

Faisal Alwayli

## Wireshark Lab 4 - IP

### IT 520-A – Enterprise Infrastructure & Networks

#### Instructions:

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

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

The screenshot shows the Wireshark interface with a packet capture of an HTTP transaction. The packet list at the top shows a GET request from 10.8.20.118 to 128.119.245.12. The packet details pane shows the structure of the HTTP request, including the status line '200 OK (application/vnd.ms-cab-compressed)'. The packet bytes pane shows the raw data of the HTTP response, including the status line '200 OK (application/vnd.ms-cab-compressed)'.

Frame 805: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0  
Ethernet II, Src: Dell126180ef (24:8d:1f:16:30:ef), Dst: Cisco391ecbf (08:00:c8:59:ec:bf)  
Internet Protocol Version 4, Src: 10.8.20.118, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 60180, Dst Port: 80, Seq: 1, Ack: 1, Len: 397  
Hypertext Transfer Protocol

0000 00 2c c8 59 ec bf 14 b3 1f 16 30 ef 08 00 45 00 ...Y...-Bo-B  
0010 01 b5 3c 7d 40 00 00 00 28 c4 0a 08 14 76 00 77 ...C)@...(-v-w  
0020 f5 8c ea cc 00 50 85 84 c6 f0 c8 3e 0b 05 50 18 ....Pe...P  
0030 05 02 a4 07 00 40 47 65 54 20 2f 60 61 76 09 63 ....ET/favic  
0040 0f 6a 2e 69 63 ef 20 48 54 54 50 2f 31 2e 31 0d on.ico HTTP/1.1  
0050 0a 48 ef 73 74 3a 20 67 61 09 61 2e 63 73 2e 75 Host: g.mile.cs.u  
0060 6d 61 73 73 2e 65 64 75 0d 0a 43 ef 6a 6e 65 63 mass.edu -Connec  
0070 74 09 ef 6a 3a 20 65 65 65 70 2f 61 6c 69 76 65 tion: ke-ap-alive  
0080 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f -User-Agent: Mo  
0090 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/S.0 (Winde  
00a0 77 73 20 4e 54 20 31 30 2e 30 30 20 57 69 6e 36 ws/1.0.0) like  
00b0 34 30 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4;MSAppWeb  
00c0 40 69 74 2f 35 33 37 2e 33 36 20 20 40 48 54 4d kit/537.36 (KHTML  
00d0 4c 2c 20 6c 69 65 20 47 65 63 0b 4f 29 20 43 1,like Gecko) C  
00e0 68 72 6f 6d 65 2f 36 35 2e 30 2e 33 33 32 35 2e hrome/65.0.3325.  
00f0 31 30 31 20 53 61 66 61 72 69 2f 35 33 37 2e 33 181.Safe-r/537.3  
0100 36 0d 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 6-icorp;Image  
0110 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,image/apng  
0120 2c 69 6d 61 67 65 2f 2c 2c 2f 2f 2a 30 71 5d 30 image/\*;\*/\*;q=0.8  
0130 2e 30 0d 0a 0e 05 26 05 75 65 71 5d 30 36 36 36 .8

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

The length is 437

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows three packets, with the third packet (No. 1465) selected. The packet details pane shows the structure of the packet, with the 'Hypertext Transfer Protocol' section expanded. The 'Total Length: 437' field is highlighted with a red circle. The packet bytes pane shows the raw data of the packet, with the first 100 bytes displayed.

Packet 1465: 1465.947950 72.21.81.240 10.8.20.118 HTTP 1295 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

Frame 805: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0

Ethernet II, Src: Dell\_16:30:0f (14:bb:1f:16:30:0f), Dst: Cisco\_99:ec:b7 (00:2c:c0:99:ec:b7)

Internet Protocol Version 4, Src: 10.8.20.118, Dst: 128.119.245.12

0100 ..... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 437

Identification: 0x3c7d (15485)

Flags: 0x0000, Don't fragment

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x02c4 [validation disabled]

[Header checksum status: Unverified]

Source: 10.8.20.118

Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 60100, Dst Port: 80, Seq: 1, Ack: 1, Len: 397

