WIRESHARK LAB: 802.3 Wired Ethernet

Firstly, we should open ethernet-wireshark-trace1 file which appears in the Figure 1 below;

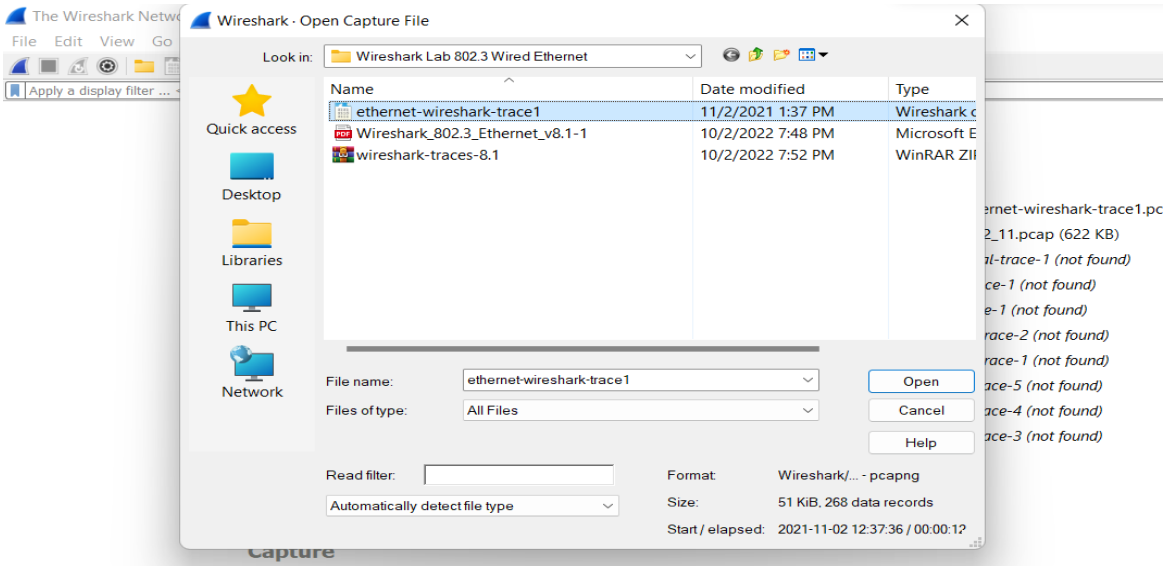

Figure 1: ethernet-wireshark-trace1 File

When we open the file, we receive all the protocols in the packet-listing window. In this lab ARP, MDNS, TCP, and HTTP some of the protocols that appear in the protocol column. Its is shown in the Figure 2 below;

