Ariel Salazar

IT 520 – Lab4

March 17th, 2019

Instructions:

1. Follow the instructions in Lab 2 and expand the IP detail section.

   Lab 2 Instructions:

   1. Part 1: Start up your web browser.

   2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).

   3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.

   4. Enter the following to your browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

   5. Stop Wireshark packet capture.

2. Pay attention to the text in bold. I expect you to explain?

   • (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.

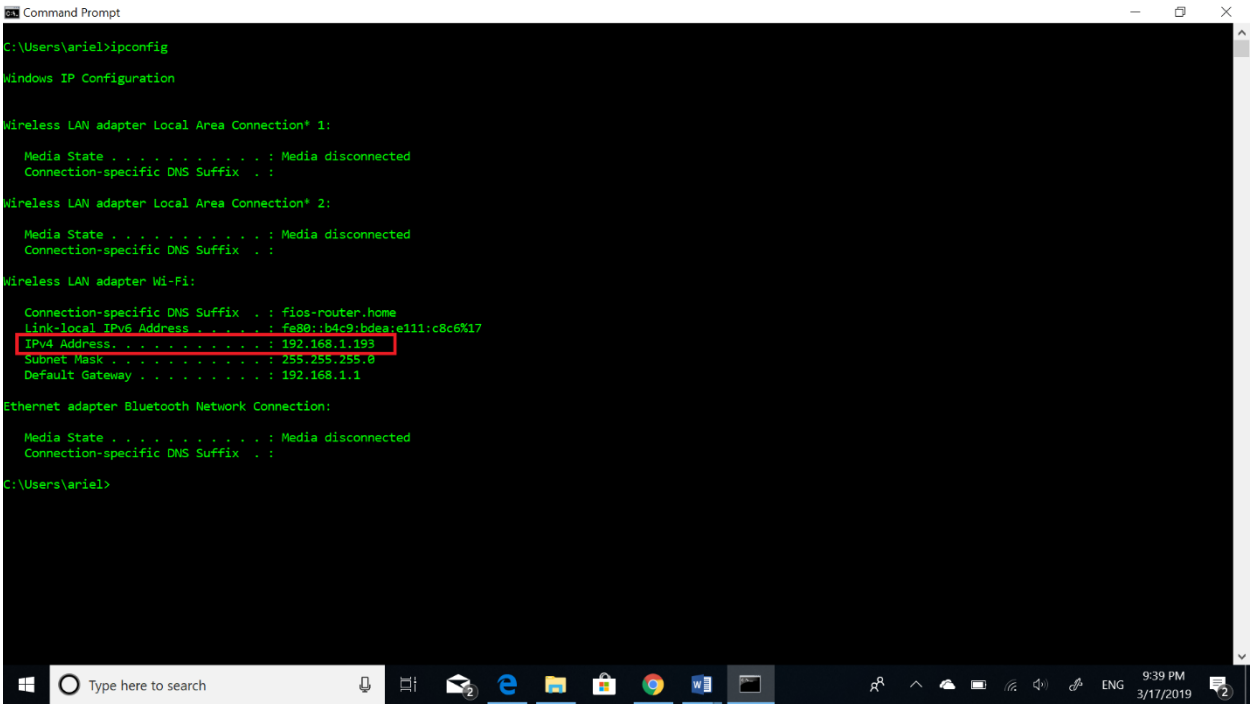
   • Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

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

Questions:

Terminal Screenshot with the IP address of my computer:

