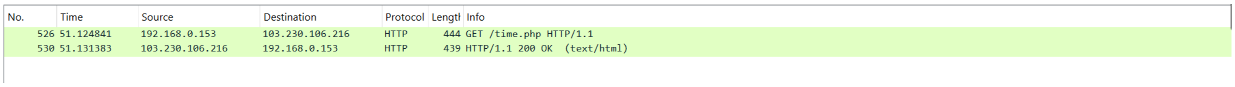
CSE421_Lab 02

Name: Sanzana Mahrukh Hassan
ID: 21101237
Section: 10

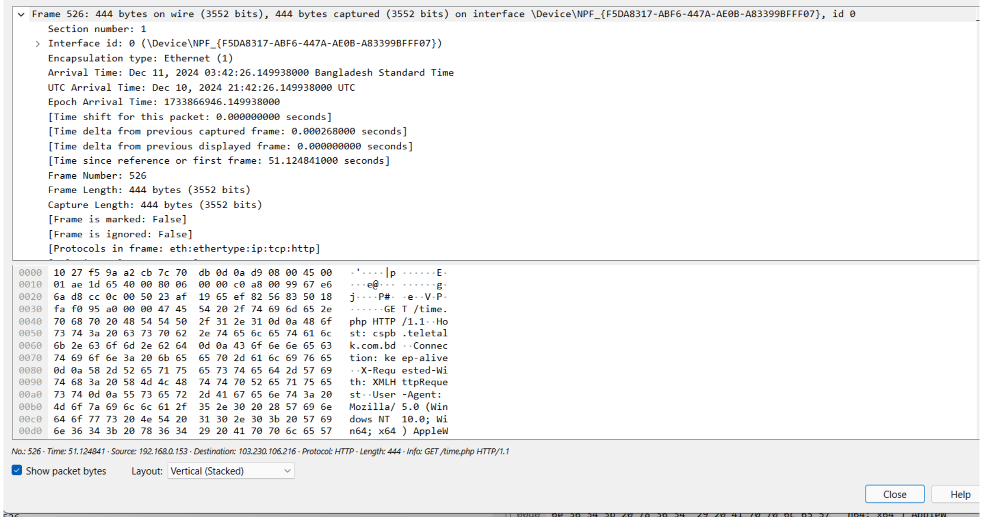
Two HTTP packets are selected, the first packet for HTTP request and the second packet for HTTP response



```
No.  Time       Source          Destination     Protocol Lengtl Info
 526 51.124841  192.168.0.153   103.230.106.216 HTTP      444 GET /time.php HTTP/1.1
 530 51.131383  103.230.106.216 192.168.0.153   HTTP      439 HTTP/1.1 200 OK  (text/html)
```

HTTP Request Packet:

Layer 1



```
v Frame 526: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface \Device\NPF_{F5DA8317-ABF6-447A-AE0B-A83399BFFF07}, id 0
     Section number: 1
   > Interface id: 0 (\Device\NPF_{F5DA8317-ABF6-447A-AE0B-A83399BFFF07})
     Encapsulation type: Ethernet (1)
     Arrival Time: Dec 11, 2024 03:42:26.149938000 Bangladesh Standard Time
     UTC Arrival Time: Dec 10, 2024 21:42:26.149938000 UTC
     Epoch Arrival Time: 1733866946.149938000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.000268000 seconds]
     [Time delta from previous displayed frame: 0.000000000 seconds]
     [Time since reference or first frame: 51.124841000 seconds]
     Frame Number: 526
     Frame Length: 444 bytes (3552 bits)
     Capture Length: 444 bytes (3552 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp:http]
```

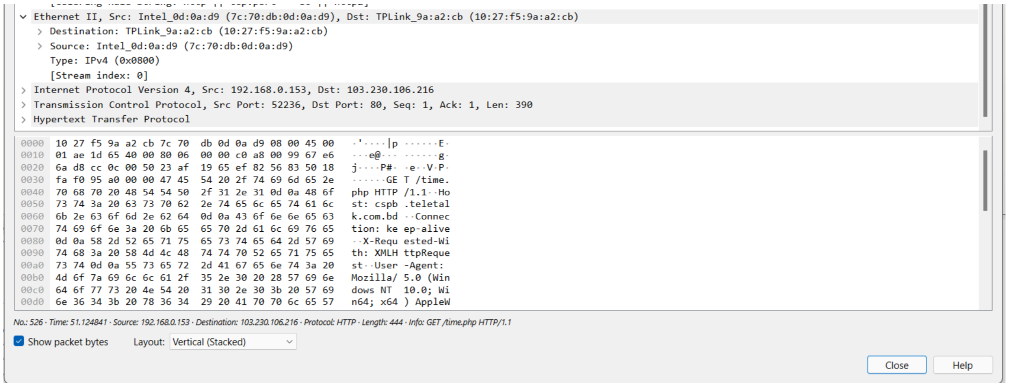
```
0000  10 27 f5 9a a2 cb 7c 70  db 0d 0a d9 08 00 45 00   ·'····|p ······E·
0010  01 ae 1d 65 40 00 80 06  00 00 c0 a8 00 99 67 e6   ···e@··· ······g·
0020  6a d8 cc 0c 00 50 23 af  19 65 ef 82 56 83 50 18   j····P#· ·e··V·P·
0030  fa f0 95 a0 00 00 47 45  54 20 2f 74 69 6d 65 2e   ······GE T /time.
0040  70 68 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   php HTTP /1.1··Ho
0050  73 74 3a 20 63 73 70 62  2e 74 65 6c 65 74 61 6c   st: cspb .teletal
0060  6b 2e 63 6f 6d 2e 62 64  0d 0a 43 6f 6e 6e 65 63   k.com.bd ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 58 2d 52 65 71 75  65 73 74 65 64 2d 57 69   ··X-Requ ested-Wi
0090  74 68 3a 20 58 4d 4c 48  74 74 70 52 65 71 75 65   th: XMLH ttpReque
00a0  73 74 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   st··User -Agent: 
00b0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00c0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00d0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
```

