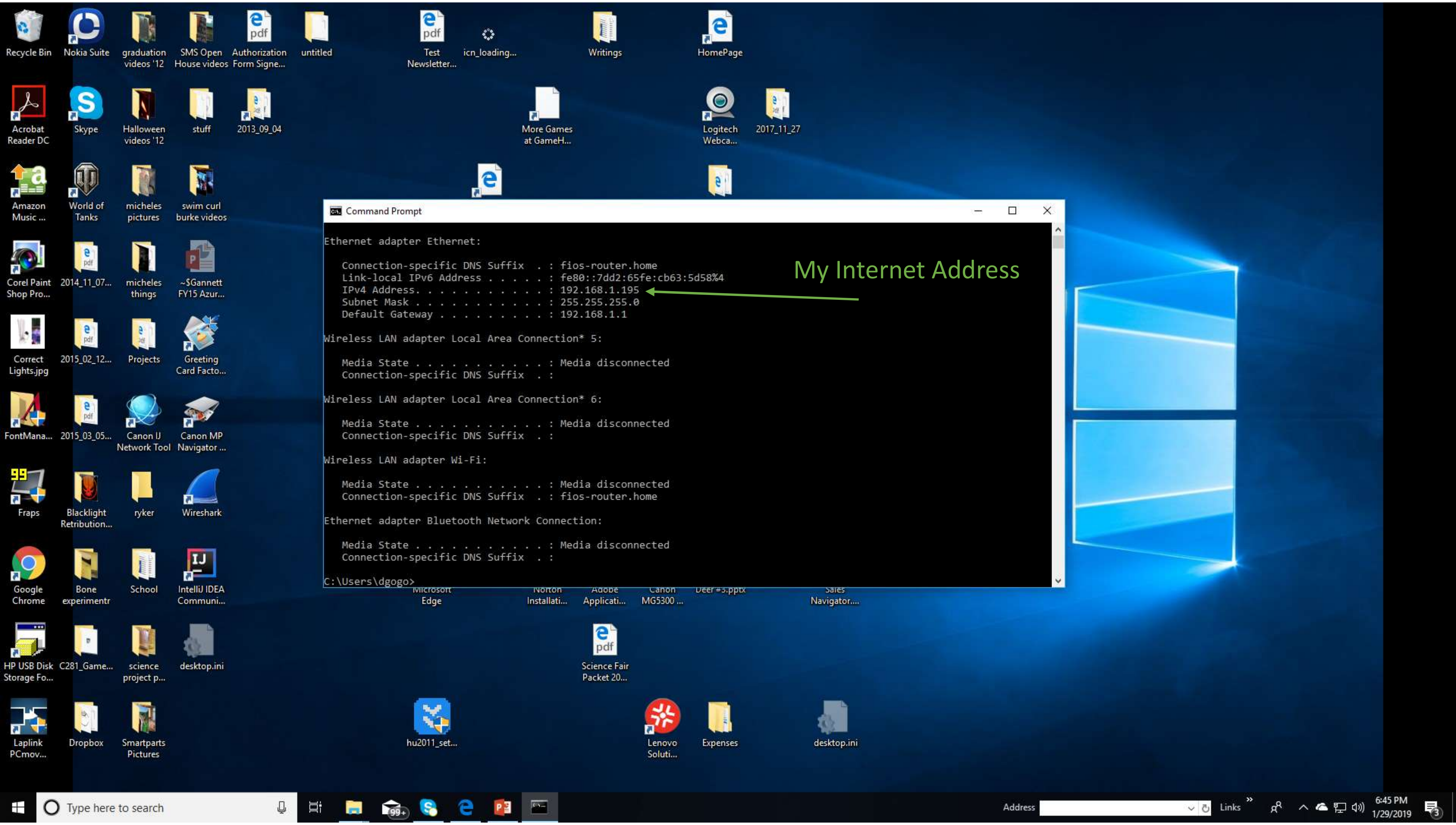
Wireshark Lab 1 - Intro

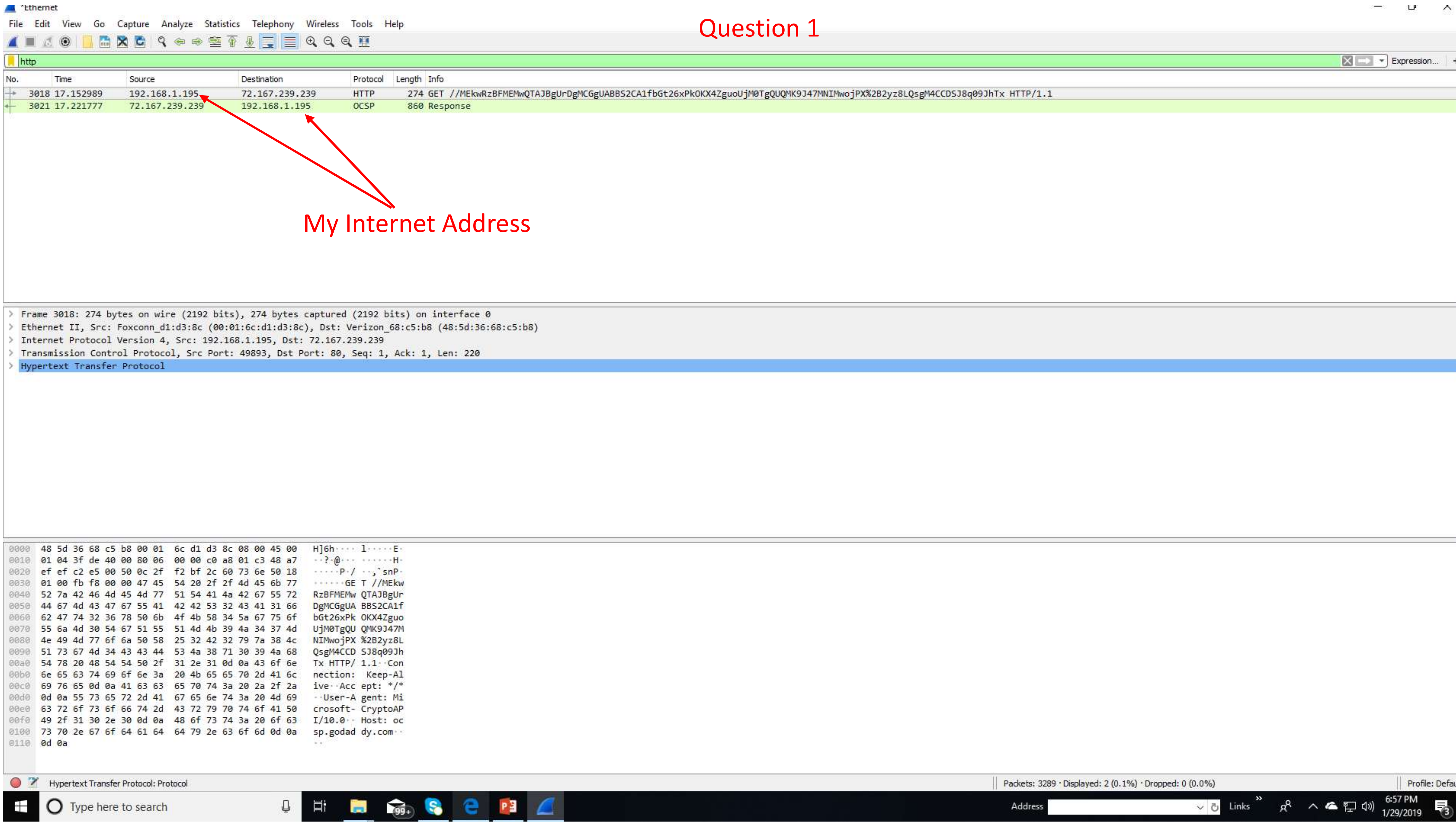
IT 520 –A – Enterprise Infrastructure & Networks

David Gogolkiewicz



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fios-router.home
   Link-local IPv6 Address . . . . . : fe80::7dd2:65fe:cb63:5d58%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.195
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Wireless LAN adapter Local Area Connection* 5:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : fios-router.home

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\dgogo>
```

My Internet Address


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Type here to search
Address
Links
6:57 PM
1/29/2019

Question 1

http

```
No.   Time       Source         Destination    Protocol Length Info
3018 17.152989  192.168.1.195  72.167.239.239  HTTP      274 GET //MEkwRzBFMEMwQTAJBgUrDgMCGgUABBS2CA1fbGt26xPkOKX4ZguoUjM0TgQUQMK9J47MNIMwojPX%2B2yz8LQsgM4CCDSJ8q09JhTx HTTP/1.1
3021 17.221777  72.167.239.239 192.168.1.195   OCSP      860 Response
```

My Internet Address

```
> Frame 3018: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface 0
> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
> Internet Protocol Version 4, Src: 192.168.1.195, Dst: 72.167.239.239
> Transmission Control Protocol, Src Port: 49893, Dst Port: 80, Seq: 1, Ack: 1, Len: 220
> Hypertext Transfer Protocol
```

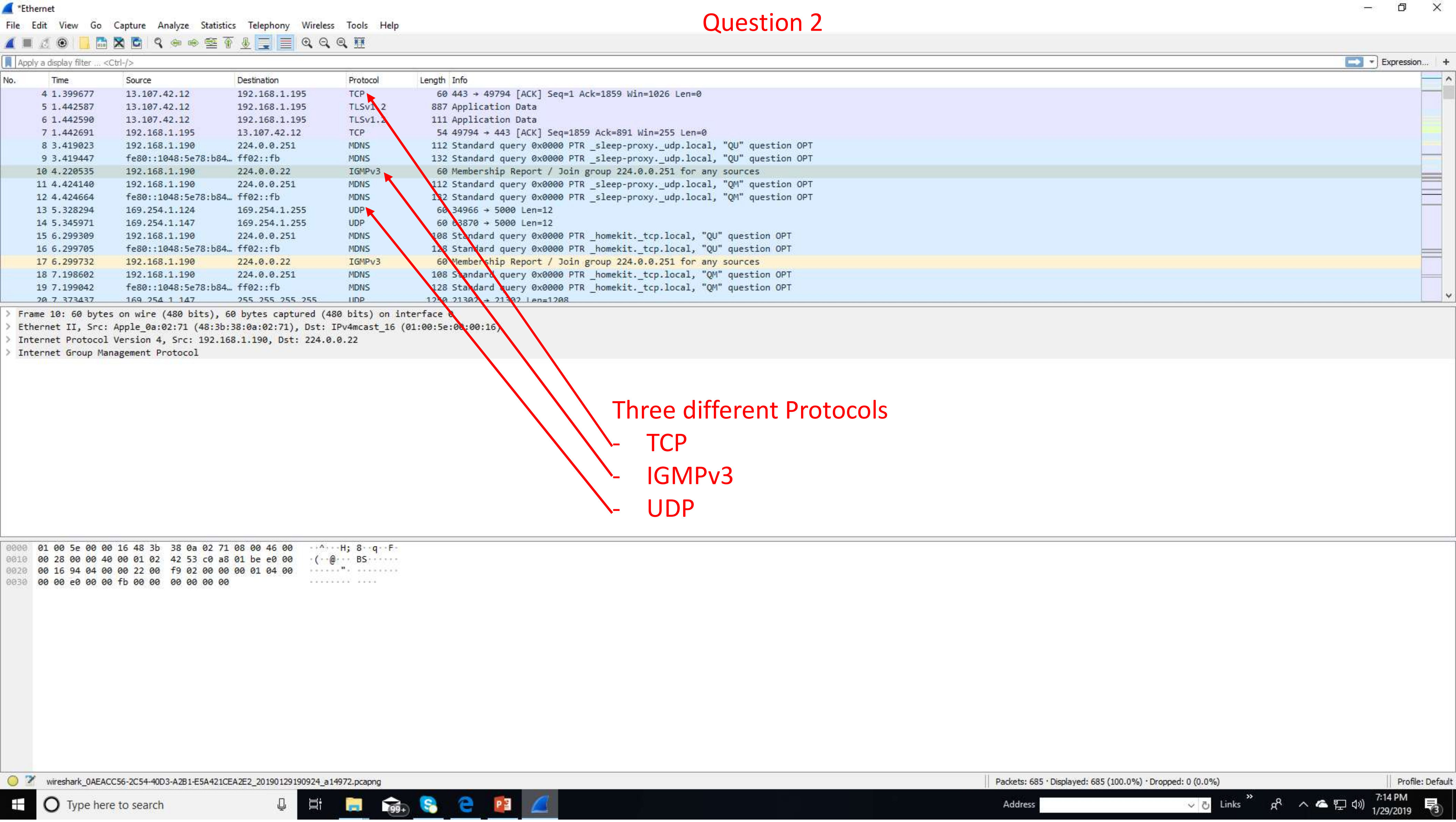
