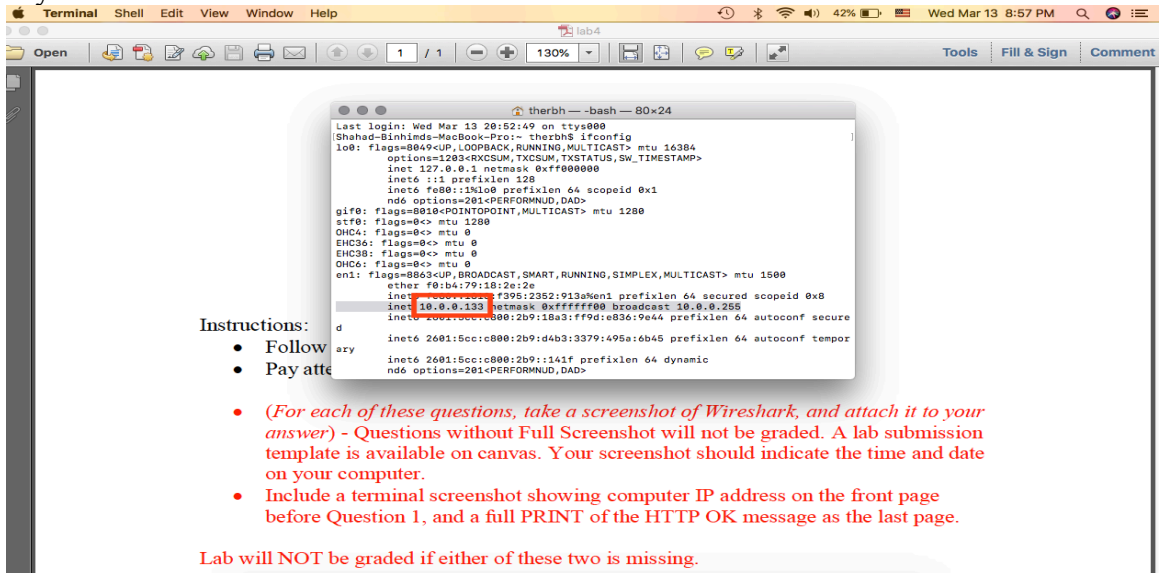


Shahad bin himd

Lab4

1. My IP Address is 10.0.0.133

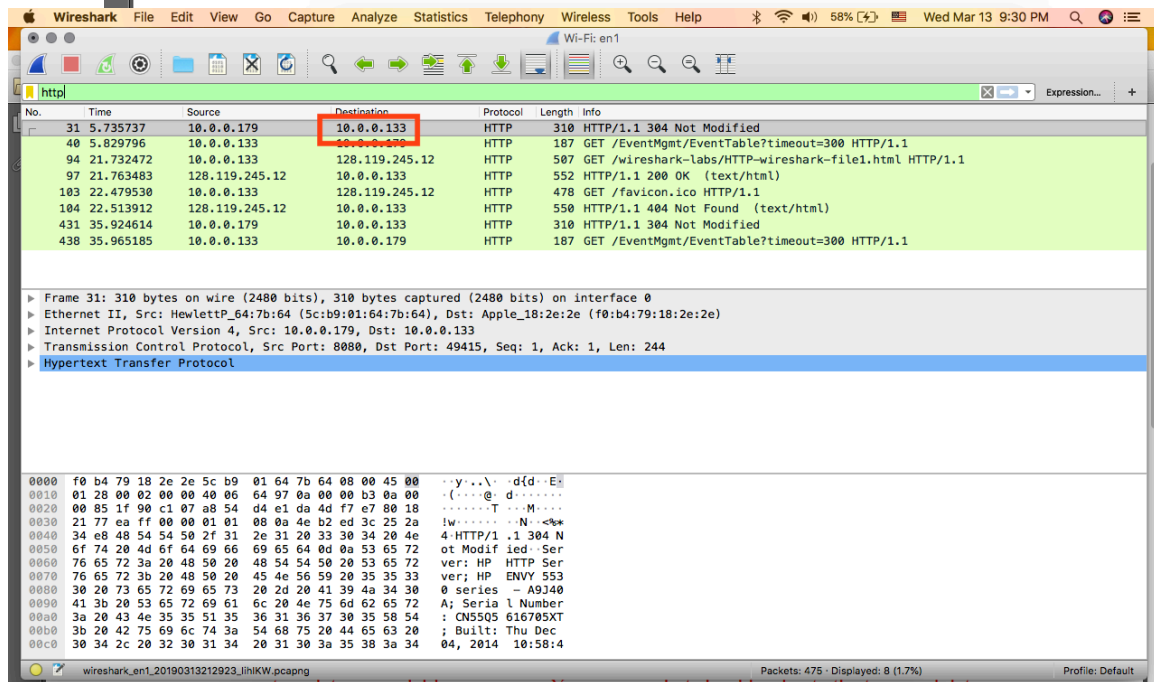


Instructions:

- Follow
- Pay attention

- (For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Lab will NOT be graded if either of these two is missing.