No.: 526 · Time: 51.124841 · Source: 192.168.0.153 · Destination: 103.230.106.216 · Protocol: HTTP · Length: 444 · Info: GET /time.php HTTP/1.1

☑ Show packet bytes   Layout: Vertical (Stacked)

Frame is in the Data Link Layer and it is the physical layer header. From the screenshot, network frame information contains the frame number 526 and a frame length of 444 bytes. It also has arrival time information.

Layer 2



```
⌄ Ethernet II, Src: Intel_0d:0a:d9 (7c:70:db:0d:0a:d9), Dst: TPLink_9a:a2:cb (10:27:f5:9a:a2:cb)
  > Destination: TPLink_9a:a2:cb (10:27:f5:9a:a2:cb)
  > Source: Intel_0d:0a:d9 (7c:70:db:0d:0a:d9)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.0.153, Dst: 103.230.106.216
> Transmission Control Protocol, Src Port: 52236, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
> Hypertext Transfer Protocol
```

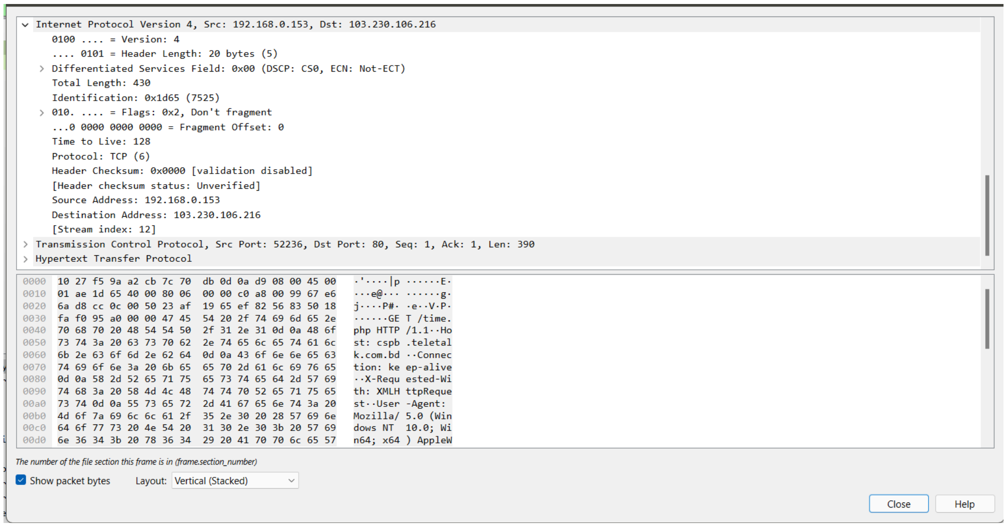
```
0000  10 27 f5 9a a2 cb 7c 70  db 0d 0a d9 08 00 45 00   ·'····|p ······E·
0010  01 ae 1d 65 40 00 80 06  00 00 c0 a8 00 99 67 e6   ···e@··· ······g·
0020  6a d8 cc 0c 00 50 23 af  19 65 ef 82 56 83 50 18   j····P#· ·e··V·P·
0030  fa f0 95 a0 00 00 47 45  54 20 2f 74 69 6d 65 2e   ······GE T /time.
0040  70 68 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   php HTTP /1.1··Ho
0050  73 74 3a 20 63 73 70 62  2e 74 65 6c 65 74 61 6c   st: cspb .teletal
0060  6b 2e 63 6f 6d 2e 62 64  0d 0a 43 6f 6e 6e 65 63   k.com.bd ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 58 2d 52 65 71 75  65 73 74 65 64 2d 57 69   ··X-Requ ested-Wi
0090  74 68 3a 20 58 4d 4c 48  74 74 70 52 65 71 75 65   th: XMLH ttpReque
00a0  73 74 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   st··User -Agent: 
00b0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00c0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00d0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
```

No.: 526 · Time: 51.124841 · Source: 192.168.0.153 · Destination: 103.230.106.216 · Protocol: HTTP · Length: 444 · Info: GET /time.php HTTP/1.1

☑ Show packet bytes Layout: Vertical (Stacked)

This layer is the Data Link Layer, which contains the type and the source and destination MAC addresses for node-to-node data transfer and error detection.