```
0000  48 5d 36 68 c5 b8 00 01  6c d1 d3 8c 08 00 45 00   H]6h···· l·····E·
0010  01 04 3f de 40 00 80 06  00 00 c0 a8 01 c3 48 a7   ··?·@··· ······H·
0020  ef ef c2 e5 00 50 0c 2f  f2 bf 2c 60 73 6e 50 18   ·····P·/ ··,`snP·
0030  01 00 fb f8 00 00 47 45  54 20 2f 2f 4d 45 6b 77   ······GE T //MEkw
0040  52 7a 42 46 4d 45 4d 77  51 54 41 4a 42 67 55 72   RzBFMEMw QTAJBgUr
0050  44 67 4d 43 47 67 55 41  42 42 53 32 43 41 31 66   DgMCGgUA BBS2CA1f
0060  62 47 74 32 36 78 50 6b  4f 4b 58 34 5a 67 75 6f   bGt26xPk OKX4Zguo
0070  55 6a 4d 30 54 67 51 55  51 4d 4b 39 4a 34 37 4d   UjM0TgQU QMK9J47M
0080  4e 49 4d 77 6f 6a 50 58  25 32 42 32 79 7a 38 4c   NIMwojPX %2B2yz8L
0090  51 73 67 4d 34 43 43 44  53 4a 38 71 30 39 4a 68   QsgM4CCD SJ8q09Jh
00a0  54 78 20 48 54 54 50 2f  31 2e 31 0d 0a 43 6f 6e   Tx HTTP/ 1.1··Con
00b0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
00c0  69 76 65 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   ive··Acc ept: */*
00d0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 69   ··User-A gent: Mi
00e0  63 72 6f 73 6f 66 74 2d  43 72 79 70 74 6f 41 50   crosoft- CryptoAP
00f0  49 2f 31 30 2e 30 0d 0a  48 6f 73 74 3a 20 6f 63   I/10.0·· Host: oc
0100  73 70 2e 67 6f 64 61 64  64 79 2e 63 6f 6d 0d 0a   sp.godad dy.com··
0110  0d 0a                                               ··
```

Hypertext Transfer Protocol: Protocol

Packets: 3289 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)