IP Address: 192.168.1.193

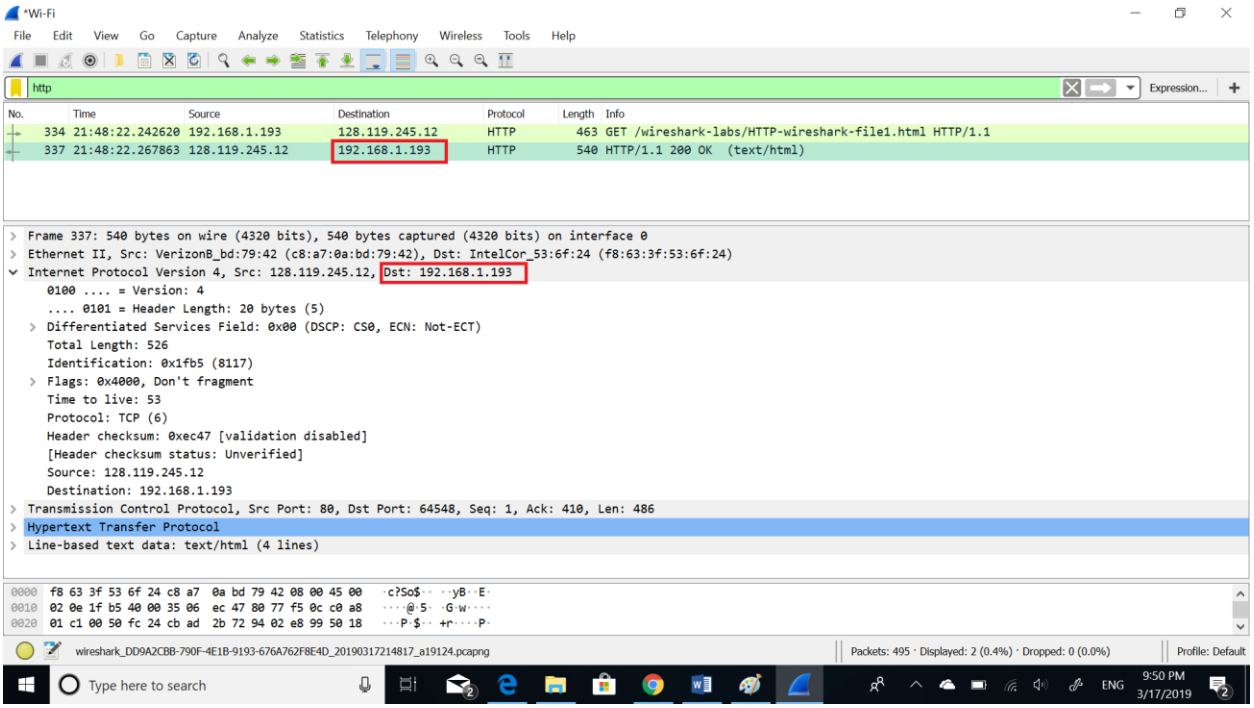


Questions:

1. What is the IP address of your computer? – Wireshark screenshot not, Terminal

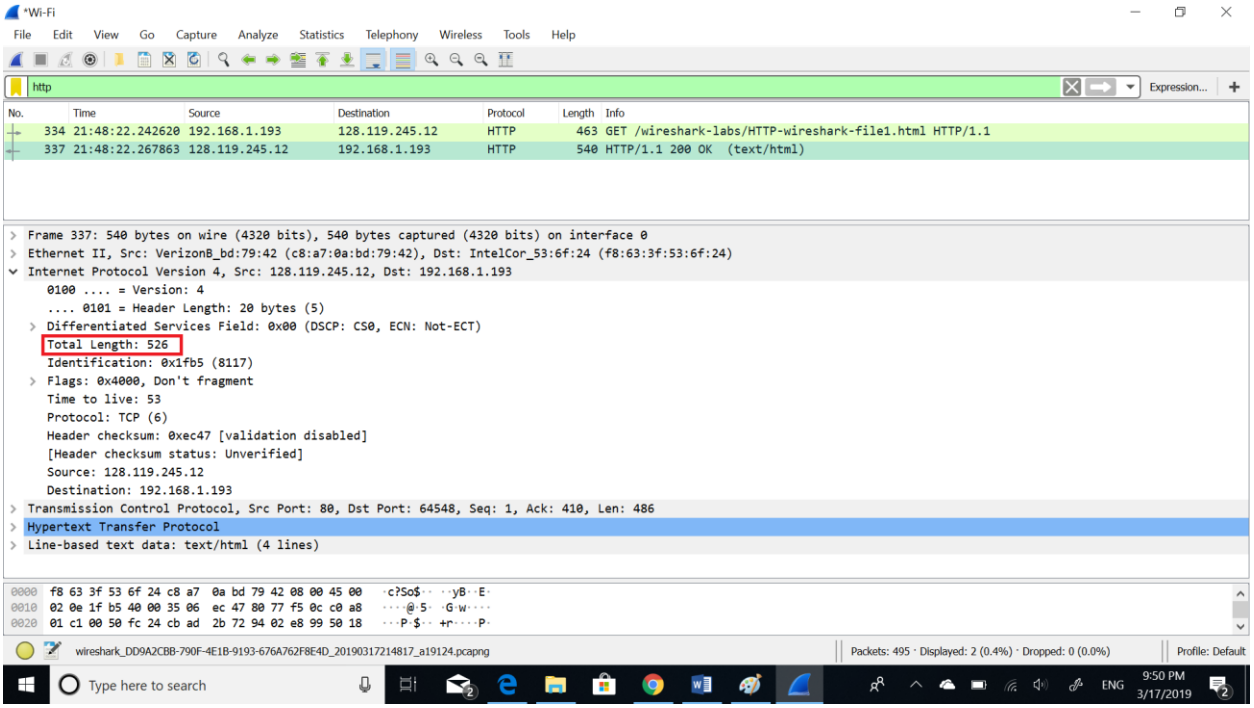
The IP address of my computer is: 192.168.1.193

The IP address that is showed as a source is the same that is in the terminal screenshot before question 1 (terminal screenshot)



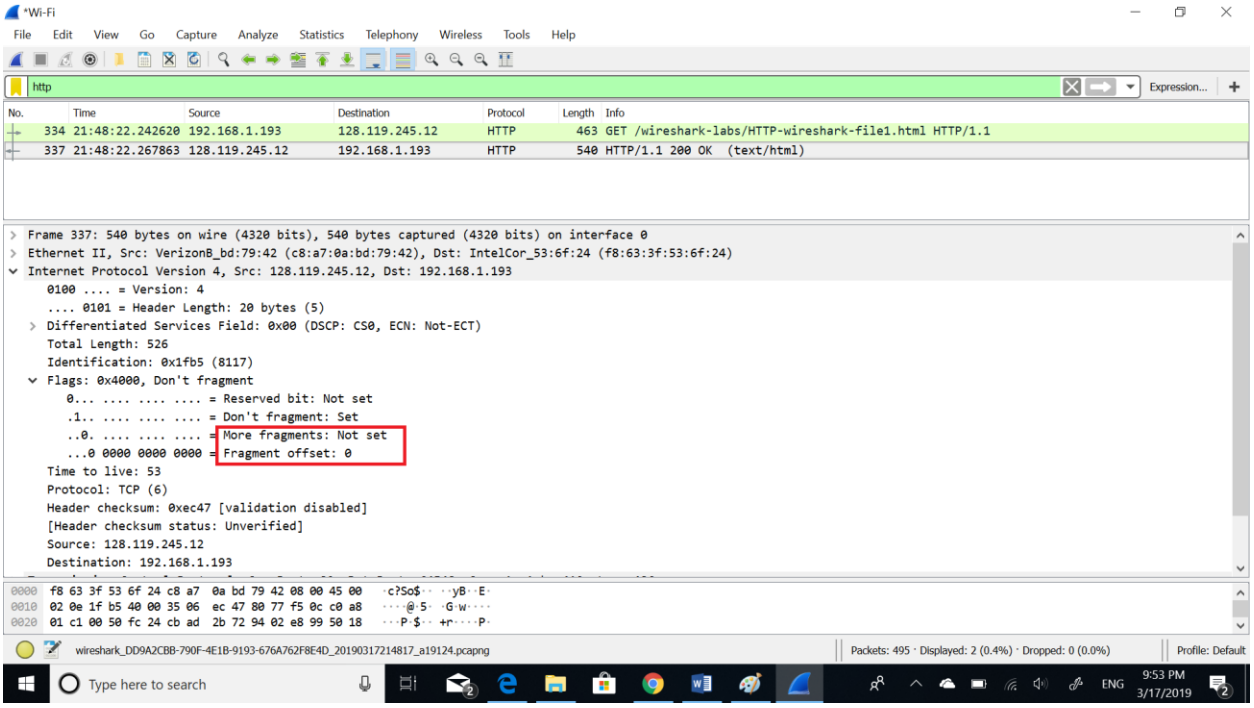
2. What is the total length of the datagram?