Layer 3



```
⌄ Internet Protocol Version 4, Src: 192.168.0.153, 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: 430
    Identification: 0x1d65 (7525)
  > 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: 192.168.0.153
    Destination Address: 103.230.106.216
    [Stream index: 12]
> Transmission Control Protocol, Src Port: 52236, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
> Hypertext Transfer Protocol
```

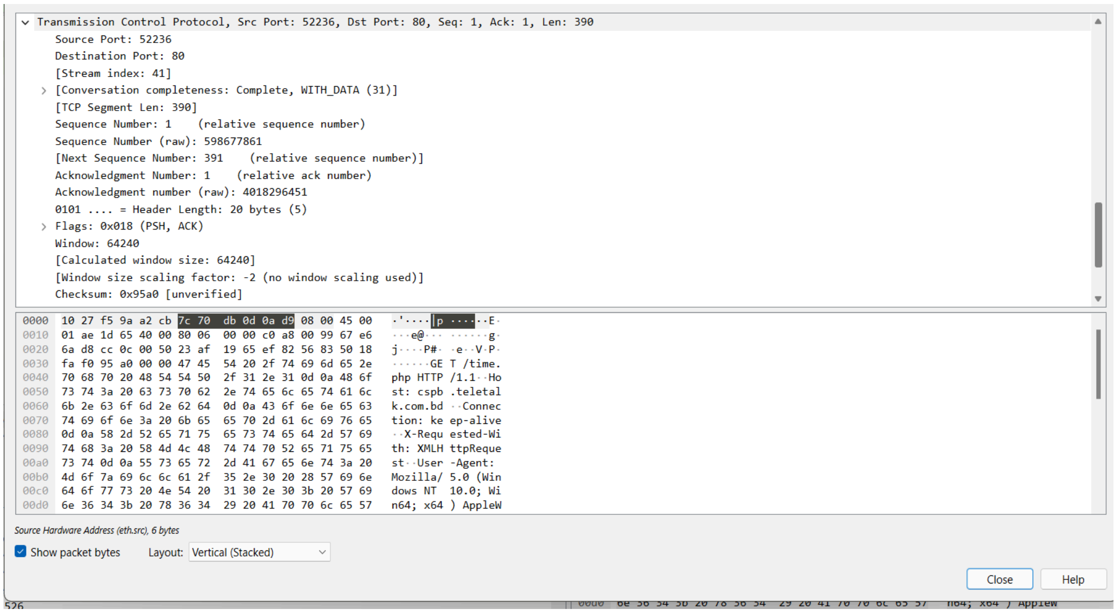
```
0000  10 27 f5 9a a2 cb 7c 70  db 0d 0a d9 08 00 45 00   ·'····|p ······E·
0010  01 ae 1d 65 40 00 80 06  00 00 c0 a8 00 99 67 e6   ···e@··· ······g·
0020  6a d8 cc 0c 00 50 23 af  19 65 ef 82 56 83 50 18   j····P#· ·e··V·P·
0030  fa f0 95 a0 00 00 47 45  54 20 2f 74 69 6d 65 2e   ······GE T /time.
0040  70 68 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   php HTTP /1.1··Ho
0050  73 74 3a 20 63 73 70 62  2e 74 65 6c 65 74 61 6c   st: cspb .teletal
0060  6b 2e 63 6f 6d 2e 62 64  0d 0a 43 6f 6e 6e 65 63   k.com.bd ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 58 2d 52 65 71 75  65 73 74 65 64 2d 57 69   ··X-Requ ested-Wi
0090  74 68 3a 20 58 4d 4c 48  74 74 70 52 65 71 75 65   th: XMLH ttpReque
00a0  73 74 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   st··User -Agent: 
00b0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00c0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00d0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
```

The number of the file section this frame is in (frame.section_number)

☑ Show packet bytes Layout: Vertical (Stacked)

The Network Layer contains the source and destination IP addresses and header information (Header Length=20 bytes) for packet routing and addressing.

Layer 4



```
v Transmission Control Protocol, Src Port: 52236, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
     Source Port: 52236
     Destination Port: 80
     [Stream index: 41]
   > [Conversation completeness: Complete, WITH_DATA (31)]
     [TCP Segment Len: 390]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 598677861
     [Next Sequence Number: 391    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 4018296451
     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: 0x95a0 [unverified]
```

