

Name : Ashakuzzamanm Odree  
ID: 20301268  
Section: 04

## HTTP REQUEST/GET PACKET

\*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4862	43.767519	172.19.20.84	152.195.38.76	HTTP	350	GET /GeoTrustLSRSACAG1.crt HTTP/1.1
4877	43.819940	152.195.38.76	172.19.20.84	HTTP	99	HTTP/1.1 200 OK (application/pkix-cert)
21057	51.895626	172.19.20.84	199.232.210.172	HTTP	300	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?de3ad8429624f1f2 HTTP/1.1
21059	51.945971	199.232.210.172	172.19.20.84	HTTP	256	HTTP/1.1 304 Not Modified
21170	55.040644	172.19.20.84	199.232.210.172	HTTP	340	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1cad2b7693accff3 HTTP/1.1
21173	55.092602	199.232.210.172	172.19.20.84	HTTP	255	HTTP/1.1 304 Not Modified
21174	55.103962	172.19.20.84	199.232.210.172	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?f176e147b40eea5a HTTP/1.1
21178	55.155702	199.232.210.172	172.19.20.84	HTTP	256	HTTP/1.1 304 Not Modified

> Frame 4862: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface \Device\NPF\_{64E9338A-BA44-4668-A8EB-73DBDB7B22B2}

> Ethernet II, Src: HP\_9d:d0:e6 (bc:e9:2f:9d:d0:e6), Dst: HuaweiTe\_90:a9:0b (c0:f6:ec:90:a9:0b)

> Internet Protocol Version 4, Src: 172.19.20.84, Dst: 152.195.38.76

> Transmission Control Protocol, Src Port: 51917, Dst Port: 80, Seq: 1, Ack: 1, Len: 296

> Hypertext Transfer Protocol

0000 c0 f6 ec 90 a9 0b bc e9 2f 9d d0 e6 08 00 45 00  
0010 01 50 07 a6 40 00 80 06 00 00 ac 13 14 54 98 c3  
0020 26 4c ca cd 00 50 57 10 71 46 c1 79 a7 23 50 18  
0030 04 02 80 b9 00 00 47 45 54 20 2f 47 65 6f 54 72  
0040 75 73 74 54 4c 53 52 53 41 43 41 47 31 2e 63 72  
0050 74 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74  
0060 3a 20 63 61 63 65 72 74 73 2e 67 65 6f 74 72 75  
0070 73 74 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69  
0080 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a  
0090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69  
00a0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73  
00b0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b  
00c0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69  
00d0 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c  
00e0 80 6c 69 0b 65 20 47 05 63 0b 6f 29 20 43 60 72  
00f0 6f 6d 65 2f 31 32 36 2e 30 2e 30 2e 30 20 53 61  
0100 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64 67 2f  
0110 31 32 36 2e 30 2e 30 2e 30 0d 0a 41 63 63 65 70  
0120 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70  
0130 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70  
0140 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55  
0150 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d 0a

## FRAME:

> Frame 4862: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface \Device\NPF\_{64E9338A-BA44-4668-A8EB-73DBDB7B22B2} ^

Section number: 1

> Interface id: 0 (\Device\NPF\_{64E9338A-BA44-4668-A8EB-73DBDB7B22B2})

Encapsulation type: Ethernet (1)

Arrival Time: Jul 4, 2024 17:18:30.801673000 Bangladesh Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1720091910.801673000 seconds

[Time delta from previous captured frame: 0.000111000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 43.767519000 seconds]

Frame Number: 4862

Frame Length: 350 bytes (2800 bits)

Capture Length: 350 bytes (2800 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: HP\_9d:d0:e6 (bc:e9:2f:9d:d0:e6), Dst: HuaweiTe\_90:a9:0b (c0:f6:ec:90:a9:0b)

Frames are part of the data link layer, which handles data transfer. In this situation, frame 4862 contains 350 bytes of data, captured at a specific time. It's linked to HTTP protocols and shows data moving between my PC and this web server.

## **ETHERNET II:**

```
▼ Ethernet II, Src: HP_9d:d0:e6 (bc:e9:2f:9d:d0:e6), Dst: HuaweiTe_90:a9:0b (c0:f6:ec:90:a9:0b)
  > Destination: HuaweiTe_90:a9:0b (c0:f6:ec:90:a9:0b)
  > Source: HP_9d:d0:e6 (bc:e9:2f:9d:d0:e6)
  Type: IPv4 (0x0800)
```

In the Data Link Layer is Ethernet II. An Ethernet frame with its source and destination MAC addresses are seen in the screenshots above.