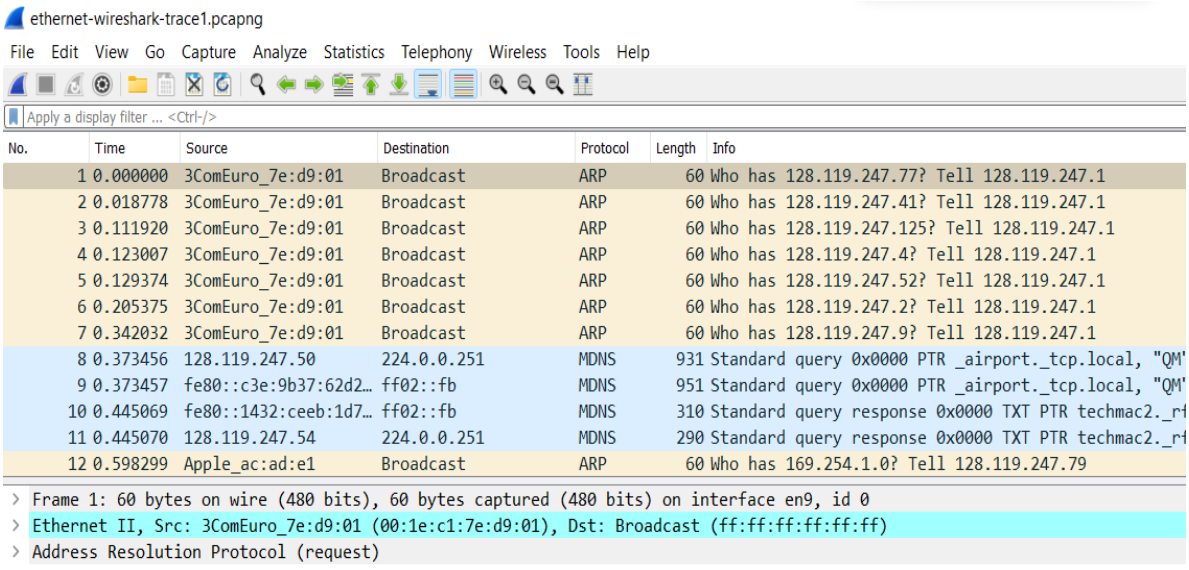

Figure 2: Protocols

To find the HTTP GET request we can use filter by typing HTTP and we can see HTTP GET request is at packet 126. It is shown in the Figure 3.

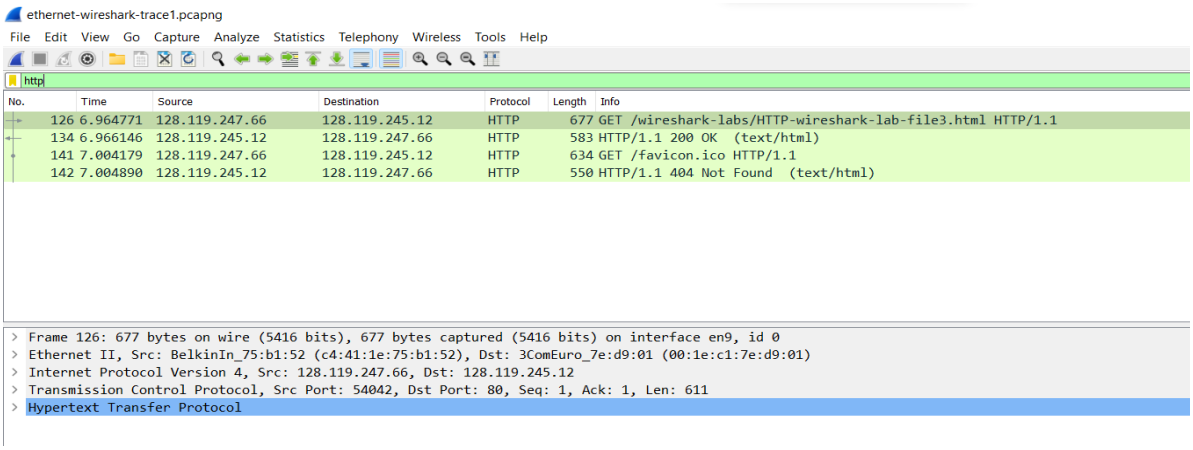

Figure 3: HTTP GET request

1. What is the 48-bit Ethernet address of the client (source) computer?

The Ethernet address of the client computer is c4:41:1e:75:b1:52. It is shown in the Figure 4 below;

