

# WIRESHARK PART

## Client to Server (Request Packet):

The image shows a Wireshark packet capture window titled "Wi-Fi 2". The main pane displays a list of captured packets. The selected packet is number 487, an HTTP GET request from 192.168.0.106 to 103.230.106.216. The packet details pane on the left shows the following information:

- Section number: 1
- Interface id: 0 (Device\NPF\_{C950F85C-1413-4707-AA50-540496E0580})
- Encapsulation type: Ethernet (1)
- Arrival Time: Oct 22, 2023 22:32:27.336340000 Bangladesh Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1697992347.336340000 seconds
- [Time delta from previous captured frame: 0.003596000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 13.806060000 seconds]
- Frame Number: 487
- Frame Length: 507 bytes (4056 bits)
- Capture Length: 507 bytes (4056 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: TendaTec\_ad:09:d3 (50:2b:73:ad:09:d3), Dst: Tp-LinkT\_65:d8:02 (50:c7:bf:65:d8:02)

The packet bytes pane on the right shows the raw data of the packet, starting with the Ethernet II header (fa f0 46 c9 00 00 47 45) and the HTTP GET request (GET / HTTP/1.1).

Frame is a part of Data-Link layer

| No. | Time      | Source          | Destination     | Protocol | Length | Info   |
|-----|-----------|-----------------|-----------------|----------|--------|--|
| 487 | 13.868696 | 192.168.0.106   | 103.230.106.216 | HTTP     | 507    | GET / HTTP/1.1                                   |
| 488 | 13.871259 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | [TCP Previous segment not captured] Continuation |
| 495 | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | [TCP Previous segment not captured] Continuation |
| 508 | 13.919975 | 192.168.0.106   | 103.230.106.216 | HTTP     | 412    | GET /css/style.css HTTP/1.1                      |
| 513 | 13.926486 | 192.168.0.106   | 103.230.106.216 | HTTP     | 465    | GET /images/govt_logo.png HTTP/1.1               |
| 517 | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 531 | 13.933726 | 192.168.0.106   | 103.230.106.216 | HTTP     | 469    | GET /images/teletalk_logo.png HTTP/1.1           |
| 534 | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535 | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541 | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545 | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 288    | Continuation                                     |
| 552 | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601 | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602 | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603 | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606 | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609 | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610 | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680 | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