## **Internet Protocol Version 4:**

```
▼ Internet Protocol Version 4, Src: 172.19.20.84, Dst: 152.195.38.76
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 336
    Identification: 0x07a6 (1958)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.19.20.84
    Destination Address: 152.195.38.76
```

This section belongs to the network layer. The information provided describes an IPv4 packet, where the source IP is my PC's IP address, which is 172.19.20.84, and the destination IP address is this web server's IP, which is 152.195.38.76.

## Transmission Control Protocol(TCP):

```
▼ Transmission Control Protocol, Src Port: 51917, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
  Source Port: 51917
  Destination Port: 80
  [Stream index: 31]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 296]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1460695366
  [Next Sequence Number: 297 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3245975331
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 1026
  [Calculated window size: 262656]
  [Window size scaling factor: 256]
  Checksum: 0x80b9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (296 bytes)
```

This is the TCP segment, which is part of the transport layer. It's about data transmission. The details show that the source port, or my PC's port, is 51917, and the destination port for the server is 80.

## Hypertext Transfer Protocol:

```
▼ Hypertext Transfer Protocol
  > GET /GeoTrustTLRSACAG1.crt HTTP/1.1\r\n
  Host: cacerts.geotrust.com\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://cacerts.geotrust.com/GeoTrustTLRSACAG1.crt]
  [HTTP request 1/1]
  [Response in frame: 4877]
```

This data means to the Application Layer and is part of the HTTP request. The request uses the GET method to retrieve data.

## HTTP RESPONSE PACKET:

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 4877 is selected, showing an HTTP 200 OK response from 152.195.38.76 to 172.19.20.84. The bottom pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The right pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4862	43.767519	172.19.20.84	152.195.38.76	HTTP	350	GET /GeoTrustTL5R5ACAG1.crt HTTP/1.1
4877	43.819940	152.195.38.76	172.19.20.84	HTTP	99	HTTP/1.1 200 OK (application/pkix-cert)
21057	51.895626	172.19.20.84	199.232.210.172	HTTP	300	GET /msdownload/update/v3/static/trustedr/en/authrootst1.cab?de3ad8429624f1f2 HTTP/1.1
21059	51.945971	199.232.210.172	172.19.20.84	HTTP	256	HTTP/1.1 304 Not Modified
21170	55.040644	172.19.20.84	199.232.210.172	HTTP	340	GET /msdownload/update/v3/static/trustedr/en/disallowedcertst1.cab?1cad2b7693acff3 HTTP/1.1
21173	55.092602	199.232.210.172	172.19.20.84	HTTP	255	HTTP/1.1 304 Not Modified
21174	55.103962	172.19.20.84	199.232.210.172	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootst1.cab?f176e147b40ee5a HTTP/1.1
21178	55.155702	199.232.210.172	172.19.20.84	HTTP	256	HTTP/1.1 304 Not Modified

Frame 4877: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF\_{64E9338A-BA44-4668-A8EB-73D8D87B22B2}, id 0  
Ethernet II, Src: HuaweiTe\_90:a9:0b (c0:f6:ec:90:a9:0b), Dst: HP\_9d:d0:e6 (bc:e9:2f:9d:d0:e6)  
Internet Protocol Version 4, Src: 152.195.38.76, Dst: 172.19.20.84  
Transmission Control Protocol, Src Port: 80, Dst Port: 51917, Seq: 1461, Ack: 297, Len: 45  
[2 Reassembled TCP Segments (1505 bytes): #4876(1460), #4877(45)]  
Hypertext Transfer Protocol  
PKIX CERT File Format

0000 bc e9 2f 9d d0 e6 c0 f6 ec 90 a9 d  
0010 00 55 ef 62 00 36 06 15 ca 98 d  
0020 14 54 00 50 ca cd c1 79 ac d7 57 1  
0030 00 83 c9 33 00 00 82 24 61 22 57 d  
0040 39 ad c3 5c 79 66 6c 07 31 4b 20 5  
0050 19 00 ee 1e 12 78 ce 98 f2 5f fb 5  
0060 fa 97 c6

Frame (99 bytes) Reassembled TCP (1505 bytes)

