

## Part 1 :

The image shows a Wireshark packet capture of an HTTP transaction. The main pane displays the details of a selected packet (No. 132), which is an HTTP 1.1 304 Not Modified response. The packet is from 129.4.9.131 to 132.5.0. The details pane shows the following fields:

- GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?fa7a1cd6d94b3d97 HTTP/1.1
- Connection: Keep-Alive
- Accept: \*/\*
- If-Modified-Since: Fri, 05 Sep 2025 17:00:56 GMT
- If-None-Match: "77413ba5861edc1:0"
- User-Agent: Microsoft-CryptoAPI/10.0
- Host: ctld1.windowsupdate.com
- HTTP/1.1 304 Not Modified
- Content-Type: application/vnd.ms-cab-compressed
- Last-Modified: Fri, 05 Sep 2025 17:00:56 GMT
- ETag: "77413ba5861edc1:0"
- Cache-Control: public,max-age=900
- Date: Sat, 13 Sep 2025 18:12:53 GMT
- Connection: keep-alive
- X-CCC: IT
- X-CID: 2

The packet list pane shows the following packets:

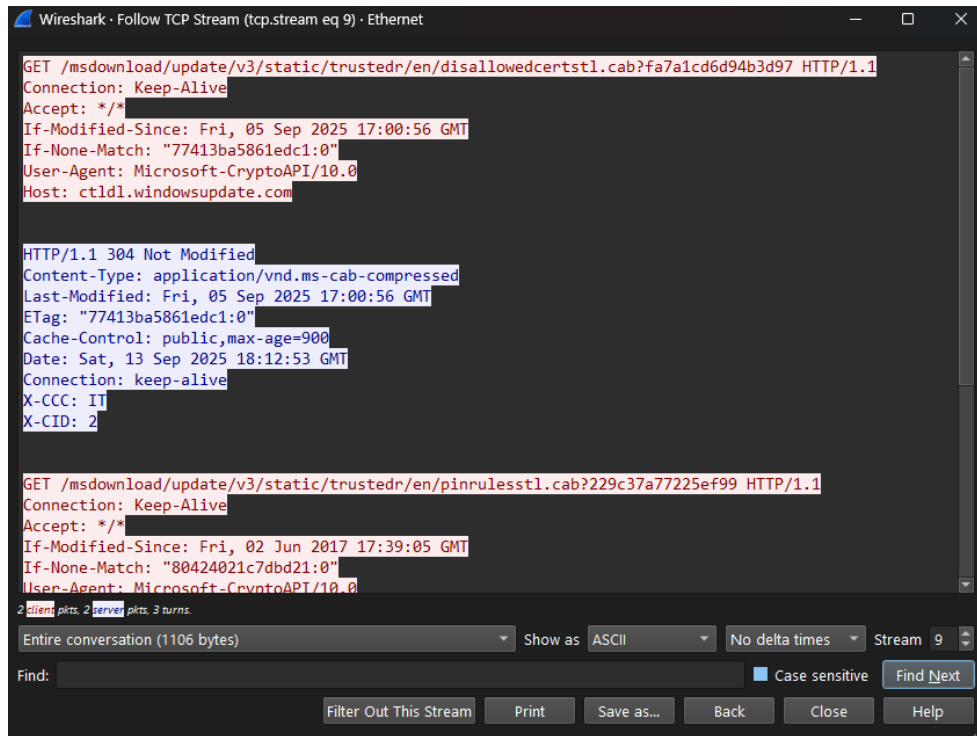
- No. 129, Time 4.9, Source 129.4.9, Destination 131.5.0
- No. 131, Time 5.0, Source 131.5.0, Destination 132.5.0
- No. 132, Time 5.0, Source 132.5.0, Destination 134.5.1
- No. 134, Time 5.1, Source 134.5.1, Destination 176.9.2
- No. 176, Time 9.2, Source 176.9.2, Destination 178.9.3
- No. 178, Time 9.3, Source 178.9.3, Destination 179.9.3
- No. 179, Time 9.3, Source 179.9.3, Destination 181.9.4
- No. 181, Time 9.4, Source 181.9.4, Destination 428.25.
- No. 428, Time 25., Source 428.25., Destination 430.25.
- No. 430, Time 25., Source 430.25., Destination 431.25.
- No. 431, Time 25., Source 431.25., Destination 433.25.
- No. 433, Time 25., Source 433.25., Destination 433.25.

The packet details pane shows the following fields:

- Frame 132:
- Ethernet II
- Internet Protocol Version 4
- Transmission Control Protocol
- Hypertext Transfer Protocol
- GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?229c37a77225ef99 HTTP/1.1
- Connection: Keep-Alive
- Accept: \*/\*
- If-Modified-Since: Fri, 02 Jun 2017 17:39:05 GMT
- If-None-Match: "80424021c7dbd21:0"
- User-Agent: Microsoft-CryptoAPI/10.0
- 2 clients pkts, 2 server pkts, 3 turns.
- Entire conversation (1106 bytes)
- Show as ASCII
- No delta times
- Stream 9
- Find: Case sensitive Find Next
- Filter Out This Stream
- Print
- Save as...
- Back
- Close
- Help

```
Transmission Control Protocol, Src Port: 80, Dst Port: 8072, Seq: 3441111111
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    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, 05 Sep 2025 17:00:56 GMT\r\n
    ETag: "77413ba5861edc1:0"\r\n
```

## Part 2 :



## Three handshake:

126	4.867882	2001:16a2:2e4d:6300::2a02:26f0:1d00::5f6...	2a02:26f0:1d00::5f6...	TCP	86 58772 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM	
127	4.948296	2a02:26f0:1d00::5f6...	2001:16a2:2e4d:6300::2a02:26f0:1d00::5f6...	TCP	86 80 → 58772 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1432 SACK_PERM WS...	
128	4.948374	2001:16a2:2e4d:6300::2a02:26f0:1d00::5f6...	2a02:26f0:1d00::5f6...	TCP	74 58772 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0	
129	4.948560	2001:16a2:2e4d:6300::2a02:26f0:1d00::5f6...	2a02:26f0:1d00::5f6...	HTTP	362 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?fa7a...	

167	9.142063	192.168.1.20	3.175.164.14	TCP	54 54007 → 443 [FIN, ACK] Seq=1 Ack=40 Win=252 Len=0	
168	9.142089	3.175.164.14	192.168.1.20	TCP	60 443 → 54007 [FIN, ACK] Seq=40 Ack=1 Win=145 Len=0	
169	9.142112	192.168.1.20	3.175.164.14	TCP	54 54007 → 443 [ACK] Seq=2 Ack=41 Win=252 Len=0	

## Comparing :

TCP or UDP	Reasons	
Reliability and Connection Establishment	<b>Tcp</b> got handshake while <b>udp</b> don't	
Data Integrity and Ordering	<b>Tcp</b> orders data and make sure that it is arrived while <b>udp</b> don't	

	TCP	UDP
Use cases	http,https emails	Videos and lives
Performance	Slow because it make sure of everything	Faster but not reliable