Profile: Defau

Question 2


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
wireshark_0AEACC56-2C54-40D3-A2B1-E5A421CEA2E2_20190129190924_a14972.pcapng
Packets: 685 · Displayed: 685 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Address
Links
7:14 PM
1/29/2019

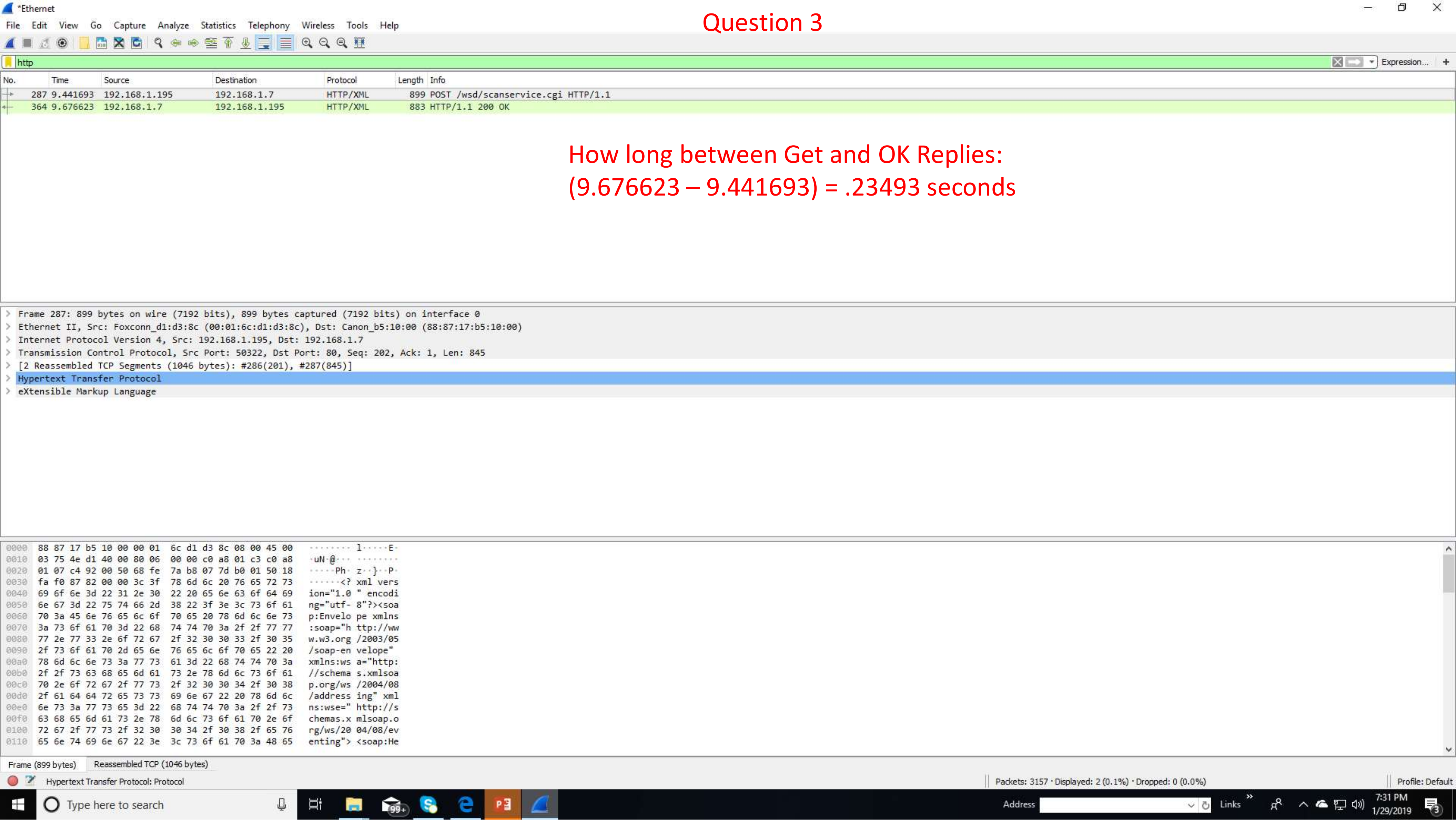
```
No.     Time        Source               Destination      Protocol  Length Info
      4 1.399677    13.107.42.12         192.168.1.195    TCP           60 443 → 49794 [ACK] Seq=1 Ack=1859 Win=1026 Len=0
      5 1.442587    13.107.42.12         192.168.1.195    TLSv1.2      887 Application Data
      6 1.442590    13.107.42.12         192.168.1.195    TLSv1.2      111 Application Data
      7 1.442691    192.168.1.195        13.107.42.12     TCP           54 49794 → 443 [ACK] Seq=1859 Ack=891 Win=255 Len=0
      8 3.419023    192.168.1.190        224.0.0.251      MDNS         112 Standard query 0x0000 PTR _sleep-proxy._udp.local, "QU" question OPT
      9 3.419447    fe80::1048:5e78:b84… ff02::fb         MDNS         132 Standard query 0x0000 PTR _sleep-proxy._udp.local, "QU" question OPT
     10 4.220535    192.168.1.190        224.0.0.22       IGMPv3        60 Membership Report / Join group 224.0.0.251 for any sources
     11 4.424140    192.168.1.190        224.0.0.251      MDNS         112 Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
