## Request Packet

## 

## Description of each field

### Application Layer (HTTP Headers)

* GET /DigiCertGlobalRootG2.crl HTTP/1.1 → Requests the file from the server.
* Cache-Control: max-age=4157 → Tells the browser how long it can cache the response.
* Connection: Keep-Alive → Keeps the connection open for more requests.
* Accept: \*/\* → Allows any type of response content.
* If-Modified-Since: Tue, 04 Mar 2025 22:15:13 GMT → Asks the server for an update only if the file has changed since this date.
* If-None-Match: "67c77b71-493" → Asks the server for an update only if the file’s unique identifier (ETag) has changed.
* User-Agent: Microsoft-CryptoAPI/10.0 → Identifies the software making the request.
* Host: crl3.digicert.com → Specifies the destination server.

### Transport Layer (TCP Headers)

* Source Port: 59913 → Identifies the sender’s application process.
* Destination Port: 80 → Identifies the server’s application (HTTP).
* Sequence Number: 1 → Identifies the order of the data in the stream.
* Acknowledgment Number: 1 → Confirms receipt of the last packet.
* Flags (PSH, ACK) → PSH forces data to be sent immediately, ACK confirms receipt.
* Window Size: 65280 → Determines how much data can be sent before waiting for an acknowledgment.

### Network Layer (IP Headers)

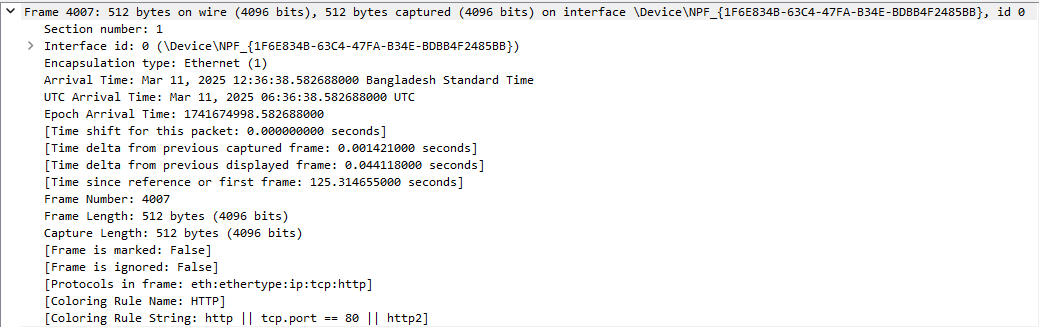
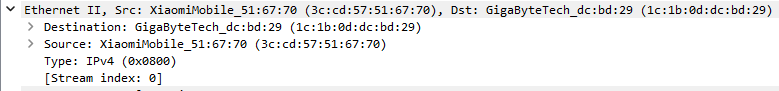
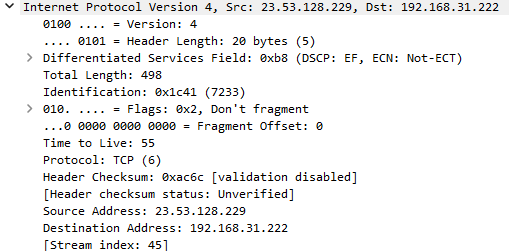
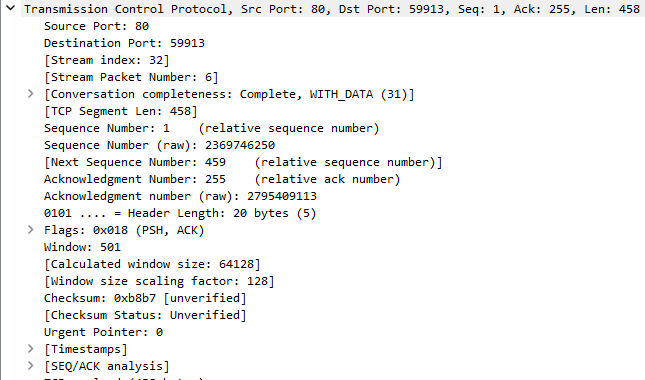
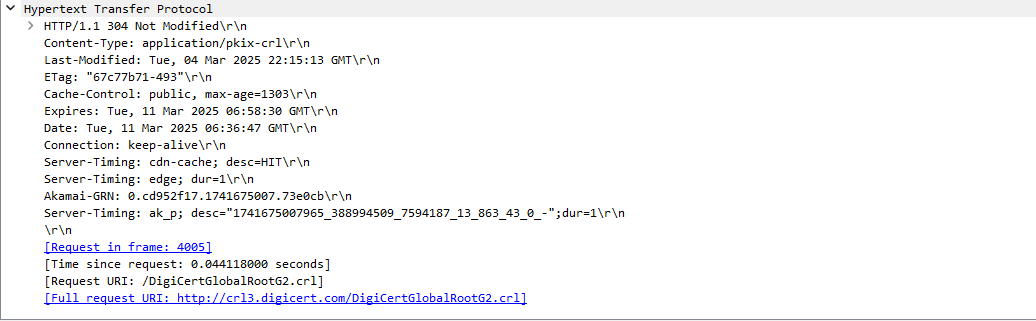
* Source IP: 192.168.31.222 → Identifies the sender’s IP address.
* Destination IP: 23.53.128.229 → Identifies the receiver’s IP address.
* Packet Length: 29 bytes → Specifies the total size of the packet.
* Time to Live (TTL): 12 → Limits how many network hops the packet can take before being discarded.
* Flags (Don't Fragment) → Prevents the packet from being split into smaller parts.

