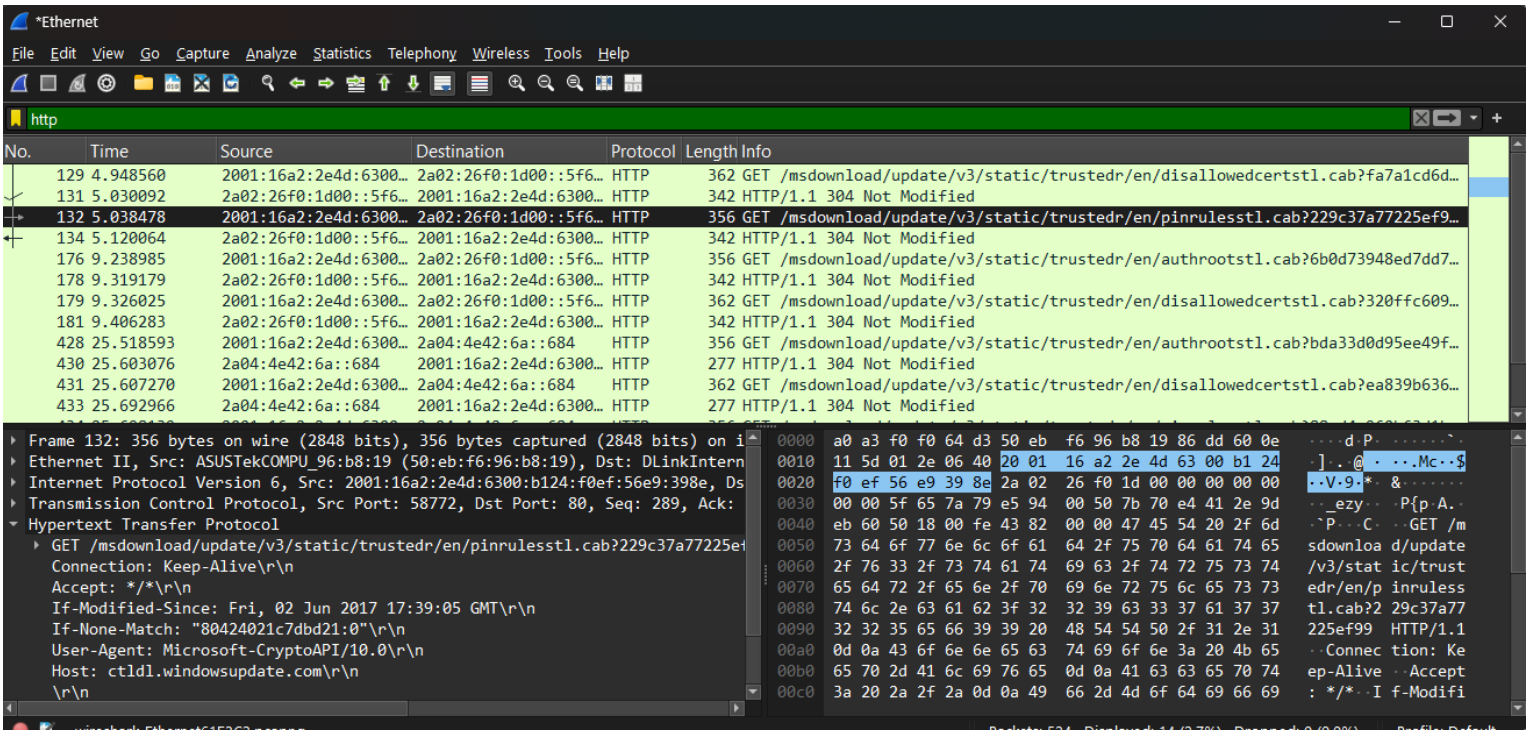
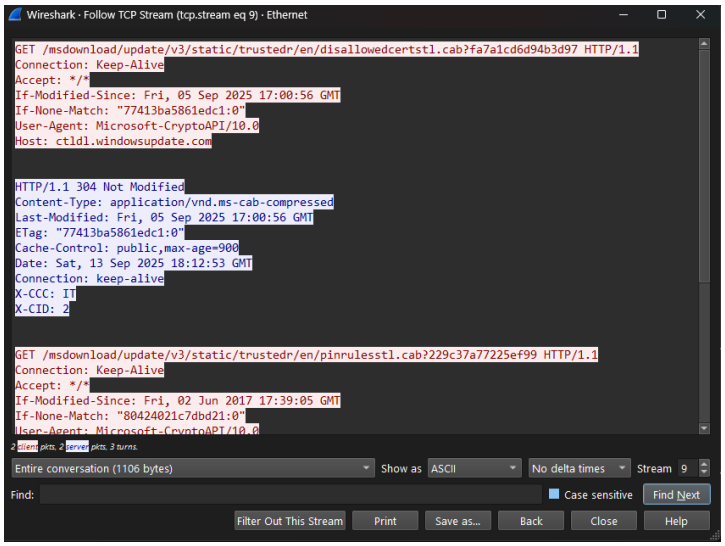