     12 4.424664    fe80::1048:5e78:b84… ff02::fb         MDNS         132 Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
     13 5.328294    169.254.1.124        169.254.1.255    UDP           60 34966 → 5000 Len=12
     14 5.345971    169.254.1.147        169.254.1.255    UDP           60 63870 → 5000 Len=12
     15 6.299309    192.168.1.190        224.0.0.251      MDNS         108 Standard query 0x0000 PTR _homekit._tcp.local, "QU" question OPT
     16 6.299705    fe80::1048:5e78:b84… ff02::fb         MDNS         128 Standard query 0x0000 PTR _homekit._tcp.local, "QU" question OPT
     17 6.299732    192.168.1.190        224.0.0.22       IGMPv3        60 Membership Report / Join group 224.0.0.251 for any sources
     18 7.198602    192.168.1.190        224.0.0.251      MDNS         108 Standard query 0x0000 PTR _homekit._tcp.local, "QM" question OPT
     19 7.199042    fe80::1048:5e78:b84… ff02::fb         MDNS         128 Standard query 0x0000 PTR _homekit._tcp.local, "QM" question OPT
     20 7.373437    169.254.1.147        255.255.255.255  UDP         1250 21302 → 21302 Len=1208
```

```
> Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Apple_0a:02:71 (48:3b:38:0a:02:71), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.1.190, Dst: 224.0.0.22
> Internet Group Management Protocol
```

```
0000  01 00 5e 00 00 16 48 3b  38 0a 02 71 08 00 46 00   ··^···H; 8··q··F·
0010  00 28 00 00 40 00 01 02  42 53 c0 a8 01 be e0 00   ·(··@··· BS······