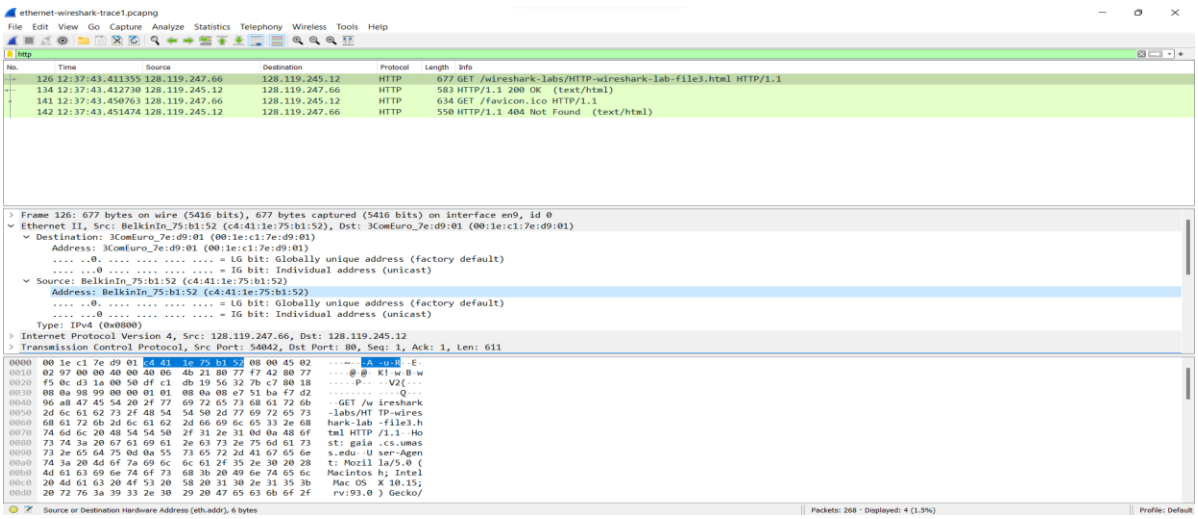

Figure 4: Ethernet address of client

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Hint: Recall that the link layer "knows" only other hosts on the same network.]

The destination address is 00:1e:c1:7e:d9:01 and it is not the Ethernet address of gaia.cs.umass.edu. It is the Ethernet/physical address of 3ComEuro_7e router which my laptop is connected.

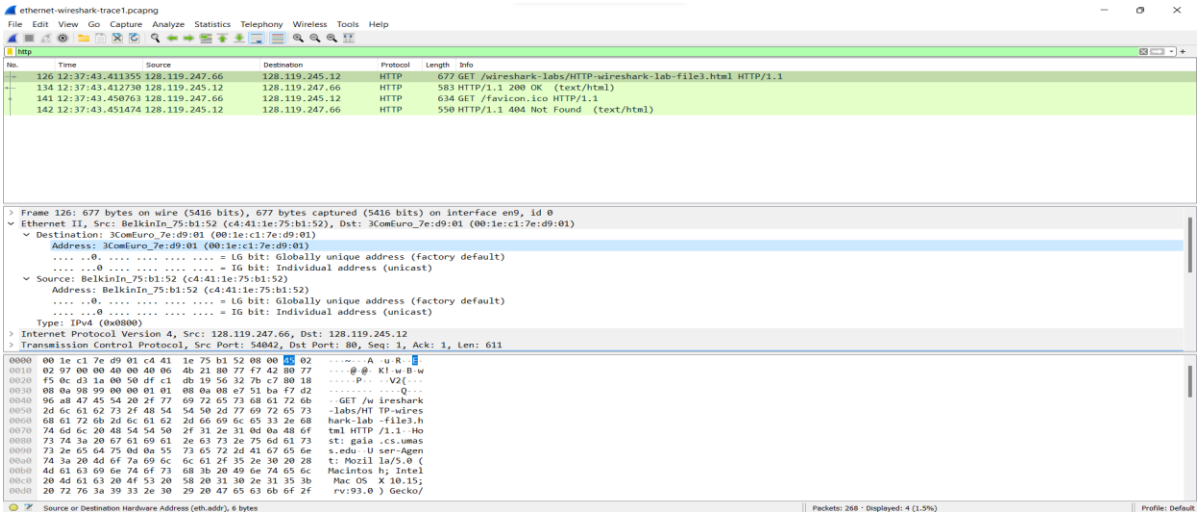

Figure 5: Destination address in the Ethernet frame

3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to? HTTP GET message print:

The hex value for the Frame type field is 0x0800. This corresponds to the IP protocol (the frame type filed indicates that the nest layer above IP – the layer to which the payload of this Ethernet frame will be passed – is IP. It is highlighted in the Figure 6 below;

```
No.     Time        Source                Destination           Protocol Length Info
    126 6.964771    128.119.247.66        128.119.245.12        HTTP     677    GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1
Frame 126: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface en9, id 0
Ethernet II, Src: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
    Destination: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
        Address: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)
        Address: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.247.66, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
Hypertext Transfer Protocol
```

Figure 6: Hex value

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

ASCII “G” in “GET” appear 66 bytes in the Ethernet frame.