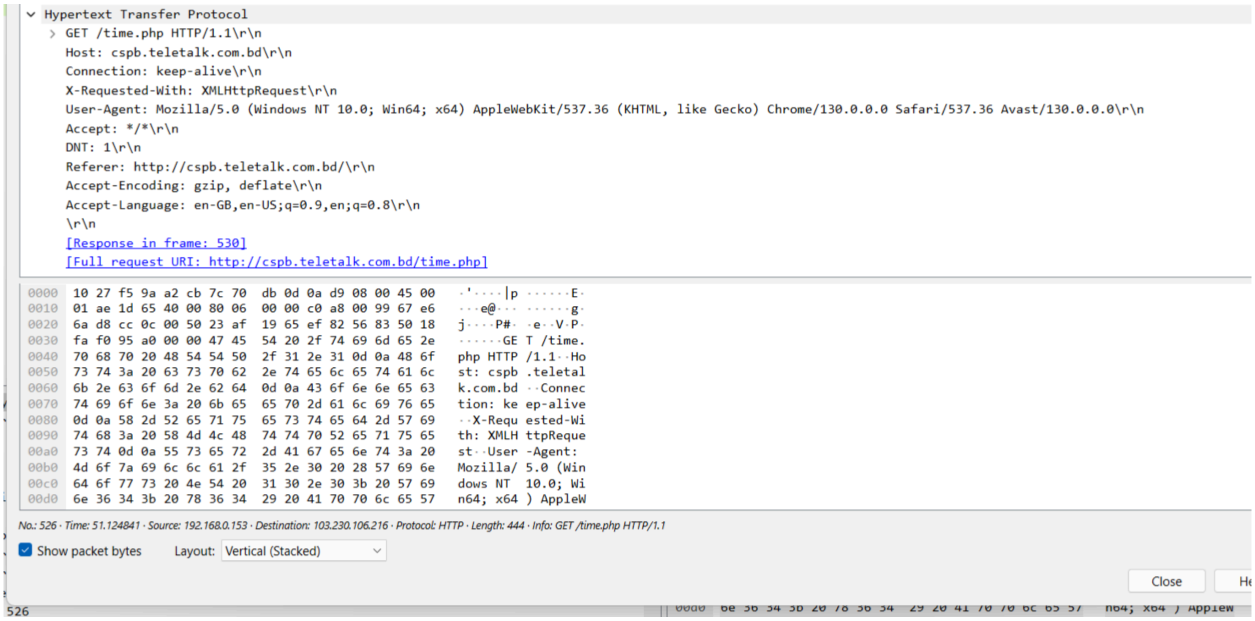
```
0000  10 27 f5 9a a2 cb 7c 70  db 0d 0a d9 08 00 45 00   ·'····|p ······E·
0010  01 ae 1d 65 40 00 80 06  00 00 c0 a8 00 99 67 e6   ···e@··· ······g·
0020  6a d8 cc 0c 00 50 23 af  19 65 ef 82 56 83 50 18   j····P#· ·e··V·P·
0030  fa f0 95 a0 00 00 47 45  54 20 2f 74 69 6d 65 2e   ······GE T /time.
0040  70 68 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   php HTTP /1.1··Ho
0050  73 74 3a 20 63 73 70 62  2e 74 65 6c 65 74 61 6c   st: cspb .teletal
0060  6b 2e 63 6f 6d 2e 62 64  0d 0a 43 6f 6e 6e 65 63   k.com.bd ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 58 2d 52 65 71 75  65 73 74 65 64 2d 57 69   ··X-Requ ested-Wi
0090  74 68 3a 20 58 4d 4c 48  74 74 70 52 65 71 75 65   th: XMLH ttpReque
00a0  73 74 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   st··User -Agent: 
00b0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00c0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00d0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
```

Source Hardware Address (eth.src), 6 bytes

☑ Show packet bytes   Layout: Vertical (Stacked)

The Transport Layer contains the TCP packets and source and destination port addresses, sequence number, acknowledgment number, and length. Here, the source port is 52236 which is a dynamically assigned port number by the client and the destination port is 80 which is the standard port for HTTP traffic on the server. Seq is the Sequence number that tracks the order of the data segments. ACK is the Acknowledgment Number that is used by the receiver to inform the sender which data has been successfully received. LEN is the length that specifies the size of the data segment.

Layer 5



```
Hypertext Transfer Protocol
  > GET /time.php HTTP/1.1\r\n
    Host: cspb.teletalk.com.bd\r\n
    Connection: keep-alive\r\n
    X-Requested-With: XMLHttpRequest\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Avast/130.0.0.0\r\n
    Accept: */*\r\n
    DNT: 1\r\n
    Referer: http://cspb.teletalk.com.bd/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Response in frame: 530]
    [Full request URI: http://cspb.teletalk.com.bd/time.php]
```

```
0000  10 27 f5 9a a2 cb 7c 70  db 0d 0a d9 08 00 45 00   ·'····|p ······E·
0010  01 ae 1d 65 40 00 80 06  00 00 c0 a8 00 99 67 e6   ···e@··· ······g·
0020  6a d8 cc 0c 00 50 23 af  19 65 ef 82 56 83 50 18   j····P#· ·e··V·P·
0030  fa f0 95 a0 00 00 47 45  54 20 2f 74 69 6d 65 2e   ······GE T /time.
0040  70 68 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   php HTTP /1.1··Ho
0050  73 74 3a 20 63 73 70 62  2e 74 65 6c 65 74 61 6c   st: cspb .teletal
0060  6b 2e 63 6f 6d 2e 62 64  0d 0a 43 6f 6e 6e 65 63   k.com.bd ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 58 2d 52 65 71 75  65 73 74 65 64 2d 57 69   ··X-Requ ested-Wi
0090  74 68 3a 20 58 4d 4c 48  74 74 70 52 65 71 75 65   th: XMLH ttpReque
00a0  73 74 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   st··User -Agent: 
00b0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00c0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00d0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
```

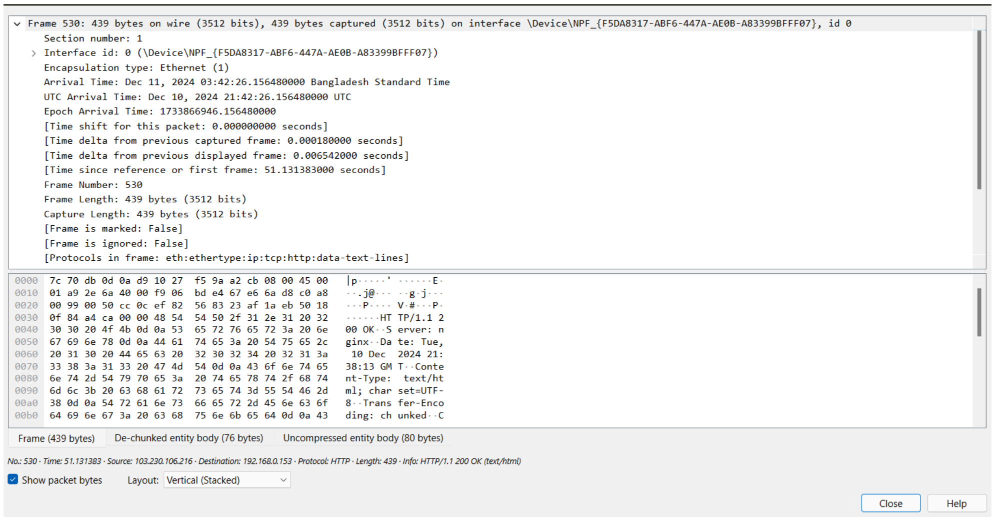
No.: 526 · Time: 51.124841 · Source: 192.168.0.153 · Destination: 103.230.106.216 · Protocol: HTTP · Length: 444 · Info: GET /time.php HTTP/1.1