0020  00 16 94 04 00 00 22 00  f9 02 00 00 00 01 04 00   ······"· ········
0030  00 00 e0 00 00 fb 00 00  00 00 00 00               ········ ····
```

Three different Protocols

- TCP
- IGMPv3
- UDP


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Type here to search
Address
Links
7:31 PM
1/29/2019

Question 3

http

```
No.     Time      Source          Destination     Protocol  Length Info
    287 9.441693  192.168.1.195   192.168.1.7     HTTP/XML     899 POST /wsd/scanservice.cgi HTTP/1.1
    364 9.676623  192.168.1.7     192.168.1.195   HTTP/XML     883 HTTP/1.1 200 OK
```

How long between Get and OK Replies:

(9.676623 – 9.441693) = .23493 seconds

```
> Frame 287: 899 bytes on wire (7192 bits), 899 bytes captured (7192 bits) on interface 0
> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Canon_b5:10:00 (88:87:17:b5:10:00)
> Internet Protocol Version 4, Src: 192.168.1.195, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 50322, Dst Port: 80, Seq: 202, Ack: 1, Len: 845
> [2 Reassembled TCP Segments (1046 bytes): #286(201), #287(845)]
> Hypertext Transfer Protocol
> eXtensible Markup Language
```

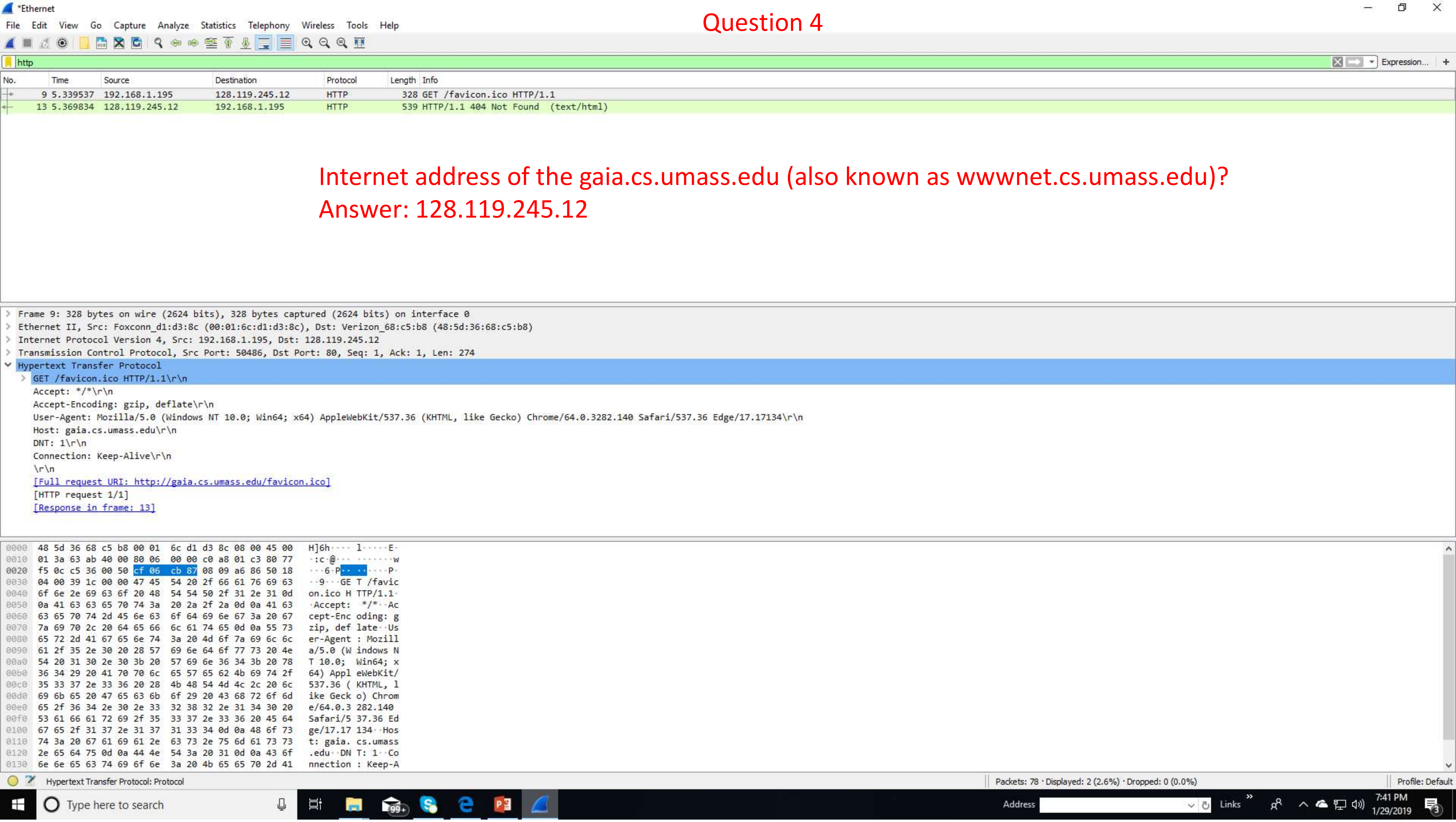
```
0000  88 87 17 b5 10 00 00 01  6c d1 d3 8c 08 00 45 00   ········ l·····E·
0010  03 75 4e d1 40 00 80 06  00 00 c0 a8 01 c3 c0 a8   ·uN·@··· ········
0020  01 07 c4 92 00 50 68 fe  7a b8 07 7d b0 01 50 18   ·····Ph· z··}··P·
0030  fa f0 87 82 00 00 3c 3f  78 6d 6c 20 76 65 72 73   ······<? xml vers