The ethernet frame (first 14 bytes containing destination address, source address, and frame type)
• The IP header (20 bytes)

• The TCP header (32 bytes)

It is highlighted in the Figure 7 below;

```
No.     Time        Source                Destination           Protocol Length Info
    126 6.964771    128.119.247.66        128.119.245.12        HTTP     677    GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1
Frame 126: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface en9, id 0
Ethernet II, Src: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
Internet Protocol Version 4, Src: 128.119.247.66, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
Hypertext Transfer Protocol
0000  00 1e c1 7e d9 01 c4 41 1e 75 b1 52 08 00 45 02   ...~...A.u.R..E.
0010  02 97 00 00 40 00 40 06 4b 21 80 77 f7 42 80 77   ....@.@.K!.w.B.w
0020  f5 0c d3 1a 00 50 df c1 db 19 56 32 7b c7 80 18   .....P....V2{...
0030  08 0a 98 99 00 00 01 01 08 0a 08 e7 51 ba f7 d2   ............Q...
0040  96 a8 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b   ..GET /wireshark
0050  2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73   -labs/HTTP-wires
```

Figure 7: Bytes of ASCII “G”

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

As shown in the Figure 8 below, the ethernet source address is 00:1e:c1:7e:d9:01. This is not the Ethernet address of gaia.cs.umass.edu. Rather, it is the Ethernet address of the 3ComEuro_7e router which my computer is connected.

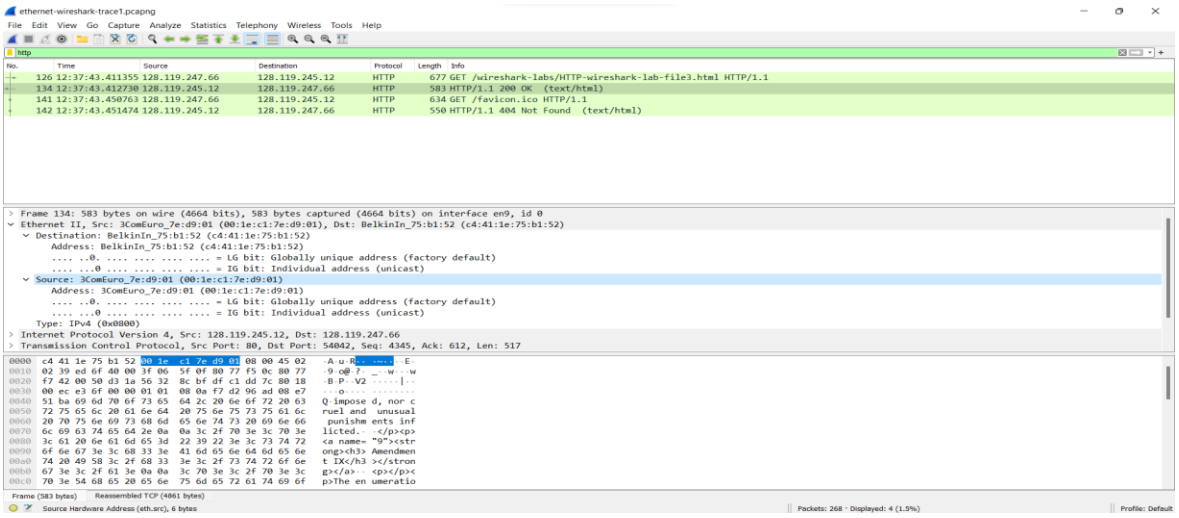

Figure 8: Ethernet Source Address

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of the client computer?