|   |      |                         |                         |                    |
|---|------|-------------------------|-------------------------|--------------------|
| > Frame 487: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface \Device\NPF_{C950...} | 0030 | fa f0 46 c9 00 00 47 45 | 54 20 2f 20 48 54 50    | ..F...GE T / HTTP  |
| > Ethernet II, Src: TendaTec_a4:09:d3 (50:2b:73:a4:09:d3), Dst: Tp-LinkT_65:d8:02 (50:c7:bf:65:d8:02)         | 0040 | 2f 31 2e 31 0d 0a 48 6f | 73 74 3a 20 63 73 70 62 | /1.1- Ho st: cspb  |
| > Destination: Tp-LinkT_65:d8:02 (50:c7:bf:65:d8:02)  | 0050 | 2e 74 65 6c 65 74 61 6c | 6b 2e 63 6f 6d 2e 62 64 | .teletalk.com.bd   |
| > Source: TendaTec_a4:09:d3 (50:2b:73:a4:09:d3)   | 0060 | 0d 0a 43 6f 6e 6e 63 74 | 69 6f 6e 3a 20 6b 65    | - Connec tion: ke  |
| > Type: IPv4 (0x0800)   | 0070 | 65 70 2d 61 6c 69 76 65 | 0d 0a 55 70 67 72 61 64 | ep-alive - Upgrad  |
| > Internet Protocol Version 4, Src: 192.168.0.106, Dst: 103.230.106.216                                       | 0080 | 65 2d 49 6e 73 65 63 75 | 72 65 2d 52 65 71 75 65 | e-Insecu re-Reque  |
| > Transmission Control Protocol, Src Port: 1436, Dst Port: 80, Seq: 1, Len: 453                               | 0090 | 73 74 73 3a 20 31 0d 0a | 55 73 65 72 2d 41 67 65 | sts: 1 - User-Age  |
| > Hypertext Transfer Protocol   | 00a0 | 6e 74 3a 20 4d 6f 7a 69 | 6c 6c 61 2f 35 2e 30 2e | nt: Mozilla/5.0    |
|   | 00b0 | 28 57 69 6e 64 6f 77 73 | 20 4e 54 20 31 30 2e 30 | (Windows NT 10.0   |
|   | 00c0 | 3b 20 57 69 6e 36 34 3b | 20 78 36 34 29 20 41 70 | p; Win64; x64) Ap  |
|   | 00d0 | 70 6c 65 57 65 62 4b 69 | 74 2f 35 33 37 2e 33 36 | pleWebKl t/537.36  |
|   | 00e0 | 20 28 4b 48 54 4d 4c 2c | 20 6c 69 6b 65 20 47 65 | (KHTML, like Ge    |
|   | 00f0 | 63 6b 6f 29 20 43 68 72 | 6f 6d 65 2f 31 32 30 2e | cko) Chrome/120.   |
|   | 0100 | 30 2e 30 2e 30 20 53 61 | 65 61 72 69 2f 35 33 37 | 0.0.0.0.50.2nd/537 |
|   | 0110 | 2e 33 36 0d 0a 41 63 63 | 65 70 74 3a 20 74 65 78 | 36; Acc ept: tex   |
|   | 0120 | 74 2f 68 74 6d 6c 2c 61 | 70 70 6c 69 63 61 74 69 | t/html,a pplicati  |
|   | 0130 | 6f 6e 2f 78 68 74 6d 6c | 2b 78 6d 6c 2c 61 70 70 | on/xhtml+xml,app   |
|   | 0140 | 6c 69 63 61 74 69 6f 6e | 2f 78 6d 6c 3b 71 3d 30 | lication /xml;q=0  |
|   | 0150 | 2e 39 2c 69 6d 61 6f 65 | 2f 61 76 69 66 2c 69 6d | .9,image /avif,im  |
|   | 0160 | 61 67 65 2f 77 65 62 70 | 2c 69 6d 61 67 65 2f 61 | age/webp ,image/a  |
|   | 0170 | 70 6e 67 2c 2a 2f 2a 3b | 71 3d 30 2e 38 2c 61 70 | png/*; q=0.8,ap    |
|   | 0180 | 70 6c 69 63 61 74 69 6f | 6e 2f 73 69 67 6e 65 64 | plicatio n/signed  |

Ethernet is part of layer. Here the source is TendaTec which is a network connection device and the destination is Tp-LinkT. From this we got IPV4 address. An IP address is like a digital home address for your device on the internet. It's a unique combination of numbers that helps your computer find and connect to other computers around the world. The senders IP address is 50:2b:73:a4:09:d3 and the destination IP address is 50:c7:bf:65:d8:02.

Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No. | Time      | Source          | Destination     | Protocol | Length | Info   |
|-----|-----------|-----------------|-----------------|----------|--------|--|
| 487 | 13.868696 | 192.168.0.106   | 103.230.106.216 | HTTP     | 507    | GET / HTTP/1.1                                   |
| 488 | 13.872222 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | [TCP Previous segment not captured] Continuation |
| 495 | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | Continuation                                     |
| 508 | 13.919975 | 192.168.0.106   | 103.230.106.216 | HTTP     | 412    | GET /css/style.css HTTP/1.1                      |
| 513 | 13.926486 | 192.168.0.106   | 103.230.106.216 | HTTP     | 465    | GET /images/govt_logo.png HTTP/1.1               |
| 517 | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 531 | 13.933726 | 192.168.0.106   | 103.230.106.216 | HTTP     | 469    | GET /images/teletalk_logo.png HTTP/1.1           |
| 534 | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535 | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541 | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545 | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 280    | Continuation                                     |
| 552 | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680 | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