0040  69 6f 6e 3d 22 31 2e 30  22 20 65 6e 63 6f 64 69   ion="1.0 " encodi
0050  6e 67 3d 22 75 74 66 2d  38 22 3f 3e 3c 73 6f 61   ng="utf- 8"?><soa
0060  70 3a 45 6e 76 65 6c 6f  70 65 20 78 6d 6c 6e 73   p:Envelo pe xmlns
0070  3a 73 6f 61 70 3d 22 68  74 74 70 3a 2f 2f 77 77   :soap="h ttp://ww
0080  77 2e 77 33 2e 6f 72 67  2f 32 30 30 33 2f 30 35   w.w3.org /2003/05
0090  2f 73 6f 61 70 2d 65 6e  76 65 6c 6f 70 65 22 20   /soap-en velope" 
00a0  78 6d 6c 6e 73 3a 77 73  61 3d 22 68 74 74 70 3a   xmlns:ws a="http:
00b0  2f 2f 73 63 68 65 6d 61  73 2e 78 6d 6c 73 6f 61   //schema s.xmlsoa
00c0  70 2e 6f 72 67 2f 77 73  2f 32 30 30 34 2f 30 38   p.org/ws /2004/08
00d0  2f 61 64 64 72 65 73 73  69 6e 67 22 20 78 6d 6c   /address ing" xml
00e0  6e 73 3a 77 73 65 3d 22  68 74 74 70 3a 2f 2f 73   ns:wse=" http://s
00f0  63 68 65 6d 61 73 2e 78  6d 6c 73 6f 61 70 2e 6f   chemas.x mlsoap.o
0100  72 67 2f 77 73 2f 32 30  30 34 2f 30 38 2f 65 76   rg/ws/20 04/08/ev
0110  65 6e 74 69 6e 67 22 3e  3c 73 6f 61 70 3a 48 65   enting"> <soap:He
```

Frame (899 bytes)   Reassembled TCP (1046 bytes)

Hypertext Transfer Protocol: Protocol

Packets: 3157 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)

Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Type here to search
Address
Links
7:41 PM
1/29/2019

Question 4

Filter: http

```
No.   Time      Source          Destination     Protocol Length Info
    9 5.339537  192.168.1.195   128.119.245.12  HTTP     328 GET /favicon.ico HTTP/1.1