☑ Show packet bytes   Layout: Vertical (Stacked)

This layer is the Application Layer which contains information about HTTP requests, the GET method since it is a request packet, and also contains information on headers such as Host, Connection, User-Agent, Referrer, Accept-Encoding, and Accept-Language. Connection keep-alive means the connection is on so that it can send data and the accepted language is also mentioned which is English.

HTTP Response Packet:

Layer 1



```
˅ Frame 530: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface \Device\NPF_{F5DA8317-ABF6-447A-AE0B-A83399BFFF07}, id 0
    Section number: 1
  › Interface id: 0 (\Device\NPF_{F5DA8317-ABF6-447A-AE0B-A83399BFFF07})
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 11, 2024 03:42:26.156480000 Bangladesh Standard Time
    UTC Arrival Time: Dec 10, 2024 21:42:26.156480000 UTC
    Epoch Arrival Time: 1733866946.156480000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000180000 seconds]
    [Time delta from previous displayed frame: 0.006542000 seconds]
    [Time since reference or first frame: 51.131383000 seconds]
    Frame Number: 530
    Frame Length: 439 bytes (3512 bits)
    Capture Length: 439 bytes (3512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
```

```
0000  7c 70 db 0d 0a d9 10 27  f5 9a a2 cb 08 00 45 00   |p·····' ······E·
0010  01 a9 2e 6a 40 00 f9 06  bd e4 67 e6 6a d8 c0 a8   ···.j@··· ··g·j···
0020  00 99 00 50 cc 0c ef 82  56 83 23 af 1a eb 50 18   ···P···· V·#···P·
0030  0f 84 a4 ca 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 54 75 65 2c   ginx··Da te: Tue,
0060  20 31 30 20 44 65 63 20  32 30 32 34 20 32 31 3a    10 Dec  2024 21:
0070  33 38 3a 31 33 20 47 4d  54 0d 0a 43 6f 6e 74 65   38:13 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
0090  6d 6c 3b 20 63 68 61 72  73 65 74 3d 55 54 46 2d   ml; char set=UTF-
00a0  38 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   8··Trans fer-Enco
00b0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
```

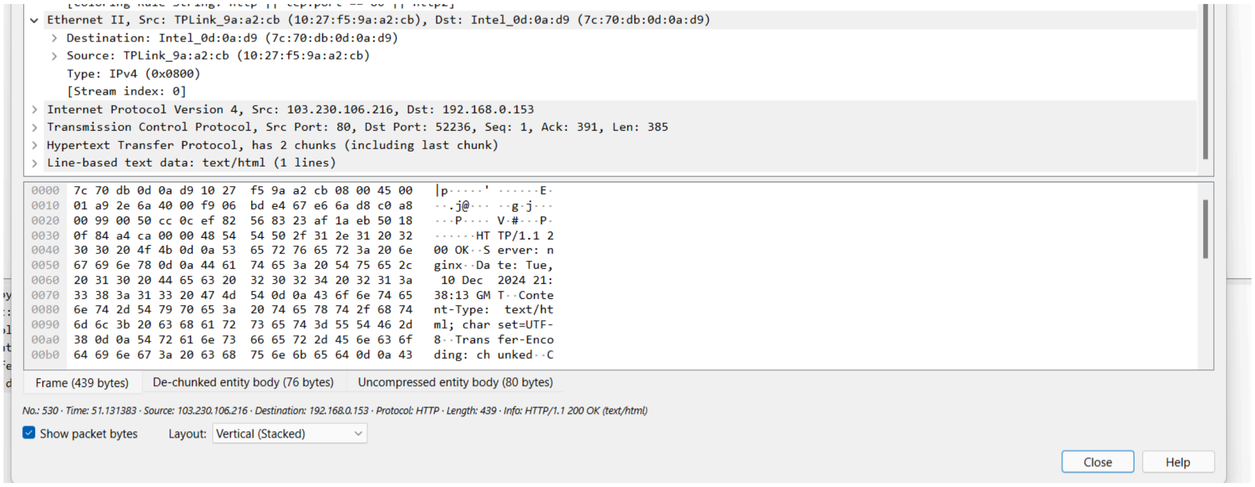
Frame (439 bytes)
De-chunked entity body (76 bytes)
Uncompressed entity body (80 bytes)

No.: 530 · Time: 51.131383 · Source: 103.230.106.216 · Destination: 192.168.0.153 · Protocol: HTTP · Length: 439 · Info: HTTP/1.1 200 OK (text/html)

☑ Show packet bytes   Layout: Vertical (Stacked)

Frame is in the Data Link Layer and it is the physical layer header. Similarly, here for the response, it has the information of frame number: 530, frame length: 439 bytes, and arrival time.

