…  172.18.63.255    UDP         82 50067 → 1947 Len=40
     fe80::1ae8:29ff:fea…   45.…  ff02::1          UDP        221 50201 → 10001 Len=159
     172.18.62.114          4.8…  239.255.255.250  UDP        698 50286 → 3702 Len=656
     172.18.62.114          5.0…  239.255.255.250  UDP        698 50286 → 3702 Len=656
     172.18.62.114          5.3…  239.255.255.250  UDP        698 50286 → 3702 Len=656
     172.18.62.114          5.7…  239.255.255.250  UDP        698 50286 → 3702 Len=656
     fe80::942d:2755:78d…   4.8…  ff02::c          UDP        718 50287 → 3702 Len=656
     fe80::942d:2755:78d…   5.0…  ff02::c          UDP        718 50287 → 3702 Len=656
     fe80::942d:2755:78d…   5.2…  ff02::c          UDP        718 50287 → 3702 Len=656
     fe80::942d:2755:78d…   5.6…  ff02::c          UDP        718 50287 → 3702 Len=656
     172.18.56.150          21.…  172.18.48.153    UDP        376 50526 → 61878 Len=334
     172.18.61.122          92.…  255.255.255.255  UDP        201 50551 → 10001 Len=159
     172.18.48.125          5.1…  172.18.63.255    UDP        212 50673 → 6646 Len=170
     172.18.49.115          40.…  239.255.255.250  UDP       1122 50678 → 3702 Len=1080
```

```
> Frame 57129: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA9
> Ethernet II, Src: IntelCor_81:ba:1e (70:a8:d3:81:ba:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

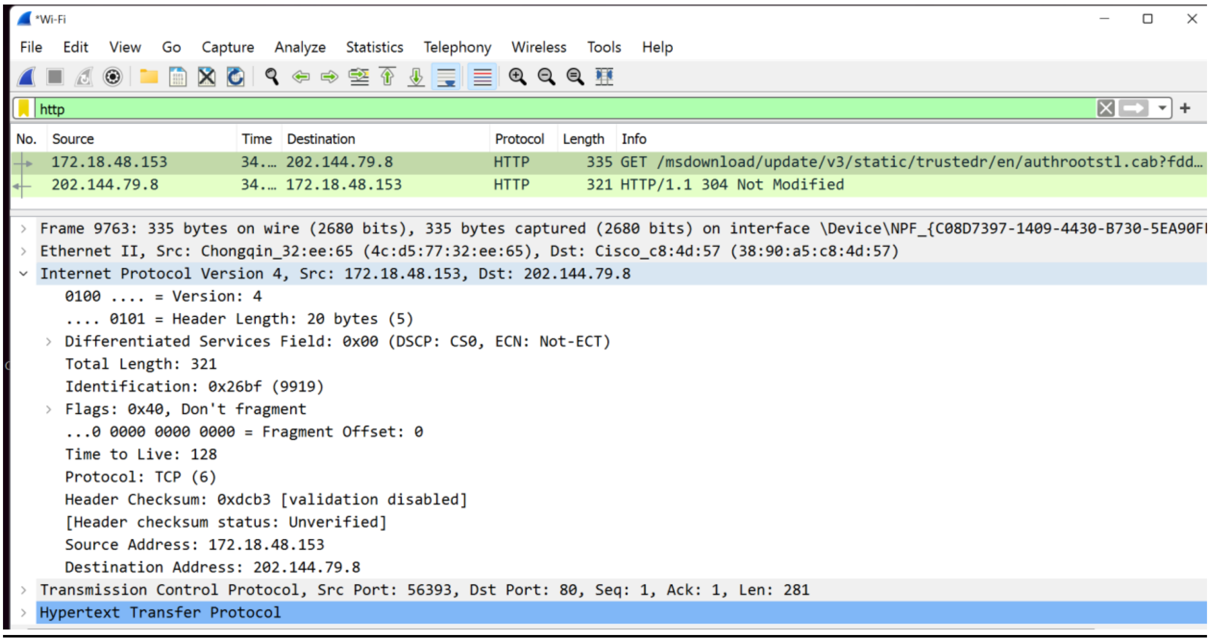
```
No.  Source         Time  Destination     Protocol  Length  Info
     172.18.48.153  34.…  202.144.79.8    HTTP         335  GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdd…
     202.144.79.8   34.…  172.18.48.153   HTTP         321  HTTP/1.1 304 Not Modified
```

```
> Frame 9763: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90F
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: Cisco_c8:4d:57 (38:90:a5:c8:4d:57)
> Internet Protocol Version 4, Src: 172.18.48.153, Dst: 202.144.79.8
> Transmission Control Protocol, Src Port: 56393, Dst Port: 80, Seq: 1, Ack: 1, Len: 281
> Hypertext Transfer Protocol
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Source         Time  Destination     Protocol  Length  Info
     172.18.48.153  34.…  202.144.79.8    HTTP         335  GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdd…
     202.144.79.8   34.…  172.18.48.153   HTTP         321  HTTP/1.1 304 Not Modified
```