> Frame 487: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface \Device\NPF\_{C950...} Ethernet II, Src: TendaTec\_a4:09:d3 (50:2b:73:a4:09:d3), Dst: Tp-LinkT\_65:d8:02 (50:c7:bf:65:d8:02)

> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 103.230.106.216

0100 .... = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 493

Identification: 0xab95 (43925)

> 010. .... = Flags: 0x2, Don't fragment

... 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0xab94 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.106

Destination Address: 103.230.106.216

> Transmission Control Protocol, Src Port: 1436, Dst Port: 80, Seq: 1, Ack: 1, Len: 453

> Hypertext Transfer Protocol

0000 fa f0 46 c9 00 00 47 45 54 20 2f 20 48 54 50 0030 --F--GE T / HTTP

0001 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 73 70 62 0040 /1.1- Ho st: cspb

0002 2e 74 65 6c 65 74 61 6c 6b 2e 63 6f 6d 2e 62 64 0050 .teletalk.com.bd

0003 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 0060 - Connec tion: ke

0004 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 0070 ep-alive - Upgrad

0005 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 0080 e-Insecu re-Reque

0006 73 74 73 3a 20 31 0d 0a 65 73 65 72 2d 41 67 65 0090 sts: 1 - User-Age

0007 6e 74 3a 20 4a 6f 7a 69 6c 6e 61 2f 35 2e 30 20 00a0 nt: Moz/1.1a/5.0

0008 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 36 00b0 (Windows NT 10.0

0009 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 00c0 ; Win64; x64) Ap

000a 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 00d0 pleWebK t/537.36

000b 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 00e0 (KHTML, like Ge

000c 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 32 30 2e 00f0 cko) Chr ome/120.

000d 30 2e 30 2e 30 20 53 61 65 61 72 69 2f 35 33 37 0100 0.0.0.0.0.0.0.0

000e 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 0110 36; Acc ept: tex

000f 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 0120 t/html,a plicati

0010 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 0130 on/xhtml+xml,app

0011 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 0140 lication /xml;q=0

0012 2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 0150 .9,image /avif,im

0013 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 0160 age/webp ,image/a

0014 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 0170 png/\*; q=0.8,ap

0015 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 0180 plicatio n/signe

⚡ Hypertext Transfer Protocol (http), 453 bytes

Packets: 2289 · Displayed: 75 (3.3%) · Dropped: 0 (0.0%)

Profile: Default

Internet protocol is the set of rules that let our devices communicate online. It's like the language of the internet, ensuring data can flow smoothly between computers. Here the source is 193:168:0:106 which is my IP address and the destination address is 103:230:106:216. It send a header file of 20bytes. Total length of 493. The protocol is used TCP. Here the error is checked by the checksum. A checksum is like a digital fingerprint that helps verify data integrity. It's used to make sure information hasn't been tampered with during transmission.

| No. | Time      | Source          | Destination     | Protocol | Length | Info   |
|-----|-----------|-----------------|-----------------|----------|--------|--|
| 487 | 13.860696 | 192.168.0.106   | 103.230.106.216 | HTTP     | 507    | GET / HTTP/1.1                                   |
| 488 | 13.872225 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | [TCP Previous segment not captured] Continuation |
| 495 | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | Continuation                                     |
| 508 | 13.919975 | 192.168.0.106   | 103.230.106.216 | HTTP     | 412    | GET /css/style.css HTTP/1.1                      |
| 513 | 13.926486 | 192.168.0.106   | 103.230.106.216 | HTTP     | 465    | GET /images/govt_logo.png HTTP/1.1               |
| 517 | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 531 | 13.933726 | 192.168.0.106   | 103.230.106.216 | HTTP     | 469    | GET /images/teletalk_logo.png HTTP/1.1           |
| 534 | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535 | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541 | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545 | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 288    | Continuation                                     |
| 552 | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680 | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