Layer 2



```
˅ Ethernet II, Src: TPLink_9a:a2:cb (10:27:f5:9a:a2:cb), Dst: Intel_0d:0a:d9 (7c:70:db:0d:0a:d9)
  › Destination: Intel_0d:0a:d9 (7c:70:db:0d:0a:d9)
  › Source: TPLink_9a:a2:cb (10:27:f5:9a:a2:cb)
    Type: IPv4 (0x0800)
    [Stream index: 0]
› Internet Protocol Version 4, Src: 103.230.106.216, Dst: 192.168.0.153
› Transmission Control Protocol, Src Port: 80, Dst Port: 52236, Seq: 1, Ack: 391, Len: 385
› Hypertext Transfer Protocol, has 2 chunks (including last chunk)
› Line-based text data: text/html (1 lines)
```

```
0000  7c 70 db 0d 0a d9 10 27  f5 9a a2 cb 08 00 45 00   |p·····' ······E·
0010  01 a9 2e 6a 40 00 f9 06  bd e4 67 e6 6a d8 c0 a8   ···.j@··· ··g·j···
0020  00 99 00 50 cc 0c ef 82  56 83 23 af 1a eb 50 18   ···P···· V·#···P·
0030  0f 84 a4 ca 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 54 75 65 2c   ginx··Da te: Tue,
0060  20 31 30 20 44 65 63 20  32 30 32 34 20 32 31 3a    10 Dec  2024 21:
0070  33 38 3a 31 33 20 47 4d  54 0d 0a 43 6f 6e 74 65   38:13 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
0090  6d 6c 3b 20 63 68 61 72  73 65 74 3d 55 54 46 2d   ml; char set=UTF-
00a0  38 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   8··Trans fer-Enco
00b0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
```

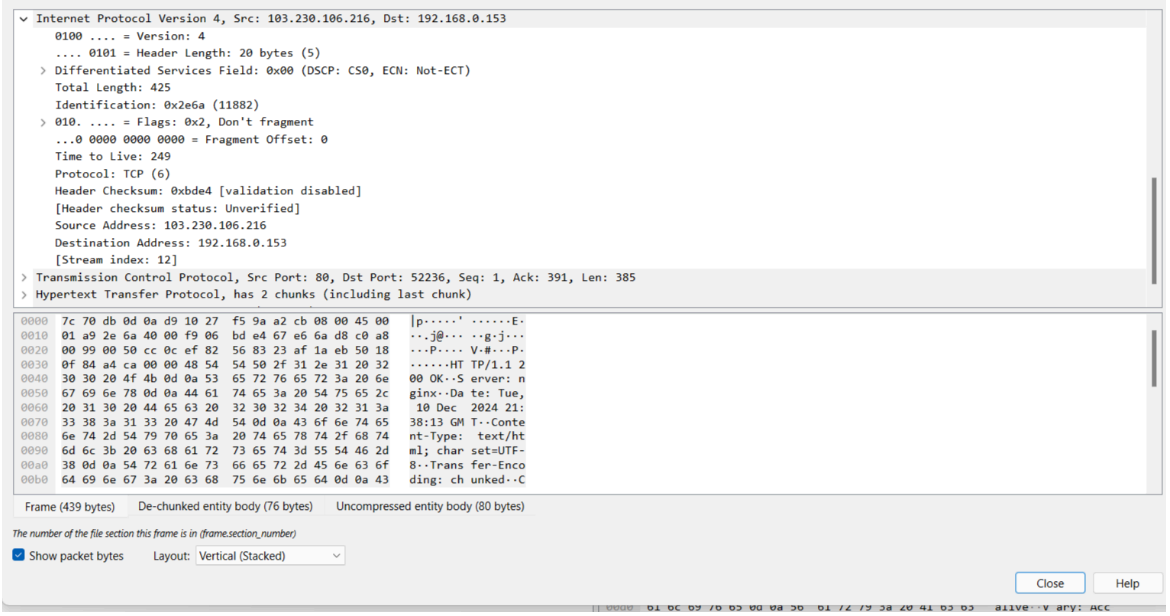
Frame (439 bytes)
De-chunked entity body (76 bytes)
Uncompressed entity body (80 bytes)

No.: 530 · Time: 51.131383 · Source: 103.230.106.216 · Destination: 192.168.0.153 · Protocol: HTTP · Length: 439 · Info: HTTP/1.1 200 OK (text/html)

☑ Show packet bytes   Layout: Vertical (Stacked)

This layer is the Data Link Layer which contains the type source and destination MAC addresses for node-to-node data transfer and error detection.

