Dipak Debnath Arka

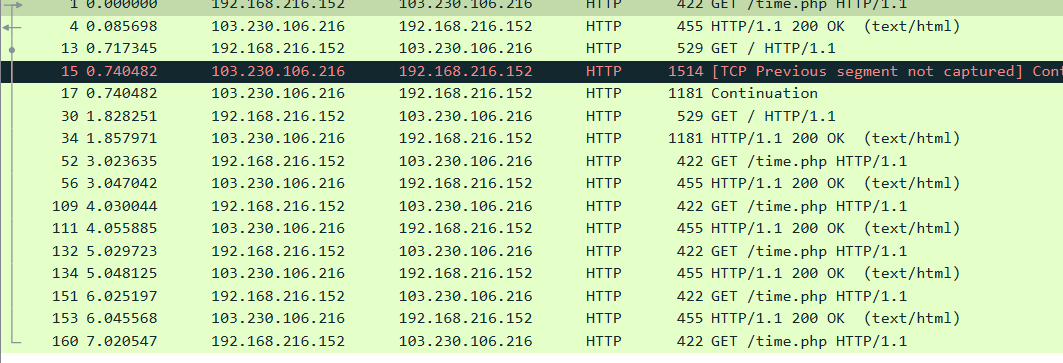
20301066

Sec: 08

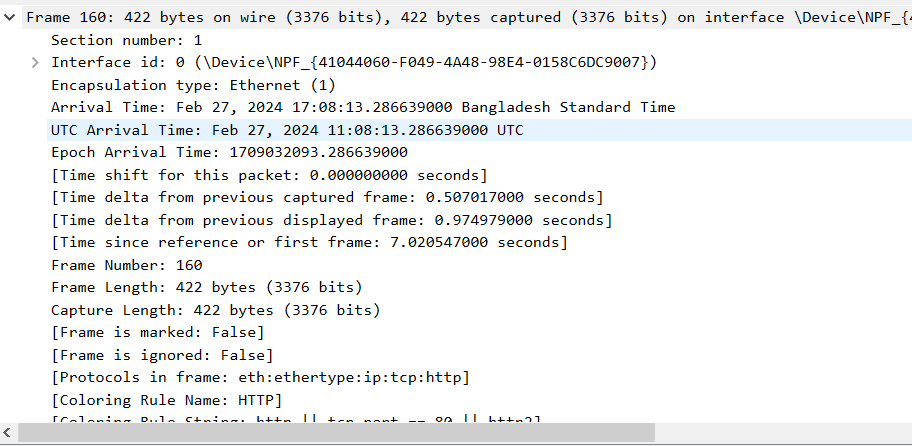
192.168.216.152 > My ip address

103.230.106.216 > Teletalk site ip address

**Wireshark**

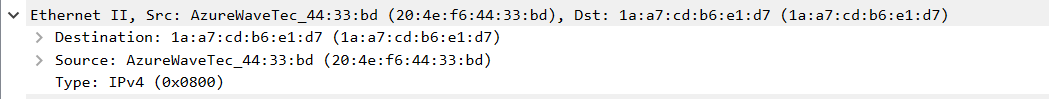


**Frame:**



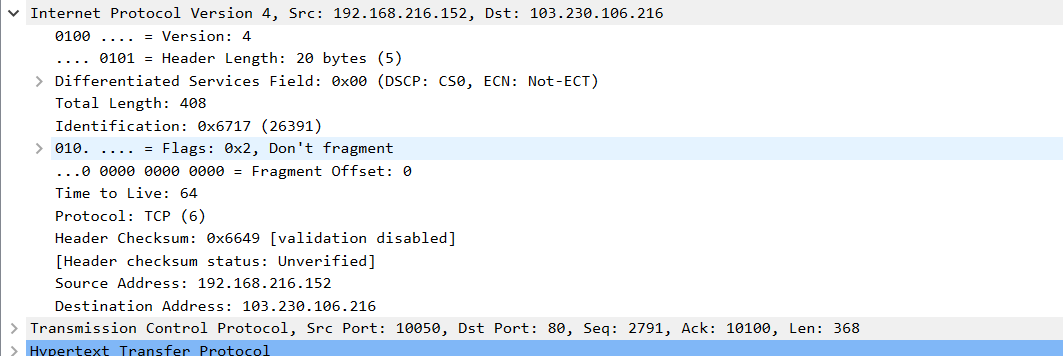
Frame falls under data link layer. Here, it indicates the frame information of this layer protocol of this capture.