   13 5.369834  128.119.245.12  192.168.1.195   HTTP     539 HTTP/1.1 404 Not Found  (text/html)
```

Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?

Answer: 128.119.245.12

```
> Frame 9: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface 0
> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
> Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50486, Dst Port: 80, Seq: 1, Ack: 1, Len: 274
v Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Host: gaia.cs.umass.edu\r\n
    DNT: 1\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
    [HTTP request 1/1]
    [Response in frame: 13]
```

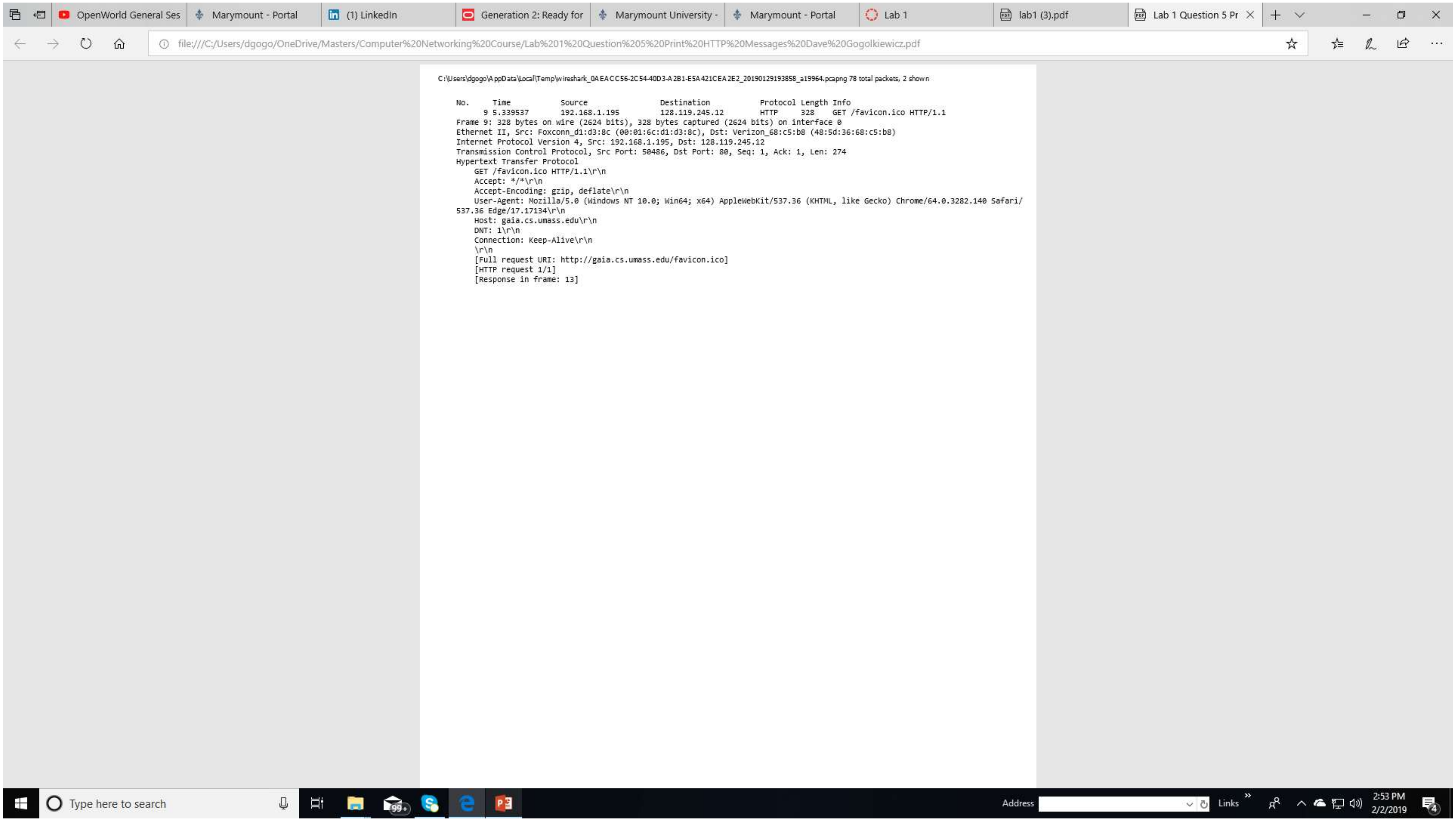
```
0000  48 5d 36 68 c5 b8 00 01  6c d1 d3 8c 08 00 45 00   H]6h···· l·····E·
0010  01 3a 63 ab 40 00 80 06  00 00 c0 a8 01 c3 80 77   ·:c·@··· ·······w
0020  f5 0c c5 36 00 50 cf 06  cb 87 08 09 a6 86 50 18   ···6·P·· ······P·
0030  04 00 39 1c 00 00 47 45  54 20 2f 66 61 76 69 63   ··9···GE T /favic
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 41 63 63 65 70 74 3a  20 2a 2f 2a 0d 0a 41 63   ·Accept:  */*··Ac
0060  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0070  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 55 73   zip, def late··Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00a0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00b0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