### Data Link Layer (Ethernet Headers)

* Source MAC: 1c:1b:0d:dc:bd:29 → Identifies the sender’s network adapter.
* Destination MAC: 3c:cd:57:51:67:70 → Identifies the recipient’s network adapter.
* Type: IPv4 (0x0800) → Specifies that the packet contains an IPv4 packet.

## 

## Response Packet



## Description of each field

## Application Layer (HTTP Response Headers)

* HTTP/1.1 304 Not Modified → The server indicates that the requested file hasn’t changed, so the client should use its cached version.
* Content-Type: application/pkix-crl → Specifies the type of content in the response (Certificate Revocation List).
* Last-Modified: Tue, 64 Mar 2025 22:15:13 GMT → The last time the file was updated on the server.
* ETag: "67c77b71-493" → A unique identifier for the file’s current version to detect changes.
* Cache-Control: public, max-age=1303 → Tells the browser how long it can cache the file before requesting a new one.
* Expires: Tue, 11 Mar 2025 06:58:30 GMT → The date when the cached response is no longer valid.
* Date: Tue, 11 Mar 2025 06:36:47 GMT → The timestamp when the server sent this response.
* Connection: keep-alive → Keeps the connection open for additional requests.
* Server-Timing: cdn-cache; desc=HIT → Indicates that the response was served from a CDN cache.
* Server-Timing: edge; dur=1 → Shows the processing time at the edge server.
* Akamai-GRN: 0.cd952f17.1741675007.73e0cb → Akamai’s unique tracking ID for debugging purposes.
* Server-Timing: ak\_p; desc="1741675007965\_388994509\_7594187\_13\_863\_43\_0\_-" → Provides additional Akamai performance metrics.

Transport Layer (TCP Headers)

* Source Port: 80 → The server’s port used for HTTP communication.
* Destination Port: 59913 → The client’s port receiving the response.
* Stream Index: 32 → Identifies the TCP stream within this capture session.
* Stream Packet Number: 6 → The packet’s order within the TCP conversation.
* TCP Segment Length: 458 → The size of the data in this TCP segment.
* Sequence Number: 1 → Identifies the order of bytes sent in the connection.
* Acknowledgment Number: 255 → Confirms the client received previous data.
* Flags (PSH, ACK) → PSH tells the receiver to process data immediately, ACK acknowledges receipt.
* Window Size: 501 → Controls how much data can be sent before waiting for an acknowledgment.
* Checksum: 0xb8b7 [Unverified] → Used for error detection in the TCP segment.
* Urgent Pointer: 0 → Indicates whether there’s urgent data in the segment (not used here).

Network Layer (IPv4 Headers)

* Version: 4 → Specifies IPv4 as the IP version.
* Header Length: 20 bytes (5) → The size of the IP header.
* Differentiated Services Field: 0xb8 (DSCP: EF, ECN: Not-ECT) → Defines priority for Quality of Service (QoS).
* Total Length: 498 → The total size of the IP packet, including headers and data.
* Identification: 0x1c41 (7233) → A unique identifier for fragmenting and reassembling packets.
* Flags: Don't Fragment (0x2) → Prevents packet fragmentation.
* Fragment Offset: 0 → Indicates the packet is not fragmented.
* Time to Live (TTL): 125 → Limits the number of hops before the packet is discarded.
* Protocol: TCP (6) → Specifies that the transport layer protocol used is TCP.
* Header Checksum: 0xac6c [Unverified] → Used to check for errors in the IP header.
* Source Address: 23.53.128.229 → The server’s IP address.
* Destination Address: 192.168.31.222 → The client’s IP address.

Data Link Layer (Ethernet Headers)

* Destination MAC: 1c:1b:0d:dc:bd:29 (GigaByteTech) → The recipient’s MAC address.
* Source MAC: 3c:cd:57:51:67:70 (XiaomiMobile) → The sender’s MAC address.
* Type: IPv4 (0x0800) → Indicates that the payload is an IPv4 packet.

Frame Details

* Frame Number: 4007 → The position of this packet in the capture.
* Frame Length: 512 bytes → The size of the frame, including headers.
* Capture Length: 512 bytes → The amount of data captured from this frame.
* Arrival Time: Mar 11, 2025, 12:36:38 Bangladesh Standard Time → The exact time the frame was received.
* Protocols in Frame: eth:ethertype:ip:tcp:http → The protocols used in this packet.
* Coloring Rule: HTTP → The display filter used in Wireshark to highlight this packet.