**Ethernet:**



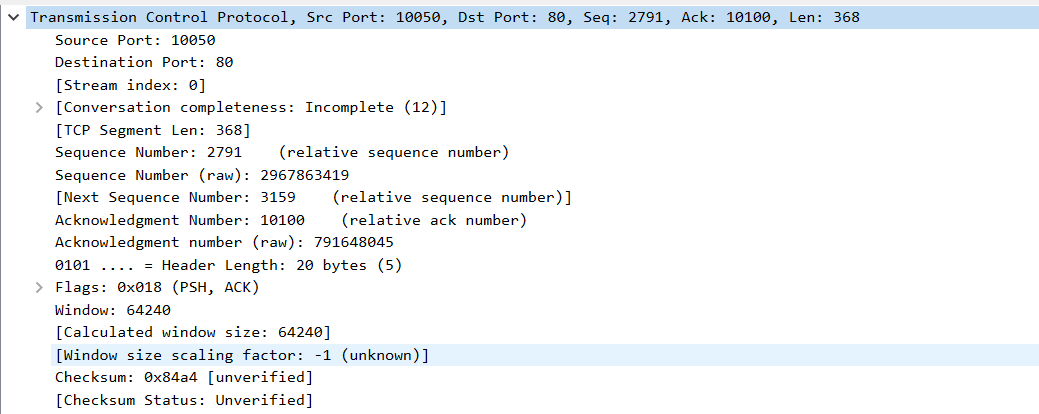
Ethernet2 falls under the datalink layer. The source indicates the device's MAC address that will receive the frame. (1a:a7:cd:b6:e1:d7) this is shown as a human readable name .Also, (1a:a7:cd:66:e1:d7) this is shown as in hexadecimal format .

**Internet Protocol Version 4:**



Here, IPV4 is in network layer. Version 4 indicates that IPV4 is used. Source Ip address is: 192.168.216.152 and Destination ip is: 103.230.106.216. Also, Header length is 20bytes . 5 shown as words. Total length is 408bytes. 0x6717 mentioned in identification is identification number which is assigned to this packet. Flags Dont fragment which indicates these packet should not be fragmented. Fragment offset is 0. TTL is 64. There are 6 TCP protocols. Header checksum number is 0x6649 . Its to verify header integrity. Here, checksum status is unverified and validation disabled.

**Transmission Control Protocol :**



Here, Source port is 10050. This indicates which sending device port started the conversation. Destination port is 80 . This indicates which port on the receiving device the data is meant to be sent to. It means that the conversation is probably a part of an online browsing session. Sequence number is 2791. Raw number is 2967863419. This indicates that the information is received and gathered at the recipient in the right sequence. Next sequence number is 3159 .Acknowledgement number is 10100. It indicates that This value is returned to the sender by the recipient in the acknowledgement (ACK) flag. Raw numbe is 791648045. Flag is 0x018. The PSH ( push flag is set). Also ACK flag is set. Window size is 64240. Checksum value is 0x84a4. The sender computes the checksum, and the recipient confirms it. The status is unverified.

**Hyper text transfer protocol**



Here, The browser is fetching information, as indicated by the "GET" method. The requested file is specifically "/time.php". "cspb.teletalk.com.bd" is the server's address displayed in the "Host" line. "Connection" optimizes performance by asking for the connection to remain open for possible future exchanges. The operating system is (Windows 10) and browser is (Chrome). The "Accept" line demonstrates how well the browser handles different types of data.