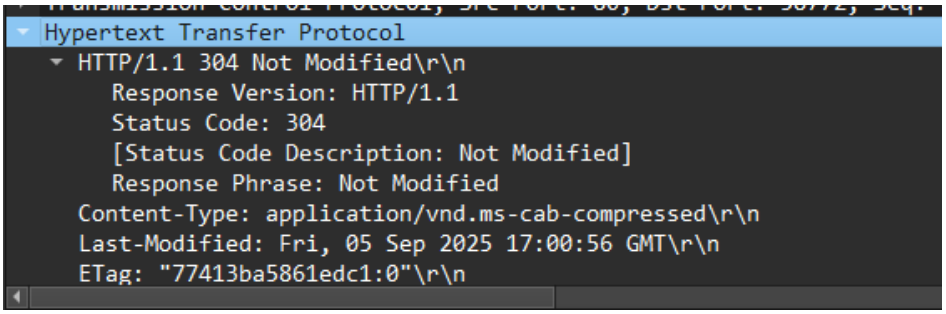
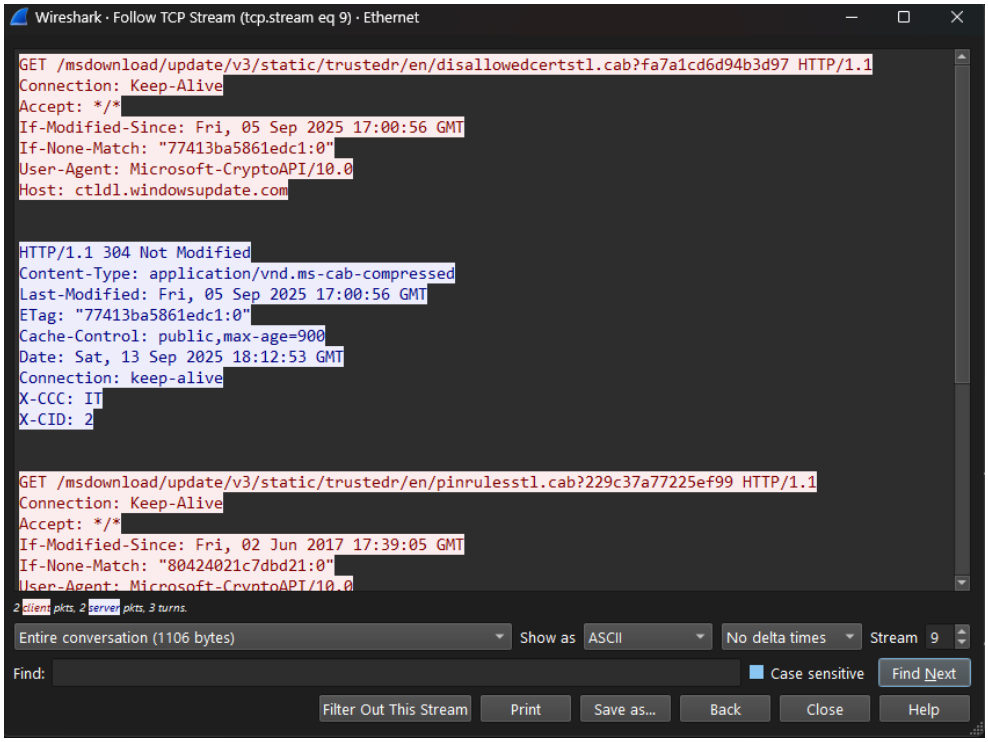
Part 1 :