| Transmission Control Protocol                             | Src Port: 1436 | Dst Port: 80 | Seq: 1 | Ack: 1 | Len: 453 |
|---|----------------|--------------|--------|--------|----------|
| [Stream index: 8]   |                |              |        |        |          |
| [Conversation completeness: Incomplete, DATA (15)]        |                |              |        |        |          |
| [TCP Segment Len: 453]                                    |                |              |        |        |          |
| Sequence Number: 1 (relative sequence number)             |                |              |        |        |          |
| Sequence Number (raw): 2366330005                         |                |              |        |        |          |
| [Next Sequence Number: 454 (relative sequence number)]    |                |              |        |        |          |
| Acknowledgment Number: 1 (relative ack number)            |                |              |        |        |          |
| Acknowledgment number (raw): 213471956                    |                |              |        |        |          |
| 0101 .... = Header Length: 20 bytes (5)                   |                |              |        |        |          |
| Flags: 0x018 (PSH, ACK)                                   |                |              |        |        |          |
| Window: 64240   |                |              |        |        |          |
| [Calculated window size: 64240]                           |                |              |        |        |          |
| [Window size scaling factor: -2 (no window scaling used)] |                |              |        |        |          |
| Checksum: 0x46c9 (unverified)                             |                |              |        |        |          |
| [Checksum Status: Unverified]                             |                |              |        |        |          |
| Urgent Pointer: 0   |                |              |        |        |          |

In transmission protocol the port address is used. The destination port address is 80 which is used to send and receive unencrypted web pages and the sender port address id 1436 which is a dynamic and random port assigned for the sender end. Here checksum is also used to maintain the integrity of data.

| No. | Time      | Source          | Destination     | Protocol | Length | Info   |
|-----|-----------|-----------------|-----------------|----------|--------|--|
| 487 | 13.860696 | 192.168.0.106   | 103.230.106.216 | HTTP     | 507    | GET / HTTP/1.1                                   |
| 488 | 13.872225 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | [TCP Previous segment not captured] Continuation |
| 495 | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | Continuation                                     |
| 508 | 13.919975 | 192.168.0.106   | 103.230.106.216 | HTTP     | 412    | GET /css/style.css HTTP/1.1                      |
| 513 | 13.926486 | 192.168.0.106   | 103.230.106.216 | HTTP     | 465    | GET /images/govt_logo.png HTTP/1.1               |
| 517 | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 531 | 13.933726 | 192.168.0.106   | 103.230.106.216 | HTTP     | 469    | GET /images/teletalk_logo.png HTTP/1.1           |
| 534 | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535 | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541 | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545 | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 288    | Continuation                                     |
| 552 | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610 | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680 | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

| Hypertext Transfer Protocol   |
|---|
| GET / HTTP/1.1\r\n  |
| Host: cspb.teletalk.com.bd\r\n  |
| Connection: keep-alive\r\n  |
| Upgrade-Insecure-Requests: 1\r\n  |
| User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/0.0.0 Safari/537.36\r\n |
| Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n                |
| Accept-Encoding: gzip, deflate\r\n  |
| Accept-Language: en-US,en;q=0.9,bn;q=0.8,de;q=0.7\r\n   |
| \r\n  |
| [Full request URI: http://cspb.teletalk.com.bd/]  |
| [HTTP request 1/18]   |
| [Next request in frame: 508]  |

Here the 5th layer talks about the transfer protocol. At first the client gives a Get request of HTTP 1.1. The \r\n means carriage return, to get the next line and start from the left corner. The host is cspb.teletalk..com.bd where the request is sending. User-agent means the backend browsing platform which is mozilla here. Then the Accept denotes the accepting formats such as text, html files, image and so on. Accept-language is for the language that will be accepted for getting in return, Here, English and Bangla is set. Then the request URL is given.