## FRAME:

The image shows the details of frame 4877 in Wireshark. It displays the frame's structure, including the interface ID, encapsulation type, arrival time, epoch time, frame number, and frame length. It also shows the protocols in the frame and the coloring rule string.

```
> Frame 4877: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{64E9338A-BA44-4668-A8EB-73D8D87B22B2}, id 0
  Section number: 1
    > Interface id: 0 (\Device\NPF_{64E9338A-BA44-4668-A8EB-73D8D87B22B2})
      Encapsulation type: Ethernet (1)
      Arrival Time: Jul  4, 2024 17:18:30.854094000 Bangladesh Standard Time
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1720091910.854094000 seconds
      [Time delta from previous captured frame: 0.000000000 seconds]
      [Time delta from previous displayed frame: 0.052421000 seconds]
      [Time since reference or first frame: 43.819940000 seconds]
      Frame Number: 4877
      Frame Length: 99 bytes (792 bits)
      Capture Length: 99 bytes (792 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:http:pkix-cert:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509sat:x509ce:x509ce:x509ce:...]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
```

A frame manages the transfer of data, so it's part of the data link layer. In this case, frame 4877 consists of 99 bytes of data.

## **ETHERNET II:**

```
▼ Ethernet II, Src: HuaweiTe_90:a9:0b (c0:f6:ec:90:a9:0b), Dst: HP_9d:d0:e6 (bc:e9:2f:9d:d0:e6)
  > Destination: HP_9d:d0:e6 (bc:e9:2f:9d:d0:e6)
  > Source: HuaweiTe_90:a9:0b (c0:f6:ec:90:a9:0b)
  Type: IPv4 (0x0800)
```

Ethernet II belongs to the Data Link Layer.

## **Internet Protocol Version 4:**

```
▼ Internet Protocol Version 4, Src: 152.195.38.76, Dst: 172.19.20.84
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 85
    Identification: 0xef62 (61282)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 54
    Protocol: TCP (6)
    Header Checksum: 0x15ca [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 152.195.38.76
    Destination Address: 172.19.20.84
```

This displays details about the IPv4 section, which is part of the network layer. It describes an IPv4 packet where the source IP is the server's IP address, 152.195.38.76 and the destination IP address is my PC's address, 172.19.20.84.

## Transmission Control Protocol(TCP):

```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 51917, Seq: 1461, Ack: 297, Len: 45
  Source Port: 80
  Destination Port: 51917
  [Stream index: 31]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 45]
  Sequence Number: 1461 (relative sequence number)
  Sequence Number (raw): 3245976791
  [Next Sequence Number: 1506 (relative sequence number)]
  Acknowledgment Number: 297 (relative ack number)
  Acknowledgment number (raw): 1460695662
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 131
  [Calculated window size: 67072]
  [Window size scaling factor: 512]
  Checksum: 0xc933 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (45 bytes)
  TCP segment data (45 bytes)
```

This is a TCP segment, which belongs to the transport layer. It signifies a data transmission.

## 2 Reassembled TCP segments:

```
▼ [2 Reassembled TCP Segments (1505 bytes): #4876(1460), #4877(45)]
  [Frame: 4876, payload: 0-1459 (1460 bytes)]
  [Frame: 4877, payload: 1460-1504 (45 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 1505]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4163636570742d52616e6765733a2062797465...]
```

## Hypertext Transfer Protocol:

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Accept-Ranges: bytes\r\n
    Age: 58051\r\n
    cache-control: max-age=172800, public\r\n
    Content-Type: application/pkix-cert\r\n
    Date: Thu, 04 Jul 2024 11:18:30 GMT\r\n
    Etag: "5a286418-491"\r\n
    expires: Sat, 06 Jul 2024 11:18:30 GMT\r\n
    last-modified: Wed, 06 Dec 2017 21:41:44 GMT\r\n
    Server: ECAcc (sgc/56D3)\r\n
    X-Cache: HIT\r\n
  > Content-Length: 1169\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.052421000 seconds]
    [Request in frame: 4862]
    [Request URI: http://cacerts.geotrust.com/GeoTrustTLRSACAG1.crt]
    File Data: 1169 bytes
```

This is the HTTP response, part of the Application Layer. It confirms the request was successful, stating '200 OK' for HTTP version 1.1.

## PKIX CERT File Format:

```
▼ PKIX CERT File Format
  > Certificate (id-at-commonName=GeoTrust TLS RSA CA G1,id-at-organizationalUnitName=www.digicert.com,id-at-organizationName=DigiCert Inc,id-at-cou...
```

It signifies text-based data in the format of HTML.