Layer 3



```
v Internet Protocol Version 4, Src: 103.230.106.216, Dst: 192.168.0.153
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 425
     Identification: 0x2e6a (11882)
   > 010. .... = Flags: 0x2, Don't fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 249
     Protocol: TCP (6)
     Header Checksum: 0xbde4 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 103.230.106.216
     Destination Address: 192.168.0.153
     [Stream index: 12]
> Transmission Control Protocol, Src Port: 80, Dst Port: 52236, Seq: 1, Ack: 391, Len: 385
> Hypertext Transfer Protocol, has 2 chunks (including last chunk)
```

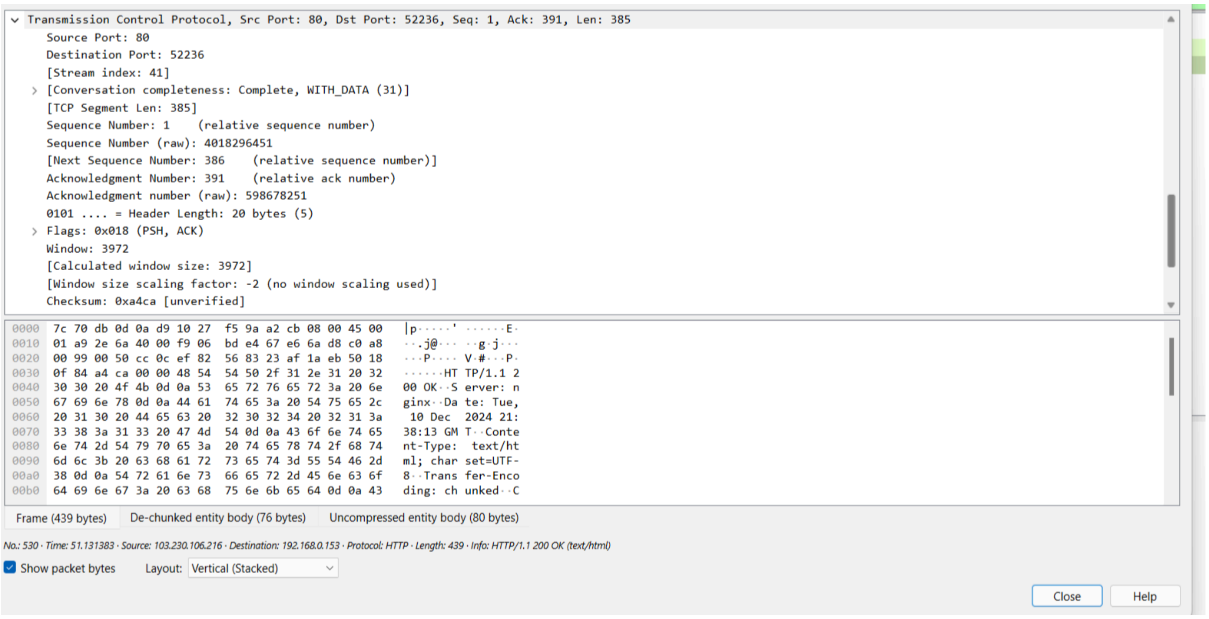
```
0000  7c 70 db 0d 0a d9 10 27  f5 9a a2 cb 08 00 45 00   |p·····' ······E·
0010  01 a9 2e 6a 40 00 f9 06  bd e4 67 e6 6a d8 c0 a8   ···.j@··· ··g·j···
0020  00 99 00 50 cc 0c ef 82  56 83 23 af 1a eb 50 18   ···P···· V·#···P·
0030  0f 84 a4 ca 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 54 75 65 2c   ginx··Da te: Tue,
0060  20 31 30 20 44 65 63 20  32 30 32 34 20 32 31 3a    10 Dec  2024 21:
0070  33 38 3a 31 33 20 47 4d  54 0d 0a 43 6f 6e 74 65   38:13 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
0090  6d 6c 3b 20 63 68 61 72  73 65 74 3d 55 54 46 2d   ml; char set=UTF-
00a0  38 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   8··Trans fer-Enco
00b0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
```

Frame (439 bytes)
De-chunked entity body (76 bytes)
Uncompressed entity body (80 bytes)
The number of the file section this frame is in (frame.section_number)
☑ Show packet bytes
Layout: Vertical (Stacked)
Close
Help

```
61 6c 69 76 65 0d 0a 56  61 72 79 3a 20 41 63 63   alive··V ary: Acc
```

The Network Layer contains the source and destination IP addresses and header information (Header Length=20 bytes) for packet routing and addressing.

Layer 4



```
v Transmission Control Protocol, Src Port: 80, Dst Port: 52236, Seq: 1, Ack: 391, Len: 385
    Source Port: 80
    Destination Port: 52236
    [Stream index: 41]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 385]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4018296451
    [Next Sequence Number: 386    (relative sequence number)]
    Acknowledgment Number: 391    (relative ack number)
    Acknowledgment number (raw): 598678251
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 3972
    [Calculated window size: 3972]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xa4ca [unverified]
```

```
0000  7c 70 db 0d 0a d9 10 27  f5 9a a2 cb 08 00 45 00   |p·····' ······E·
0010  01 a9 2e 6a 40 00 f9 06  bd e4 67 e6 6a d8 c0 a8   ···.j@··· ··g·j···
0020  00 99 00 50 cc 0c ef 82  56 83 23 af 1a eb 50 18   ···P···· V·#···P·
0030  0f 84 a4 ca 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 54 75 65 2c   ginx··Da te: Tue,
0060  20 31 30 20 44 65 63 20  32 30 32 34 20 32 31 3a    10 Dec  2024 21:
0070  33 38 3a 31 33 20 47 4d  54 0d 0a 43 6f 6e 74 65   38:13 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
0090  6d 6c 3b 20 63 68 61 72  73 65 74 3d 55 54 46 2d   ml; char set=UTF-
00a0  38 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   8··Trans fer-Enco
00b0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
```