## Server to client (Response Packet):

The image shows a Wireshark packet capture of an HTTP response. The top pane displays a list of packets, with packet 517 selected. The middle pane shows the details of packet 517, which is an HTTP response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

| No.  | Time      | Source          | Destination     | Protocol | Length | Info   |
|------|-----------|-----------------|-----------------|----------|--------|--|
| 2260 | 22.881559 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2267 | 23.883701 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2280 | 24.876200 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2284 | 25.874956 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 450  | 13.974259 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | [TCP Previous segment not captured] Continuation |
| 495  | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | Continuation                                     |
| 517  | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 534  | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535  | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541  | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545  | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 280    | Continuation                                     |
| 552  | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601  | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602  | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603  | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606  | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609  | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610  | 13.960088 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680  | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

**Frame 517: 1379 bytes on wire (11032 bits), 1379 bytes captured (11032 bits) on interface \Device\NPF...**

**Section number: 1**

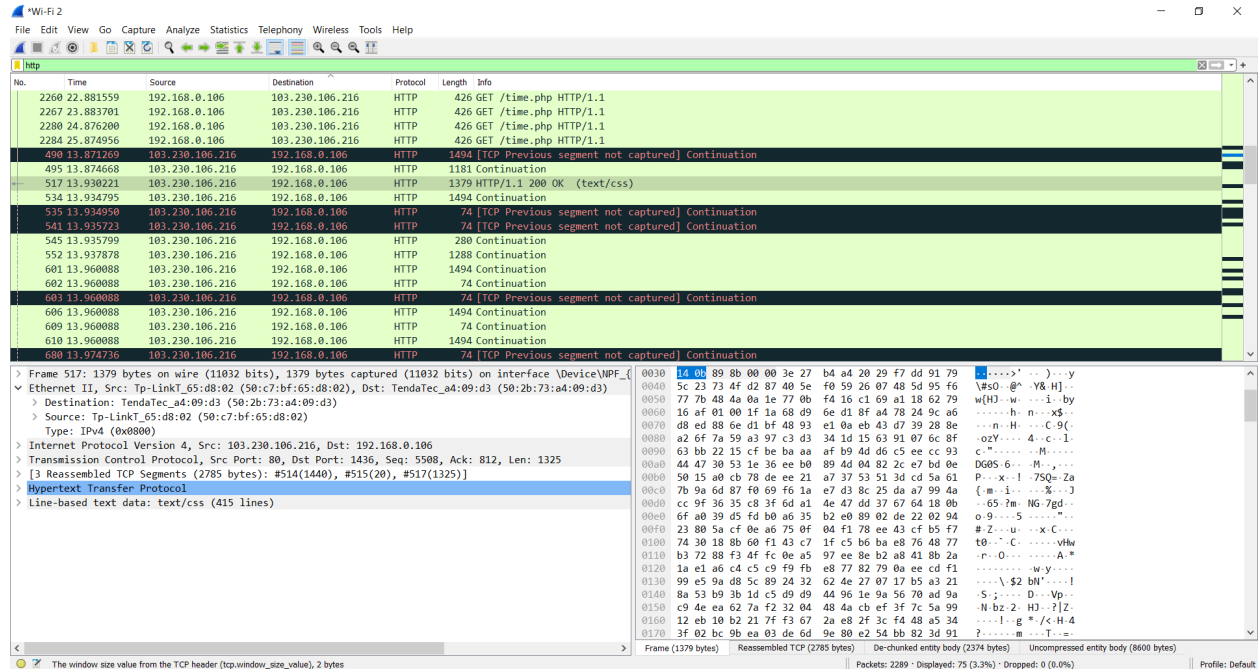
- Interface id: 0 (\Device\NPF\_{C950F85C-1413-4707-AA50-540496E6D580})
- Encapsulation type: Ethernet (1)
- Arrival Time: Oct 22, 2023 22:32:27.405865000 Bangladesh Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1697992347.405865000 seconds
- [Time delta from previous captured frame: 0.001844000 seconds]
- [Time delta from previous displayed frame: 0.000735000 seconds]
- [Time since reference or first frame: 13.930221000 seconds]
- Frame Number: 517
- Frame Length: 1379 bytes (11032 bits)
- Capture Length: 1379 bytes (11032 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:http-data-text-lines]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]