Hypertext Transfer Protocol

0000 00 2c c8 50 ec bf 14 b3 1f 16 30 0f 00 00 45 00 . . Y . . . . . 00 : E-

0010 01 05 3c 7d 40 00 00 00 28 c4 0a 00 14 70 00 77 . < j b . . . . . v w

0020 f5 0c ea cc 00 50 05 04 c0 f0 c0 be d0 50 18 . . . . . P

0030 81 62 ea 07 00 00 47 45 54 20 2f 60 61 76 69 63 . . . . . DE T / favic

0040 6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d on .ico H TTP/1.1

0050 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 Host: g .ia .tt .u

0060 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 mass .edu Connec

0070 74 69 6f 6e 3a 20 69 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive

0080 0d 0a 53 73 05 72 2d 41 67 65 6e 7a 3a 20 4d 6f . User-A gent: No

0090 7a 69 6c 6e 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo

00a0 77 73 2d 4a 54 20 31 30 2e 30 20 28 57 69 6e 36 vs NT 5.0; Win6

00b0 34 30 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4; x64) Applieab

00c0 4b 69 74 2f 35 33 37 2e 33 36 20 20 48 54 4d Kit/537. 36 (KHTML

00d0 4c 2c 20 6c 69 60 65 28 47 65 63 60 6f 29 20 43 ., like Gecko) C

00e0 68 72 6f 6d 65 2f 36 35 2e 30 2e 33 33 32 35 2e hrome/65 .0.3525.

00f0 31 30 31 20 53 61 66 61 72 69 2f 35 33 37 2d 33 181 Safa ri/537.3

0100 36 0d 0a 43 63 65 70 7a 3a 20 69 6d 61 67 65 6 . Accp ti .image

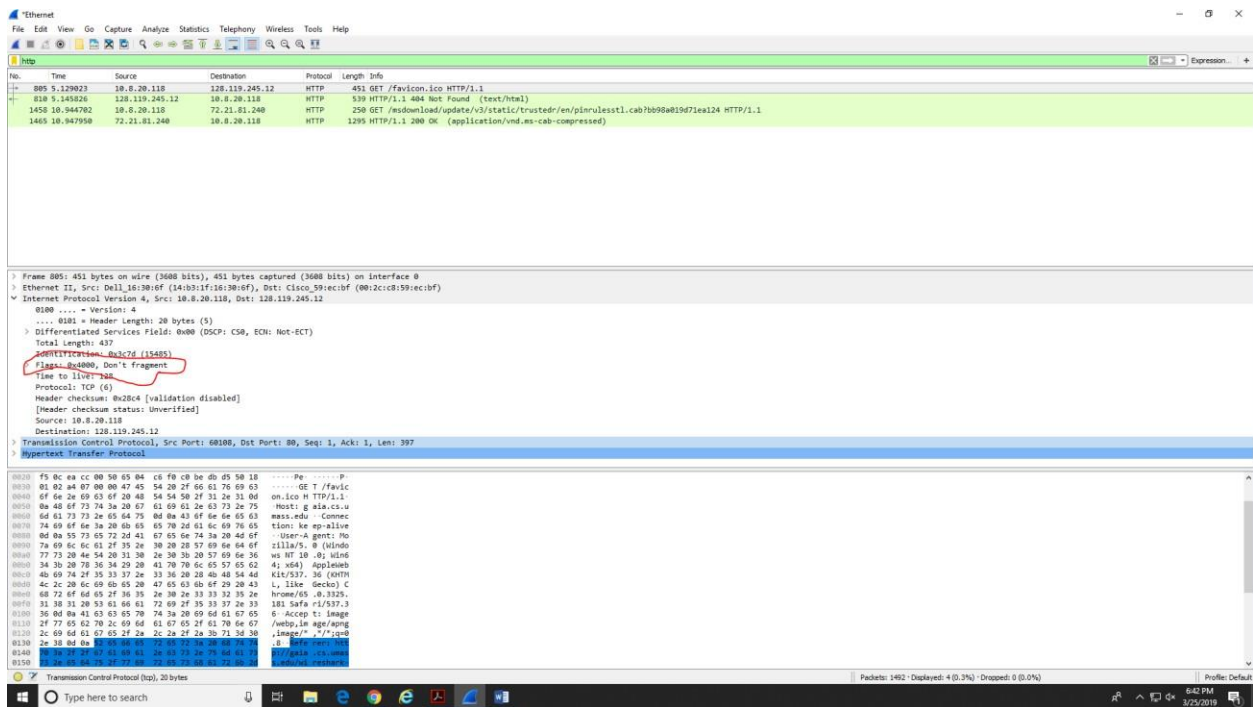
0110 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,im age/spng