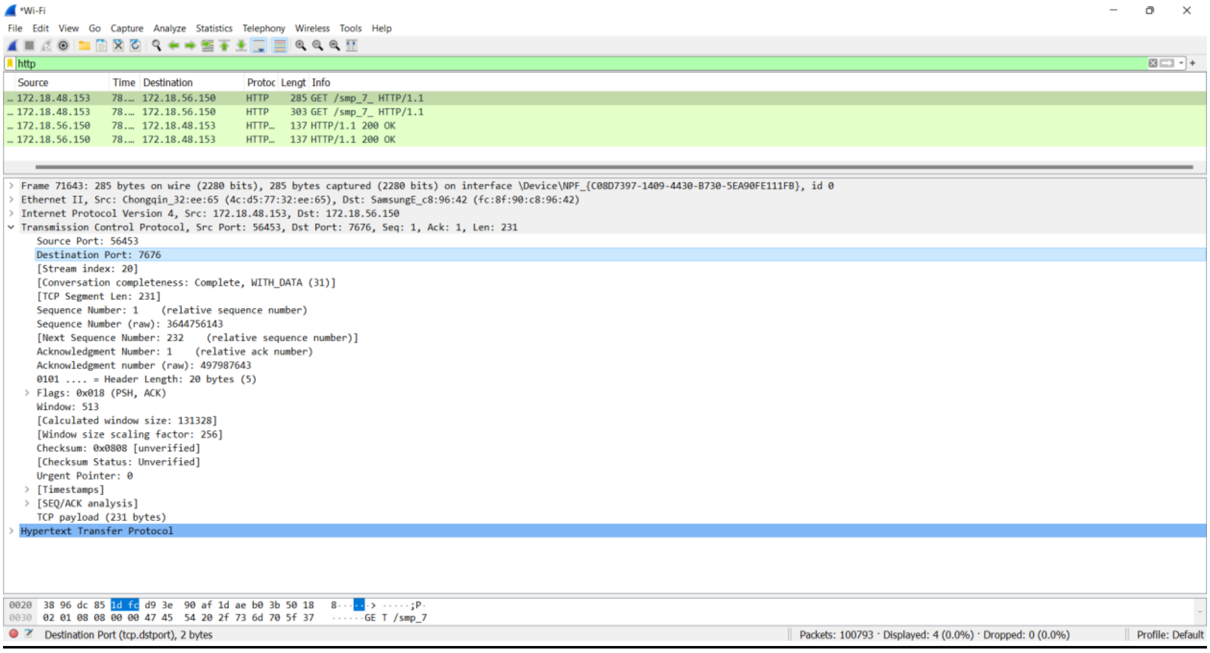
```
> Frame 9763: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90F
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: Cisco_c8:4d:57 (38:90:a5:c8:4d:57)
> Internet Protocol Version 4, Src: 172.18.48.153, Dst: 202.144.79.8
> Transmission Control Protocol, Src Port: 56393, Dst Port: 80, Seq: 1, Ack: 1, Len: 281
v Hypertext Transfer Protocol
  > GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdd97832475f7541 HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    If-Modified-Since: Tue, 29 Nov 2022 19:02:07 GMT\r\n
    If-None-Match: "80a16713254d91:0"\r\n
    User-Agent: Microsoft-CryptoAPI/10.0\r\n
    Host: ctldl.windowsupdate.com\r\n
    \r\n
    [Full request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdd97832475f7541]
    [HTTP request 1/1]
    [Response in frame: 9790]
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.  Source          Time  Destination     Protocol  Length  Info
     172.18.48.153   34.…  202.144.79.8    HTTP         335  GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?fdd…
     202.144.79.8    34.…  172.18.48.153   HTTP         321  HTTP/1.1 304 Not Modified
```

```
> Frame 9763: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90FI
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: Cisco_c8:4d:57 (38:90:a5:c8:4d:57)
v Internet Protocol Version 4, Src: 172.18.48.153, Dst: 202.144.79.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 321
    Identification: 0x26bf (9919)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xdcb3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.18.48.153
    Destination Address: 202.144.79.8
> Transmission Control Protocol, Src Port: 56393, Dst Port: 80, Seq: 1, Ack: 1, Len: 281
> Hypertext Transfer Protocol
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

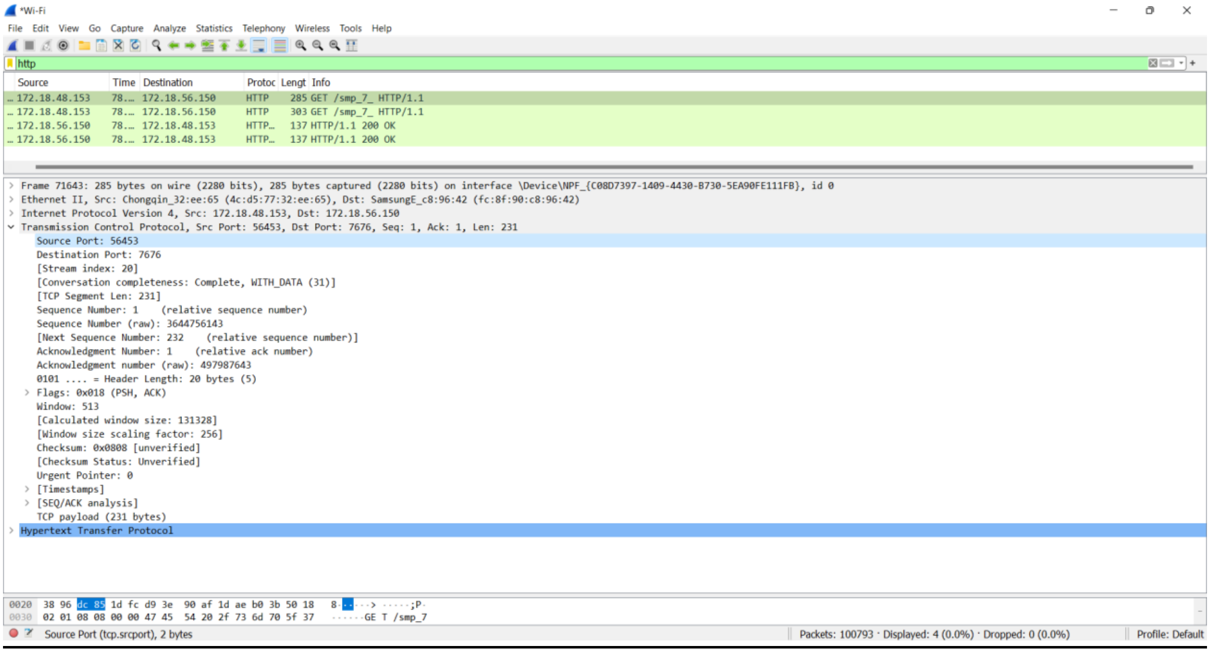
```
http
```