**Ethernet II, Src: Tp-LinkT\_65:d8:02 (50:c7:bf:65:d8:02), Dst: TendaTec\_a4:09:d3 (50:2b:73:a4:09:d3)**

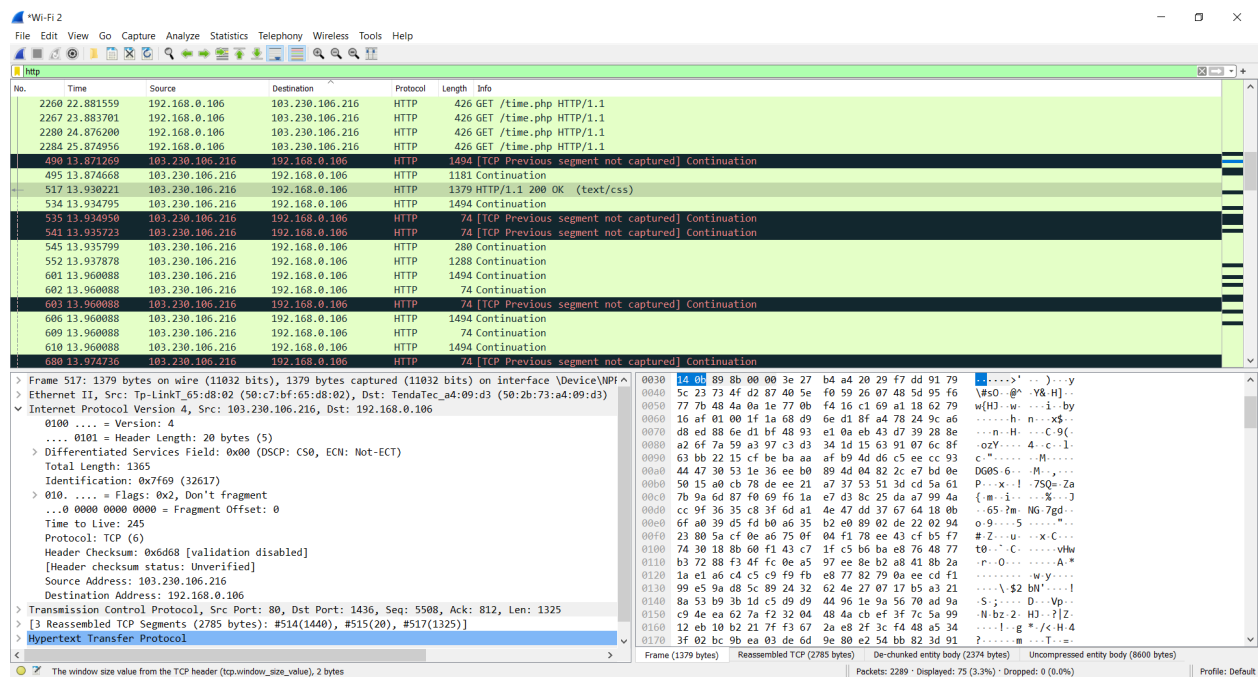
**Raw packet data (hex and ASCII):**

```
0030 14 08 89 8b 00 00 3e 27 b4 a4 20 29 f7 dd 91 79  ....>...y
0040 5c 23 73 4f d2 87 40 5e f0 59 26 07 48 5d 95 f6  \#0-@^Y8H]-
0050 77 7b 48 4a 0a 1e 77 0b f4 16 c1 69 a1 18 62 79  w(H)-w...i-by
0060 16 af 01 00 1f 1a 68 d9 6e d1 8f a4 78 24 9c a6  ....h...x$-
0070 d8 ed 88 6e d1 bf 48 93 e1 0a eb 43 d7 39 28 8e  -n-H...C-9(
0080 a2 6f 7a 59 a3 97 c3 d3 34 1d 15 63 91 07 6c 8f  -oZ...-d...-l
0090 63 bb 22 15 cf be ba aa af b9 4d d6 c5 ee cc 93  c...M...
00a0 44 47 30 53 1e 3e ee b0 89 4d 04 82 2c e7 bd 0e  DG05-6...M...
00b0 50 15 a0 cb 78 de ee 21 a7 37 53 51 3d cd 5a 61  P...x-!-75Q=Za
00c0 7b 9a 6d 87 f0 69 f6 1a e7 d3 8c 25 da a7 99 4a  {m-1...-J
00d0 cc 9f 36 35 c8 3f 6d a1 4e 47 dd 37 67 64 18 0b  -65-7a IG-7gd-
00e0 6f a0 39 d5 fd b0 a6 35 b2 e0 89 02 de 22 02 94  #Z...5...-
00f0 23 80 5a cf 0e a6 75 0f 04 f1 78 ee 43 cf b5 f7  #Z...x-C...
0100 74 30 18 8b 60 f1 43 c7 1f c5 b6 ba e8 76 48 77  t0...C...Vhw
0110 b3 72 88 f3 4f fc 0e a5 97 ee 8e b2 a8 41 8b 2a  -n-0...-A.*
0120 1a e1 a6 c4 c5 c9 f9 fb e8 77 82 79 0a ee cd f1  -n-0...-w.y...
0130 99 e5 9a d8 5c 89 24 32 62 4e 27 07 17 b5 a3 21  -...$2 BN'...-l
0140 8a 53 b9 3b 1d c5 d9 d9 44 96 1e 9a 56 70 ad 9a  -S...-D...Vp...
0150 c9 4e ea 62 7a f2 32 04 48 4a cb ef 3f 7c 5a 99  -N-bz-2-HJ-?Z-
0160 12 eb 10 b2 21 7f f3 67 2a e8 2f 3c f4 48 a5 34  -...-g */<-H-4
0170 3f 02 bc 9b ea 03 de 6d 9e 80 e2 54 b6 82 3d 91  ?...m...T...=
```