The total length of the datagram is 526 bytes



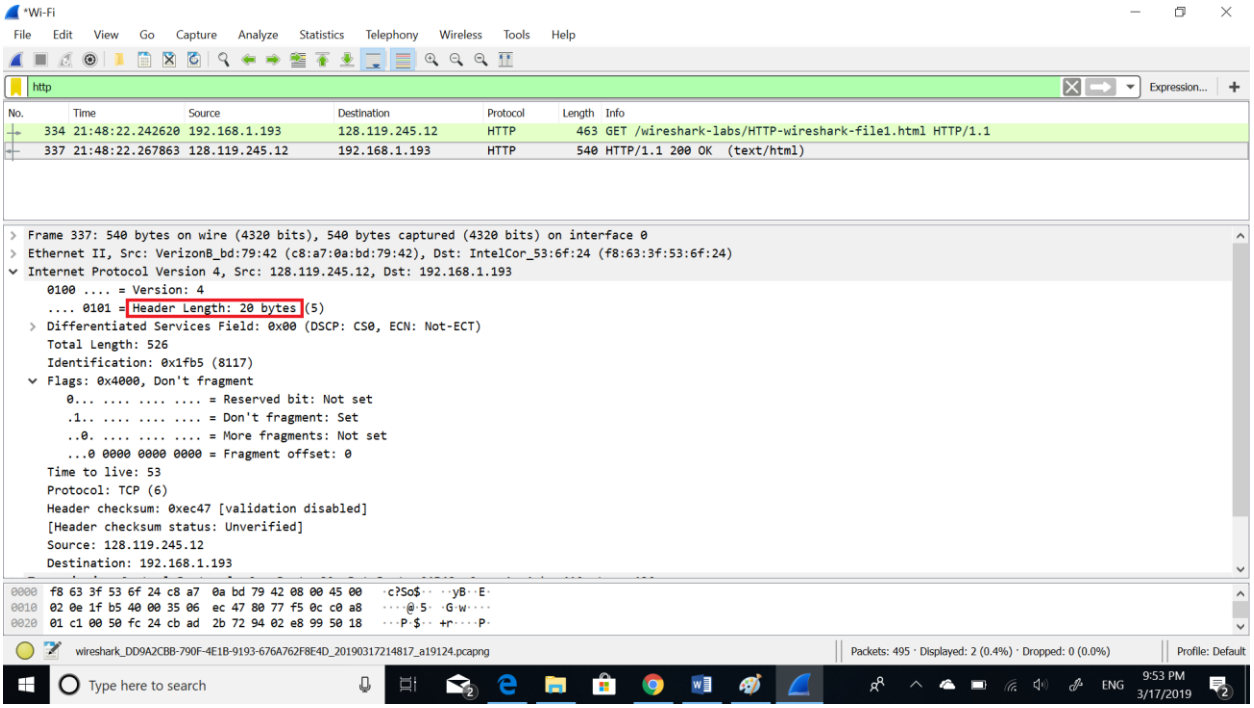
3. Has this IP datagram been fragmented?

The datagram has not been fragmented. The “more fragments” flag is not set and the “fragments offset” flag is set to “0”



4. How many bytes are in the IP header?

There are 20 bytes in the IP header.