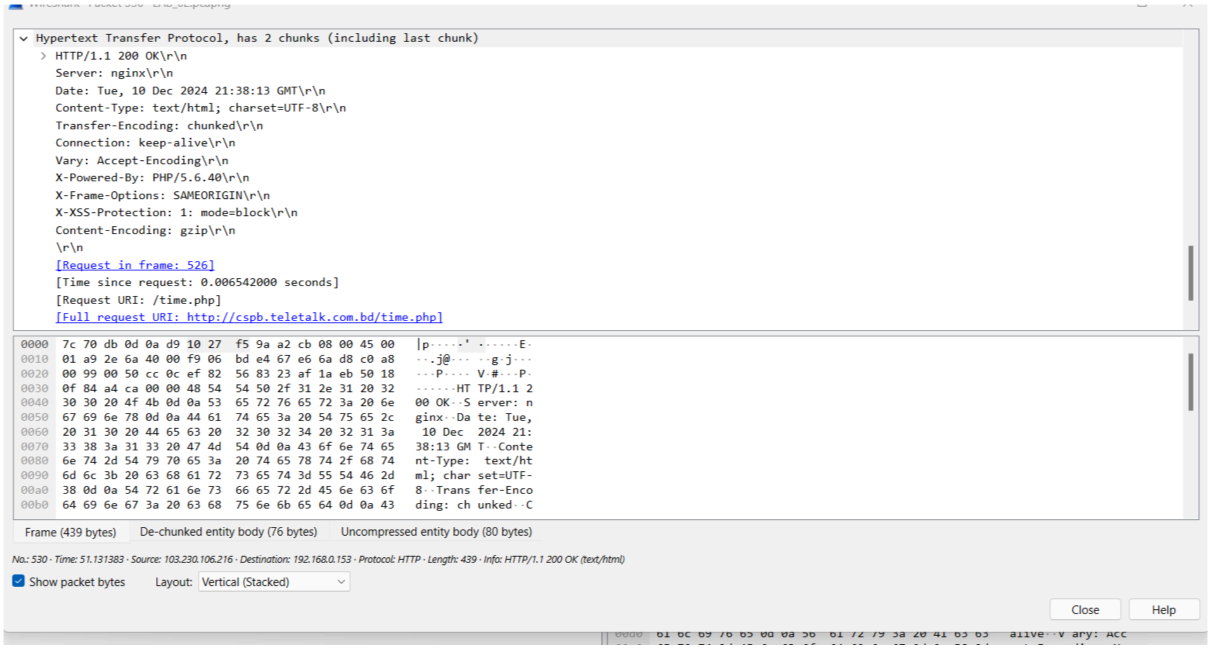
Frame (439 bytes)
De-chunked entity body (76 bytes)
Uncompressed entity body (80 bytes)

No.: 530 · Time: 51.131383 · Source: 103.230.106.216 · Destination: 192.168.0.153 · Protocol: HTTP · Length: 439 · Info: HTTP/1.1 200 OK (text/html)

☑ Show packet bytes   Layout: Vertical (Stacked)

The Transport Layer contains the TCP packets and source and destination port addresses, sequence number, acknowledgment number, and length. Here, the source port is 80 which is used by the server to send HTTP responses. Port 80 is the standard port for HTTP traffic. Destination Port 52236 is a randomly selected port from the client's dynamic port range to receive the HTTP response. Seq is the Sequence number that tracks the order of the data segments. ACK is the Acknowledgment Number used to acknowledge receipt of data. LEN is the length that specifies the size of the data segment.

Layer 5



```
∨ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    Server: nginx\r\n
    Date: Tue, 10 Dec 2024 21:38:13 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Vary: Accept-Encoding\r\n
    X-Powered-By: PHP/5.6.40\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1: mode=block\r\n
    Content-Encoding: gzip\r\n
    \r\n
    [Request in frame: 526]
    [Time since request: 0.006542000 seconds]
    [Request URI: /time.php]
    [Full request URI: http://cspb.teletalk.com.bd/time.php]
```

```
0000  7c 70 db 0d 0a d9 10 27  f5 9a a2 cb 08 00 45 00   |p·····' ······E·
0010  01 a9 2e 6a 40 00 f9 06  bd e4 67 e6 6a d8 c0 a8   ···.j@··· ··g·j···
0020  00 99 00 50 cc 0c ef 82  56 83 23 af 1a eb 50 18   ···P···· V·#···P·
0030  0f 84 a4 ca 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 54 75 65 2c   ginx··Da te: Tue,
0060  20 31 30 20 44 65 63 20  32 30 32 34 20 32 31 3a    10 Dec  2024 21:
0070  33 38 3a 31 33 20 47 4d  54 0d 0a 43 6f 6e 74 65   38:13 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
0090  6d 6c 3b 20 63 68 61 72  73 65 74 3d 55 54 46 2d   ml; char set=UTF-
00a0  38 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   8··Trans fer-Enco
00b0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
```

Frame (439 bytes)
De-chunked entity body (76 bytes)
Uncompressed entity body (80 bytes)

No.: 530 · Time: 51.131383 · Source: 103.230.106.216 · Destination: 192.168.0.153 · Protocol: HTTP · Length: 439 · Info: HTTP/1.1 200 OK (text/html)

☑ Show packet bytes   Layout: Vertical (Stacked)

This layer is the Application Layer which contains the HTTP version (1.1) and Status code 200 (OK) and contains HTTP response headers along with the server name, content length, date, and last modification date.