The destinating address c4:41:1e:75:b1:52 is the Ethernet address of the client computer. It is shown in the Figure 9 below;

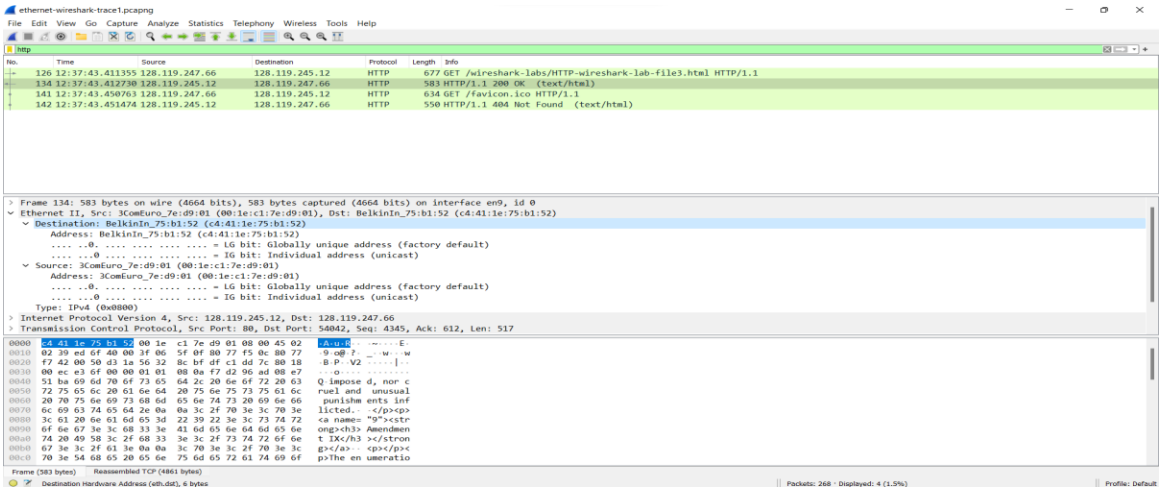

Figure 9: Destination Address in the Ethernet Frame

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hex value for the Frame type field is 0x0800. This corresponds to the IP protocol (the frame type filed indicates that the nest layer above IP – the layer to which the payload of this Ethernet frame will be passed – is IP. It is highlighted in the Figure 10 below;

```
No.     Time        Source                Destination           Protocol Length Info
    134 6.966146    128.119.245.12        128.119.247.66        HTTP     583    HTTP/1.1 200 OK  (text/html)
Frame 134: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en9, id 0
Ethernet II, Src: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)
    Destination: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)
        Address: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
        Address: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.119.247.66
Transmission Control Protocol, Src Port: 80, Dst Port: 54042, Seq: 4345, Ack: 612, Len: 517
[4 Reassembled TCP Segments (4861 bytes): #131(1448), #132(1448), #133(1448), #134(517)]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
```

Figure 10: Hex value

8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

There are 12 bytes before the “O” (or “O” appears as the 13rd byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text. It is shown in Figure 11 below;