No.	Time	Source	Destination	Protocol	Length	Info
31	5.735737	10.0.0.179	10.0.0.133	HTTP	310	HTTP/1.1 304 Not Modified
40	5.829796	10.0.0.133	10.0.0.179	HTTP	187	GET /EventMgmt/EventTable?timeout=300 HTTP/1.1
94	21.732472	10.0.0.133	128.119.245.12	HTTP	507	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
97	21.763483	128.119.245.12	10.0.0.133	HTTP	552	HTTP/1.1 200 OK (text/html)
103	22.479530	10.0.0.133	128.119.245.12	HTTP	478	GET /favicon.ico HTTP/1.1
104	22.513912	128.119.245.12	10.0.0.133	HTTP	550	HTTP/1.1 404 Not Found (text/html)
431	35.924614	10.0.0.179	10.0.0.133	HTTP	310	HTTP/1.1 304 Not Modified
438	35.965185	10.0.0.133	10.0.0.179	HTTP	187	GET /EventMgmt/EventTable?timeout=300 HTTP/1.1

Frame 31: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0
Ethernet II, Src: HewlettP_64:7b:64 (5c:b9:01:64:7b:64), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:2e)
Internet Protocol Version 4, Src: 10.0.0.179, Dst: 10.0.0.133
Transmission Control Protocol, Src Port: 8080, Dst Port: 49415, Seq: 1, Ack: 1, Len: 244
Hypertext Transfer Protocol

0000 f0 b4 79 18 2e 2e 5c b9 01 64 7b 64 08 00 45 00 ...y...d{d-E
0010 01 28 00 02 00 00 40 06 64 97 0a 00 00 b3 0a 00 ...@. d.....
0020 00 85 1f 90 c1 07 a8 54 d4 e1 da 4d f7 e7 80 18T...M...
0030 21 77 ea ff 00 00 01 01 08 0a 4e b2 ed 3c 25 2a iw.....N...<*&
0040 34 e8 48 54 50 2f 31 2e 31 20 33 30 34 20 4e 4 HTTP/1.1 304 N
0050 6f 74 20 4d 6f 64 69 66 69 65 64 04 0a 53 65 72 ot Modified Ser
0060 76 65 72 3a 20 48 50 20 48 54 50 20 53 65 72 ver: HP HTTP Ser
0070 76 65 72 3b 20 48 50 20 45 4e 56 59 20 35 35 33 ver: HP ENVY 553
0080 30 20 73 65 72 69 65 73 20 2d 20 41 39 4a 34 30 0 series - A9J40
0090 41 3b 20 53 65 72 69 61 6c 20 4e 75 6d 62 65 72 A; Serial Number
00a0 3a 20 43 4e 35 51 35 36 31 36 37 30 35 58 54 : CN505 616785XT
00b0 3b 20 42 75 69 6c 74 3a 54 68 75 20 44 65 63 20 ; Built: Thu Dec
00c0 30 34 2c 20 32 30 31 34 20 31 30 3a 35 38 3a 34 04, 2014 10:58:4