00c0  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
00d0  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
00e0  65 2f 36 34 2e 30 2e 33  32 38 32 2e 31 34 30 20   e/64.0.3 282.140
00f0  53 61 66 61 72 69 2f 35  33 37 2e 33 36 20 45 64   Safari/5 37.36 Ed
0100  67 65 2f 31 37 2e 31 37  31 33 34 0d 0a 48 6f 73   ge/17.17 134··Hos
0110  74 3a 20 67 61 69 61 2e  63 73 2e 75 6d 61 73 73   t: gaia. cs.umass
0120  2e 65 64 75 0d 0a 44 4e  54 3a 20 31 0d 0a 43 6f   .edu··DN T: 1··Co
0130  6e 6e 65 63 74 69 6f 6e  3a 20 4b 65 65 70 2d 41   nnection : Keep-A
```

Hypertext Transfer Protocol: Protocol

Packets: 78 · Displayed: 2 (2.6%) · Dropped: 0 (0.0%)

Profile: Default

Question 5



C:\Users\dgogo\AppData\Local\Temp\wireshark_0AEACC56-2C54-40D3-A2B1-E5A421CEA2E2_20190129193858_a19964.pcapng 78 total packets, 2 shown

```
No.     Time           Source                Destination           Protocol Length Info
      9 5.339537       192.168.1.195         128.119.245.12        HTTP     328    GET /favicon.ico HTTP/1.1
Frame 9: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface 0
Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50486, Dst Port: 80, Seq: 1, Ack: 1, Len: 274
Hypertext Transfer Protocol
    GET /favicon.ico HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/
537.36 Edge/17.17134\r\n
    Host: gaia.cs.umass.edu\r\n
    DNT: 1\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
    [HTTP request 1/1]
    [Response in frame: 13]
```