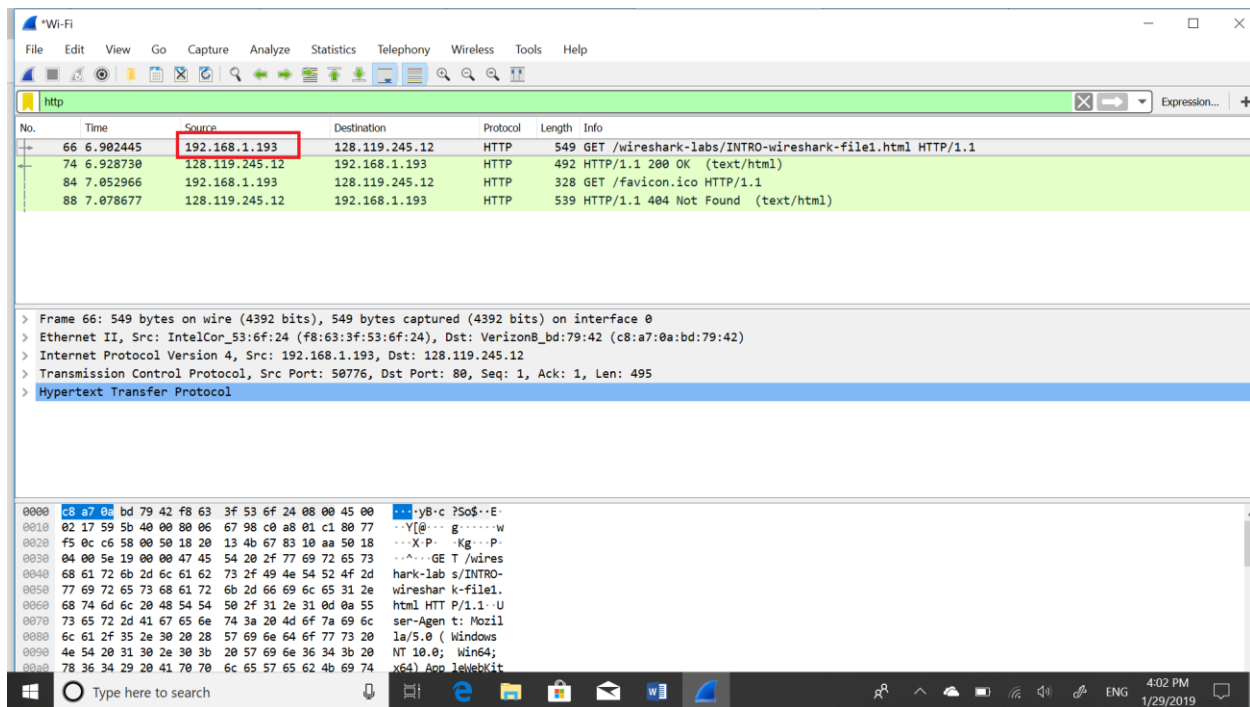


1. What is the Internet address of your computer?

The Internet address of my computer is: **192.168.1.193**

Using Wireshark:



Using Terminal:

```
Command Prompt

C:\Users\ariel>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : fios-router.home
    Link-local IPv6 Address . . . . . : fe80::b4c9:bdea:e111:c8c6%18
    IPv4 Address. . . . . : 192.168.1.193
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\ariel>
```

2. List 3 different protocols that appear in the protocol column in the unfiltered packetlisting window in step 7 above.

Protocols: **TLSv1.2, TCP, MDNS**

Wireshark packet capture window showing network traffic. The packet list pane shows several packets, with the first three highlighted in blue. The first packet is a TLSv1.2 application data packet (54 bytes). The second packet is a TCP ACK packet (54 bytes). The third packet is an MDNS query (82 bytes). The packet details pane shows the structure of the selected packet (Frame 66: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface 0). The packet bytes pane shows the raw data of the selected packet.

