```
No.     Time           Source                Destination           Protocol Length Info
   1967 33.776369      192.168.1.49          77.75.149.208         HTTP     336    GET /msdownload/update/v3/static/trustedr/en/
pinrulesstl.cab?2a6253800db2a34e HTTP/1.1
Frame 1967: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits) on interface \Device\NPF_{E8F1393B-10D6-4491-
A631-26A44CA59FE2}, id 0
    Interface id: 0 (\Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2})
        Interface name: \Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: May  1, 2021 22:23:31.463494000 Финляндия (лето)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1619897011.463494000 seconds
    [Time delta from previous captured frame: 0.001212000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 33.776369000 seconds]
    Frame Number: 1967
    Frame Length: 336 bytes (2688 bits)
    Capture Length: 336 bytes (2688 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e), Dst: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
    Destination: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
        Address: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
        Address: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.49, Dst: 77.75.149.208
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 322
    Identification: 0x0c8e (3214)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.49
    Destination Address: 77.75.149.208
Transmission Control Protocol, Src Port: 63395, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
    Source Port: 63395
    Destination Port: 80
    [Stream index: 16]
    [TCP Segment Len: 282]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2199486840
    [Next Sequence Number: 283    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2337377537
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0xa629 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.003157000 seconds]
        [Bytes in flight: 282]
        [Bytes sent since last PSH flag: 282]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.004369000 seconds]
        [Time since previous frame in this TCP stream: 0.001212000 seconds]
    TCP payload (282 bytes)
Hypertext Transfer Protocol
    GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?2a6253800db2a34e HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?2a6253800db2a34e HTTP/1.1\r\n]
            [GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?2a6253800db2a34e HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?2a6253800db2a34e
            Request URI Path: /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab
            Request URI Query: 2a6253800db2a34e
                Request URI Query Parameter: 2a6253800db2a34e
        Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    If-Modified-Since: Fri, 02 Jun 2017 17:39:05 GMT\r\n
    If-None-Match: "80424021c7dbd21:0"\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/pinrulesstl.cab?2a6253800db2a34e]
    [HTTP request 1/1]
    [Response in frame: 1969]
No.     Time           Source                Destination           Protocol Length Info
   1969 33.786083      77.75.149.208         192.168.1.49          HTTP     325    HTTP/1.1 304 Not Modified
Frame 1969: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface \Device\NPF_{E8F1393B-10D6-4491-
A631-26A44CA59FE2}, id 0
    Interface id: 0 (\Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2})
        Interface name: \Device\NPF_{E8F1393B-10D6-4491-A631-26A44CA59FE2}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: May  1, 2021 22:23:31.473208000 Финляндия (лето)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1619897011.473208000 seconds
    [Time delta from previous captured frame: 0.002710000 seconds]
    [Time delta from previous displayed frame: 0.009714000 seconds]
    [Time since reference or first frame: 33.786083000 seconds]
    Frame Number: 1969
    Frame Length: 325 bytes (2600 bits)
    Capture Length: 325 bytes (2600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80), Dst: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
    Destination: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
        Address: IntelCor_88:6b:3e (c8:b2:9b:88:6b:3e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
        Address: ASUSTekC_e5:39:80 (18:31:bf:e5:39:80)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 77.75.149.208, Dst: 192.168.1.49
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 311
    Identification: 0x8068 (32872)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 59
    Protocol: TCP (6)
    Header Checksum: 0x1964 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 77.75.149.208
    Destination Address: 192.168.1.49
Transmission Control Protocol, Src Port: 80, Dst Port: 63395, Seq: 1, Ack: 283, Len: 271
    Source Port: 80
    Destination Port: 63395
    [Stream index: 16]
    [TCP Segment Len: 271]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2337377537
    [Next Sequence Number: 272    (relative sequence number)]
    Acknowledgment Number: 283    (relative ack number)
    Acknowledgment number (raw): 2199487122
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
```

```
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x6ade [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.003157000 seconds]
        [Bytes in flight: 271]
        [Bytes sent since last PSH flag: 271]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.014083000 seconds]
        [Time since previous frame in this TCP stream: 0.002710000 seconds]
    TCP payload (271 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Content-Type: application/vnd.ms-cab-compressed\r\n
    Last-Modified: Fri, 02 Jun 2017 17:39:05 GMT\r\n
    ETag: "80424021c7dbd21:0"\r\n
    Cache-Control: public,max-age=172800\r\n
    Date: Sat, 01 May 2021 19:23:30 GMT\r\n
    Connection: keep-alive\r\n
    X-CCC: UA\r\n
    X-CID: 2\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.009714000 seconds]
    [Request in frame: 1967]
    [Request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?2a6253800db2a34e]
```