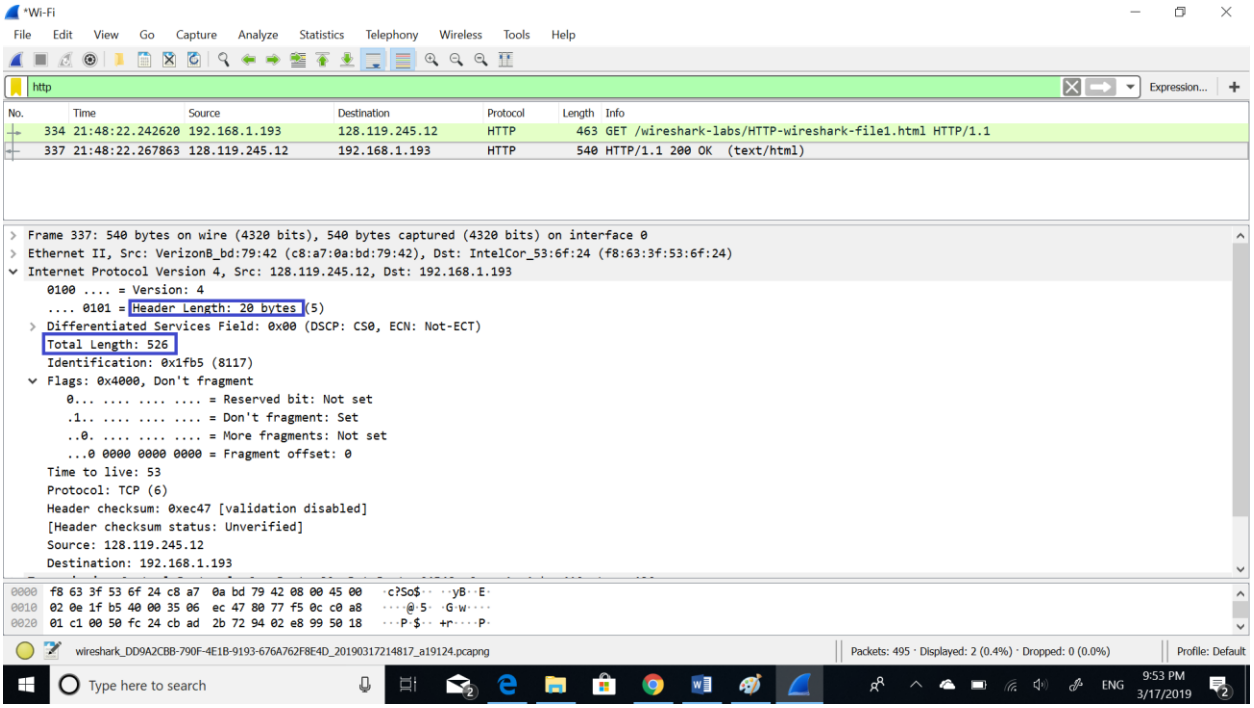
5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

The payload will be:

Number of bytes in the payload = Number of bytes of the datagram – number of bytes of the header

Number of bytes in the payload = 526 – 20

Number of bytes in the payload = 506 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Length Info
334 21:48:22.242620 192.168.1.193 128.119.245.12 HTTP 463 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
337 21:48:22.267863 128.119.245.12 192.168.1.193 HTTP 540 HTTP/1.1 200 OK (text/html)
Frame 337: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42), Dst: IntelCor_53:6f:24 (f8:63:3f:53:6f:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 526
Identification: 0x1fb5 (8117)
Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 53
Protocol: TCP (6)
Header checksum: 0xec47 [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
Destination: 192.168.1.193
0000 f8 63 3f 53 6f 24 c8 a7 0a bd 79 42 08 00 45 00
0010 02 0e 1f b5 40 00 35 06 ec 47 80 77 f5 0c c0 a8
0020 01 c1 00 50 fc 24 cb ad 2b 72 94 02 e8 99 50 18
wireshark_DD9A2CBB-790F-4E1B-9193-676A762F8E4D_20190317214817_a19124.pcapng
Packets: 495 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG
9:53 PM
3/17/2019