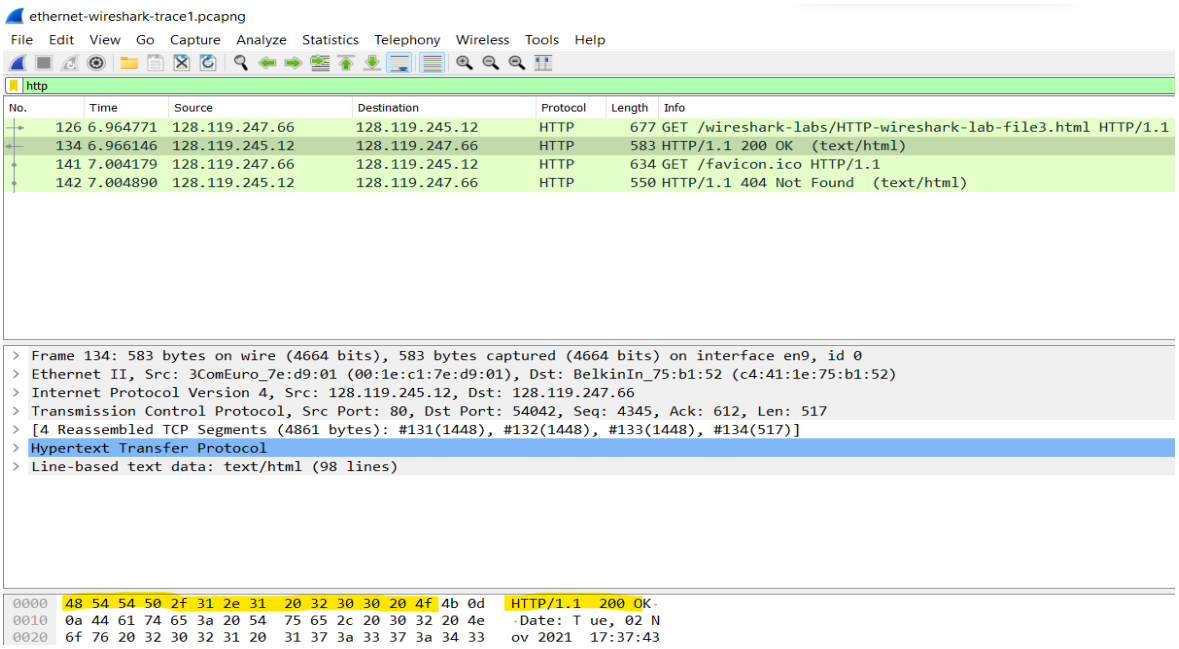

Figure 11: Bytes ACII “O”

9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP “OK 200 ...” reply message?

As shown in Figure 12 below, 4 frame carry date that is part of the complete HTTP “OK 200 …" reply message.

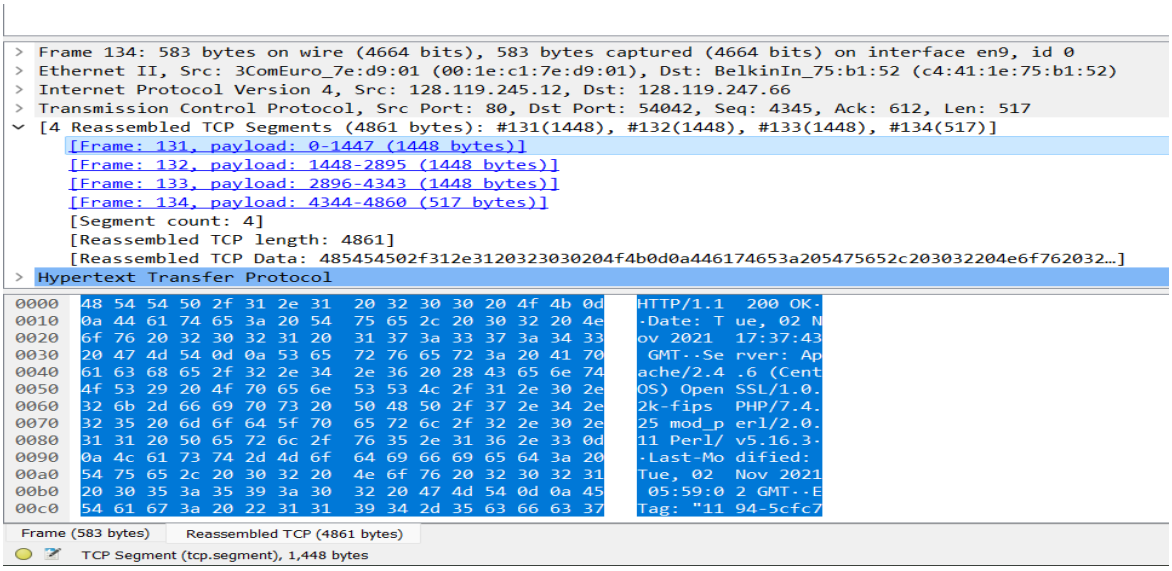

Figure 12: Frames