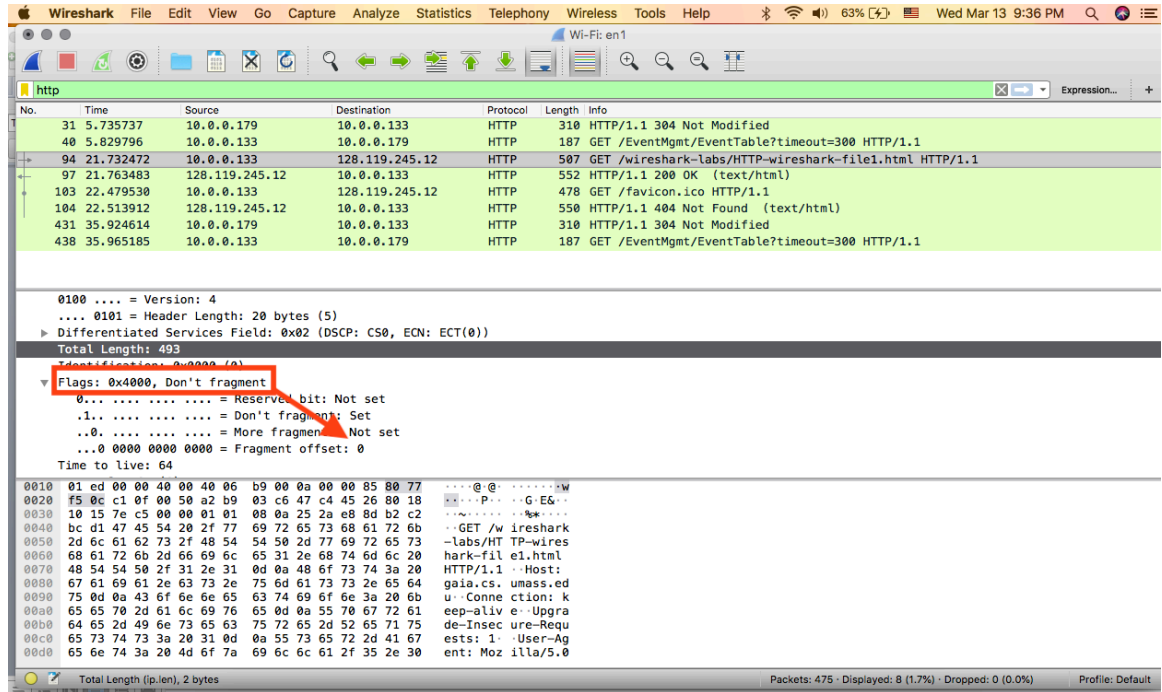
2. What is the total length of the datagram? 493

The screenshot shows the Wireshark interface with a packet capture on the 'Wi-Fi: en1' interface. The packet list shows several HTTP requests. The selected packet is packet 94, an HTTP GET request to 'http://128.119.245.12/wireshark-labs/HTTP-wireshark-file1.html'. The packet details pane shows the following information:

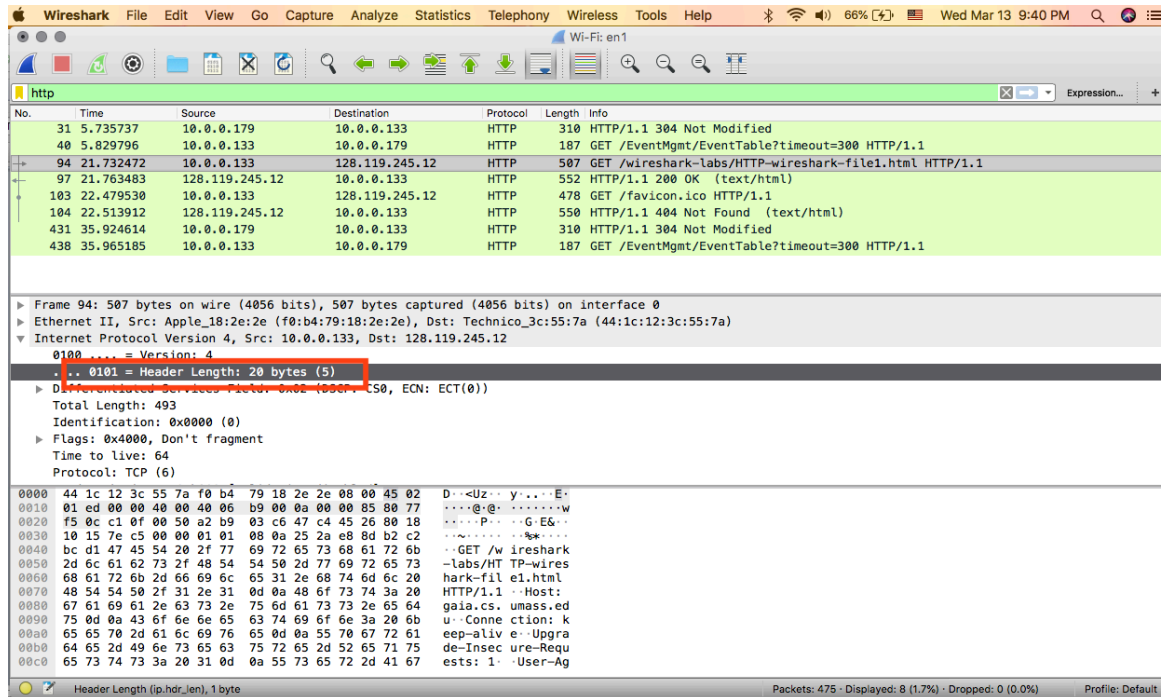
- Frame 94: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface 0
- Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)
- Internet Protocol Version 4, Src: 10.0.0.133, Dst: 128.119.245.12
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
- Total Length: 493**
- Identification: 0x0000 (0)
- Flags: 0x4000, Don't fragment
- Time to live: 64
- Protocol: TCP (6)