Frame is a part of Data-Link layer



Here the IP addresses got swapped. The destination IP address is 50:2b:73:a4:09:d3 and the sender or client's IP address is 50:c7:bf:65:d8:02.



Here the destination is 193:168:0:106 which is my IP address and the source address is 103:230:106:216. It send a header file of 20bytes. The protocol is used TCP. Here the error is checked by the checksum.



Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

| No.  | Time      | Source          | Destination     | Protocol | Length | Info   |
|------|-----------|-----------------|-----------------|----------|--------|--|
| 2260 | 22.881559 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2267 | 23.083701 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2280 | 24.876200 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2284 | 25.874956 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 490  | 13.871269 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | [TCP Previous segment not captured] Continuation |
| 495  | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | Continuation                                     |
| 517  | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 534  | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535  | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541  | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545  | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 280    | Continuation                                     |
| 552  | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680  | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

> Frame 517: 1379 bytes on wire (11032 bits), 1379 bytes captured (11032 bits) on interface \Device\NPF...  
 > Ethernet II, Src: Tp-LinkT\_65:d8:02 (50:c7:bf:65:d8:02), Dst: TendaTec\_a4:09:d3 (50:2b:73:a4:09:d3)  
 > Internet Protocol Version 4, Src: 103.230.106.216, Dst: 192.168.0.106  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 1436, Seq: 5508, Ack: 182, Len: 1325  
 > Source Port: 80  
 > Destination Port: 1436  
 > [Stream index: 8]  
 > [Conversation completeness: Incomplete, DATA (15)]  
 > [TCP Segment Len: 1325]  
 > Sequence Number: 5508 (relative sequence number)  
 > Sequence Number (raw): 2133477463  
 > [Next Sequence Number: 6833 (relative sequence number)]  
 > Acknowledgment Number: 812 (relative ack number)  
 > Acknowledgment Number (raw): 2366330816  
 > 0101 .... = Header Length: 20 bytes (5)  
 > Flags: 0x018 (PSH, ACK)  
 > Window: 5131  
 > [Calculated window size: 5131]  
 > [Window size scaling factor: -2 (no window scaling used)]