```
  Source          Time  Destination     Protoc  Lengt  Info
… 172.18.48.153   78.…  172.18.56.150   HTTP      285  GET /smp_7_ HTTP/1.1
… 172.18.48.153   78.…  172.18.56.150   HTTP      303  GET /smp_7_ HTTP/1.1
… 172.18.56.150   78.…  172.18.48.153   HTTP…     137  HTTP/1.1 200 OK
… 172.18.56.150   78.…  172.18.48.153   HTTP…     137  HTTP/1.1 200 OK
```

```
> Frame 71643: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90FE111FB}, id 0
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: SamsungE_c8:96:42 (fc:8f:90:c8:96:42)
> Internet Protocol Version 4, Src: 172.18.48.153, Dst: 172.18.56.150
v Transmission Control Protocol, Src Port: 56453, Dst Port: 7676, Seq: 1, Ack: 1, Len: 231
    Source Port: 56453
    Destination Port: 7676
    [Stream index: 20]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 231]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3644756143
    [Next Sequence Number: 232    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 497987643
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x0808 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (231 bytes)
> Hypertext Transfer Protocol
```

```
0020  38 96 dc 85 1d fc d9 3e  90 af 1d ae b0 3b 50 18   8······> ·····;P·
0030  02 01 08 08 00 00 47 45  54 20 2f 73 6d 70 5f 37   ······GE T /smp_7
```

```
Destination Port (tcp.dstport), 2 bytes    Packets: 100793 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
  Source        Time  Destination     Protoc  Lengt Info
… 172.18.48.153  78.… 172.18.56.150   HTTP     285 GET /smp_7_ HTTP/1.1
… 172.18.48.153  78.… 172.18.56.150   HTTP     303 GET /smp_7_ HTTP/1.1
… 172.18.56.150  78.… 172.18.48.153   HTTP…    137 HTTP/1.1 200 OK
… 172.18.56.150  78.… 172.18.48.153   HTTP…    137 HTTP/1.1 200 OK
```

```
> Frame 71643: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits) on interface \Device\NPF_{C08D7397-1409-4430-B730-5EA90FE111FB}, id 0
> Ethernet II, Src: Chongqin_32:ee:65 (4c:d5:77:32:ee:65), Dst: SamsungE_c8:96:42 (fc:8f:90:c8:96:42)
> Internet Protocol Version 4, Src: 172.18.48.153, Dst: 172.18.56.150
v Transmission Control Protocol, Src Port: 56453, Dst Port: 7676, Seq: 1, Ack: 1, Len: 231
    Source Port: 56453
    Destination Port: 7676
    [Stream index: 20]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 231]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3644756143
    [Next Sequence Number: 232    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 497987643
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x0808 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (231 bytes)
> Hypertext Transfer Protocol
```

```
0020  38 96 dc 85 1d fc d9 3e  90 af 1d ae b0 3b 50 18   8·······>·····;P·
0030  02 01 08 08 00 00 47 45  54 20 2f 73 6d 70 5f 37   ······GE T /smp_7
```

Source Port (tcp.srcport), 2 bytes    Packets: 100793 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)    Profile: Default