The packet bytes pane shows the raw data of the packet, including the IP header and the HTTP request line: 'GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1'.

3. Has this IP datagram been fragmented? **No it didn't**



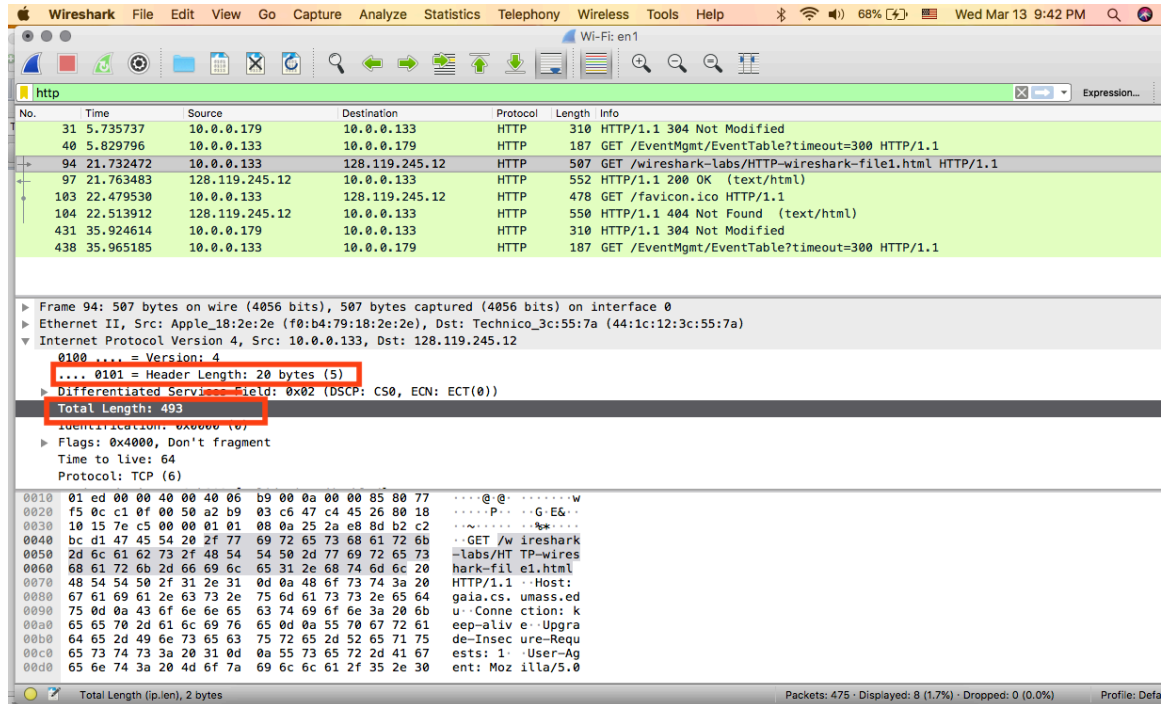
4. How many bytes are in the IP header? **20 bytes**



5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Total length – IP header = Payload

$$493 - 20 = 473$$



/var/folders/7n/7s6q636n28b9cyb16svls__w0000gn/T//wireshark_en1_20190313212923_IihIKW.pcapng 475 total packets, 8 shown

No.	Time	Source	Destination	Protocol	Length	Info
94	21.732472	10.0.0.133	128.119.245.12	HTTP	507	GET /

wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 94: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface 0
Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)
Internet Protocol Version 4, Src: 10.0.0.133, Dst: 128.119.245.12
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
 Total Length: 493
 Identification: 0x0000 (0)
 Flags: 0x4000, Don't fragment
 Time to live: 64
 Protocol: TCP (6)
 Header checksum: 0xb900 [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.0.0.133
 Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 49423, Dst Port: 80, Seq: 1, Ack: 1, Len: 441
Hypertext Transfer Protocol