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
129 4.948560 2001:16a2:2e4d:6300… 2a02:26f0:1d00::5f6… HTTP 362 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?fa7a1cd6d…
131 5.030092 2a02:26f0:1d00::5f6… 2001:16a2:2e4d:6300… HTTP 342 HTTP/1.1 304 Not Modified
132 5.038478 2001:16a2:2e4d:6300… 2a02:26f0:1d00::5f6… HTTP 356 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?229c37a77225ef9…
134 5.120064 2a02:26f0:1d00::5f6… 2001:16a2:2e4d:6300… HTTP 342 HTTP/1.1 304 Not Modified
176 9.238985 2001:16a2:2e4d:6300… 2a02:26f0:1d00::5f6… HTTP 356 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?6b0d73948ed7dd7…
178 9.319179 2a02:26f0:1d00::5f6… 2001:16a2:2e4d:6300… HTTP 342 HTTP/1.1 304 Not Modified
179 9.326025 2001:16a2:2e4d:6300… 2a02:26f0:1d00::5f6… HTTP 362 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?320ffc609…
181 9.406283 2a02:26f0:1d00::5f6… 2001:16a2:2e4d:6300… HTTP 342 HTTP/1.1 304 Not Modified
428 25.518593 2001:16a2:2e4d:6300… 2a04:4e42:6a::684 HTTP 356 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?bda33d0d95ee49f…
430 25.603076 2a04:4e42:6a::684 2001:16a2:2e4d:6300… HTTP 277 HTTP/1.1 304 Not Modified
431 25.607270 2001:16a2:2e4d:6300… 2a04:4e42:6a::684 HTTP 362 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ea839b636…
433 25.692966 2a04:4e42:6a::684 2001:16a2:2e4d:6300… HTTP 277 HTTP/1.1 304 Not Modified
Frame 132: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on i
Ethernet II, Src: ASUSTekCOMPU_96:b8:19 (50:eb:f6:96:b8:19), Dst: DLinkIntern
Internet Protocol Version 6, Src: 2001:16a2:2e4d:6300:b124:f0ef:56e9:398e, Ds
Transmission Control Protocol, Src Port: 58772, Dst Port: 80, Seq: 289, Ack:
Hypertext Transfer Protocol
GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?229c37a77225e
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
0000 a0 a3 f0 f0 64 d3 50 eb f6 96 b8 19 86 dd 60 0e
0010 11 5d 01 2e 06 40 20 01 16 a2 2e 4d 63 00 b1 24
0020 f0 ef 56 e9 39 8e 2a 02 26 f0 1d 00 00 00 00 00
0030 00 00 5f 65 7a 79 e5 94 00 50 7b 70 e4 41 2e 9d
0040 eb 60 50 18 00 fe 43 82 00 00 47 45 54 20 2f 6d
0050 73 64 6f 77 6e 6c 6f 61 64 2f 75 70 64 61 74 65
0060 2f 76 33 2f 73 74 61 74 69 63 2f 74 72 75 73 74
0070 65 64 72 2f 65 6e 2f 70 69 6e 72 75 6c 65 73 73
0080 74 6c 2e 63 61 62 3f 32 32 39 63 33 37 61 37 37
0090 32 32 35 65 66 39 39 20 48 54 54 50 2f 31 2e 31
00a0 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65
00b0 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74
00c0 3a 20 2a 2f 2a 0d 0a 49 66 2d 4d 6f 64 69 66 69

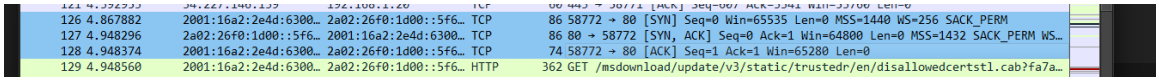

Wireshark · Follow TCP Stream (tcp.stream eq 9) · Ethernet
GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?fa7a1cd6d94b3d97 HTTP/1.1
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Fri, 05 Sep 2025 17:00:56 GMT
If-None-Match: "77413ba5861edc1:0"
User-Agent: Microsoft-CryptoAPI/10.0
Host: ctldl.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
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 client 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

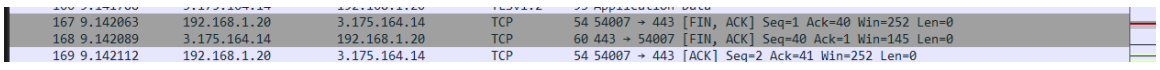

Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Content-Type: application/vnd.ms-cab-compressed\r\n
Last-Modified: Fri, 05 Sep 2025 17:00:56 GMT\r\n
ETag: "77413ba5861edc1:0"\r\n

Part 2 :



Three handshake:





Comparing :

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

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