0120 2c 69 6d 61 67 65 2f 2a 2e 2a 2f 2a 30 71 5d 30 .image?/.7z/jpeg

0130 2e 38 0d 0a 05 0a 05 52 05 14 16 30 4c 0a 05 .b . . . . .

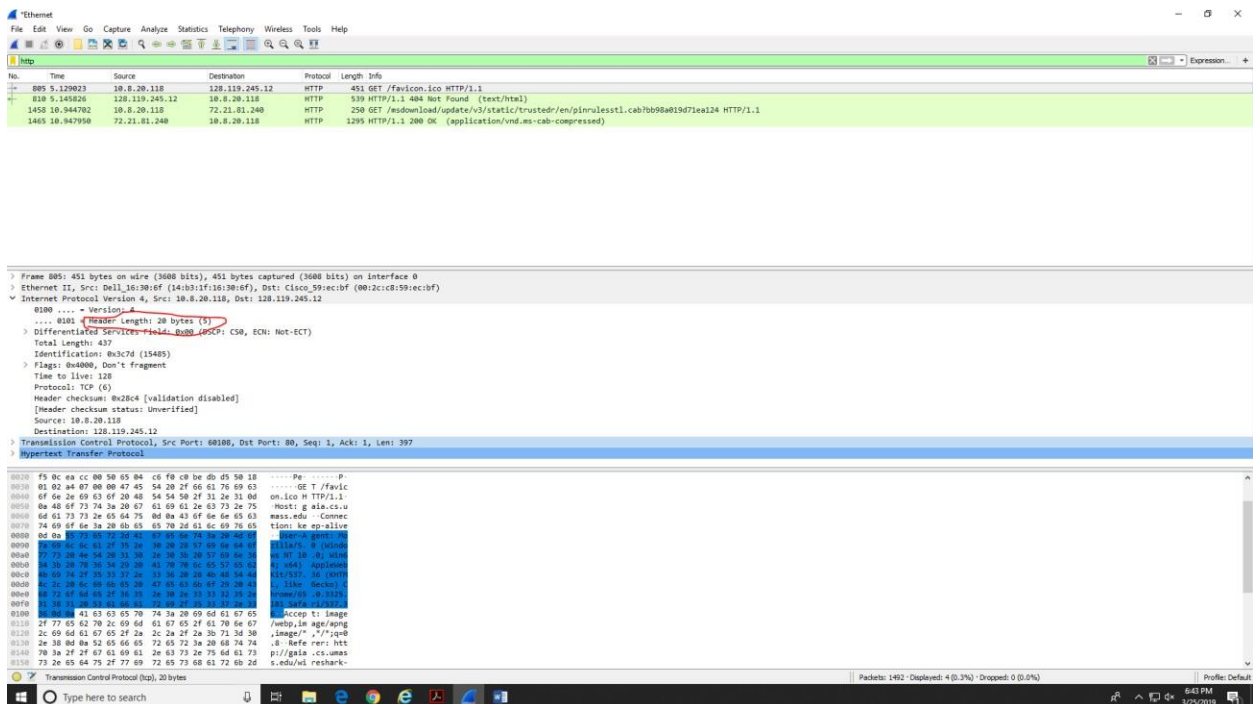
## 3. Has this IP datagram been fragmented?

No



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.

There are 417 bytes in the payload

The header is 20 bytes and the total is 437 bytes that gives is 417 bytes in the payload