3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Time:

$$6.928730 - 6.902445 = 0.026285 \text{ seconds}$$

Wireshark packet capture window showing an HTTP GET request and its 200 OK response. The Time column is set to 'Time-of-day' format. The packet list shows packet 66 at 6.902445 and packet 74 at 6.928730. The packet details pane shows the structure of the HTTP response, including Ethernet II, IP, TCP, and HTTP layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
66	6.902445	192.168.1.193	128.119.245.12	HTTP	549	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
74	6.928730	128.119.245.12	192.168.1.193	HTTP	492	HTTP/1.1 200 OK (text/html)
84	7.052966	192.168.1.193	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
88	7.078677	128.119.245.12	192.168.1.193	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 74: 492 bytes on wire (3936 bits), 492 bytes captured (3936 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
> Transmission Control Protocol, Src Port: 80, Dst Port: 50776, Seq: 1, Ack: 496, Len: 438
> Hypertext Transfer Protocol
> Line-based text data: text/html (3 lines)

0000 f8 63 3f 53 6f 24 c8 a7 0a bd 79 42 08 00 45 00 ...So\$...yB...E-
0010 01 de 5c 9b 40 00 35 06 af 91 80 77 f5 0c c0 a8 ...@5...w...
0020 01 c1 00 50 c6 58 67 83 10 aa 18 20 15 3a 50 18 ...P.Xg...:P-
0030 00 ed 7f 54 00 00 48 54 54 50 2f 31 2e 31 20 32 ...T...HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK...D ate: Tue
0050 2c 20 32 39 20 4a 61 6e 20 32 30 31 39 20 32 30 , 29 Jan 2019 20
0060 3a 35 39 3a 35 39 20 47 4d 54 0d 0a 53 65 72 76 :59:59 G MT...Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per

Displaying the time in format: Time-of-day

The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
66	16:00:00.319809	192.168.1.193	128.119.245.12	HTTP	549	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
74	16:00:00.346094	128.119.245.12	192.168.1.193	HTTP	492	HTTP/1.1 200 OK (text/html)
84	16:00:00.470330	192.168.1.193	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
88	16:00:00.496041	128.119.245.12	192.168.1.193	HTTP	539	HTTP/1.1 404 Not Found (text/html)

The packet details pane for packet 74 shows the following structure:

- Frame 74: 492 bytes on wire (3936 bits), 492 bytes captured (3936 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
- Transmission Control Protocol, Src Port: 80, Dst Port: 50776, Seq: 1, Ack: 496, Len: 438
- Hypertext Transfer Protocol
- Line-based text data: text/html (3 lines)

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The ASCII portion includes the following text:

```
..c?So$...yB...E...
..Y@...g...w...
..X.P...Kg...P...
..^...GE T /wires
hark-lab s/INTRO-
wireshar k-file1.
html HT P/1.1..U
ser-Agen t: Mozil
la/5.0 (Windows
NT 10.0; Win64;
x64) App Telebit
```

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

The Internet address of gaia.cs.umass.edu is: 128.119.245.12

The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
66	6.902445	192.168.1.193	128.119.245.12	HTTP	549	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
74	6.928730	128.119.245.12	192.168.1.193	HTTP	492	HTTP/1.1 200 OK (text/html)
84	7.052966	192.168.1.193	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
88	7.078677	128.119.245.12	192.168.1.193	HTTP	539	HTTP/1.1 404 Not Found (text/html)

The packet details pane for packet 66 shows the following structure:

- Frame 66: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface 0
- Ethernet II, Src: IntelCor_53:6f:24 (f8:63:3f:53:6f:24), Dst: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42)
- Internet Protocol Version 4, Src: 192.168.1.193, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 50776, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The ASCII portion includes the following text:

```
..yB..c?So$...E...
..Y@...g...w...
..X.P...Kg...P...
..^...GE T /wires
hark-lab s/INTRO-
wireshar k-file1.
html HT P/1.1..U
ser-Agen t: Mozil
la/5.0 (Windows
NT 10.0; Win64;
x64) App Telebit
```

5. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

Name of the documents with the print:

Lab_1_GET message

Lab_1_OK message