Frame (1379 bytes)   Reassembled TCP (2785 bytes)   De-chunked entity body (2374 bytes)   Uncompressed entity body (8600 bytes)

⚙ The window size value from the TCP header (tcp.window\_size\_value), 2 bytes   Packets: 2289 · Displayed: 75 (3.3%) · Dropped: 0 (0.0%)   Profile: Default

In this specific instance, the source port address is designated as 80, a port employed for the exchange of unencrypted web pages. Meanwhile, the destination's port address is 1436, a dynamically generated and random port allocated to the sender's end. To keep the data segment clear, it used the sequel number which is 5508 here.

Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

| No.  | Time      | Source          | Destination     | Protocol | Length | Info   |
|------|-----------|-----------------|-----------------|----------|--------|--|
| 2260 | 22.881559 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2267 | 23.083701 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2280 | 24.876200 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 2284 | 25.874956 | 192.168.0.106   | 103.230.106.216 | HTTP     | 426    | GET /time.php HTTP/1.1                           |
| 490  | 13.871269 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | [TCP Previous segment not captured] Continuation |
| 495  | 13.874668 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1181   | Continuation                                     |
| 517  | 13.930221 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1379   | HTTP/1.1 200 OK (text/css)                       |
| 534  | 13.934795 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 535  | 13.934950 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 541  | 13.935723 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 545  | 13.935799 | 103.230.106.216 | 192.168.0.106   | HTTP     | 280    | Continuation                                     |
| 552  | 13.937878 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1288   | Continuation                                     |
| 601  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 602  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 603  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |
| 606  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 609  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | Continuation                                     |
| 610  | 13.960888 | 103.230.106.216 | 192.168.0.106   | HTTP     | 1494   | Continuation                                     |
| 680  | 13.974736 | 103.230.106.216 | 192.168.0.106   | HTTP     | 74     | [TCP Previous segment not captured] Continuation |

> [3] Reassembled TCP Segments (2785 bytes): #514(1440), #515(20), #517(1325)]  
 > Hypertext Transfer Protocol  
 > HTTP/1.1 200 OK\r\n  
 > Server: nginx\r\n  
 > Date: Sun, 22 Oct 2023 16:32:19 GMT\r\n  
 > Content-Type: text/css\r\n  
 > Last-Modified: Tue, 20 Sep 2022 06:33:23 GMT\r\n  
 > Transfer-Encoding: chunked\r\n  
 > Connection: keep-alive\r\n  
 > Vary: Accept-Encoding\r\n  
 > ETag: W/"63295eb3-2198"\r\n  
 > Expires: Tue, 21 Nov 2023 16:32:19 GMT\r\n  
 > Cache-Control: max-age=2592000\r\n  
 > Cache-Control: public\r\n  
 > Pragma: public\r\n  
 > Vary: Accept-encoding\r\n  
 > Content-Encoding: gzip\r\n  
 > \r\n  
 > [HTTP response 2/18]

Frame (1379 bytes)   Reassembled TCP (2785 bytes)   De-chunked entity body (2374 bytes)   Uncompressed entity body (8600 bytes)

⚙ The window size value from the TCP header (tcp.window\_size\_value), 2 bytes   Packets: 2289 · Displayed: 75 (3.3%) · Dropped: 0 (0.0%)   Profile: Default

This part is the replay of HTTP. 200 OK means the connection has been set and the site is been connected. Then the server type and date is mentioned. The content type is text which means in return the server will send text format only to the client. The connection to the server will remain active and the expires, cache control is shown. The content got encoded while sending. They used gzip encoding technique. At last the HTTP response is shown.