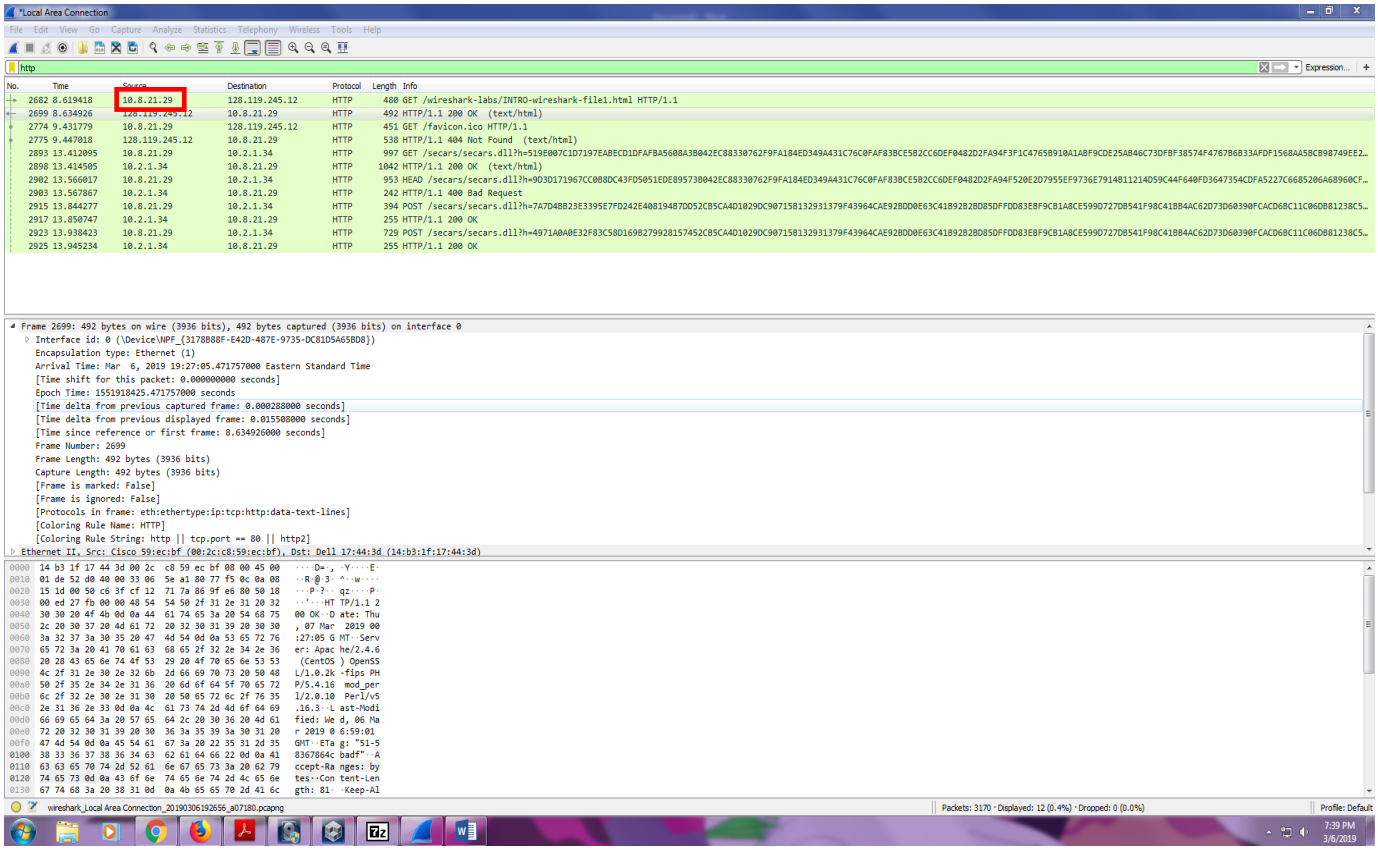
Abdullah Alrfeedi

Lab #1

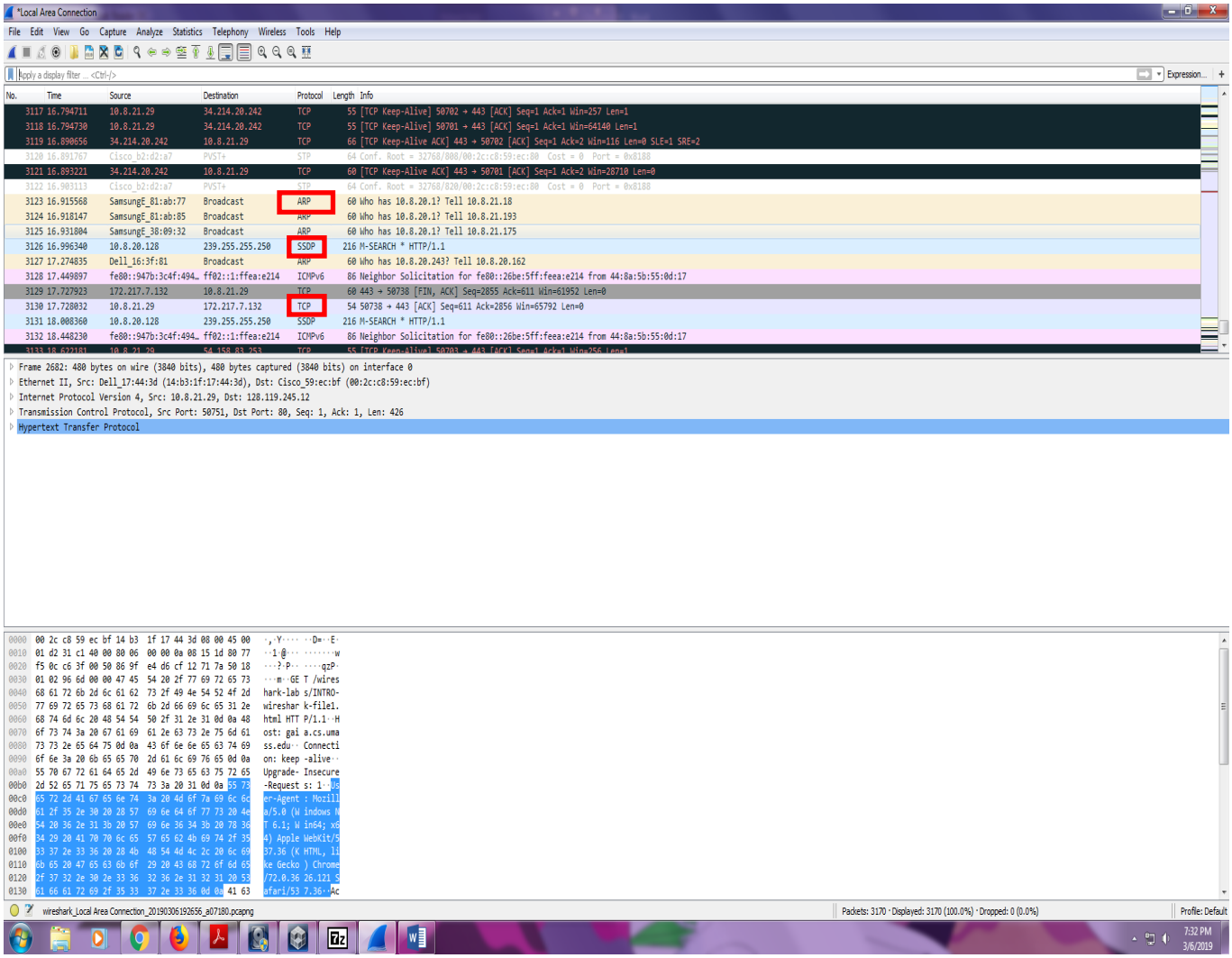
1) What is the Internet address of your computer?

The IP Address is 10.8.21.29.

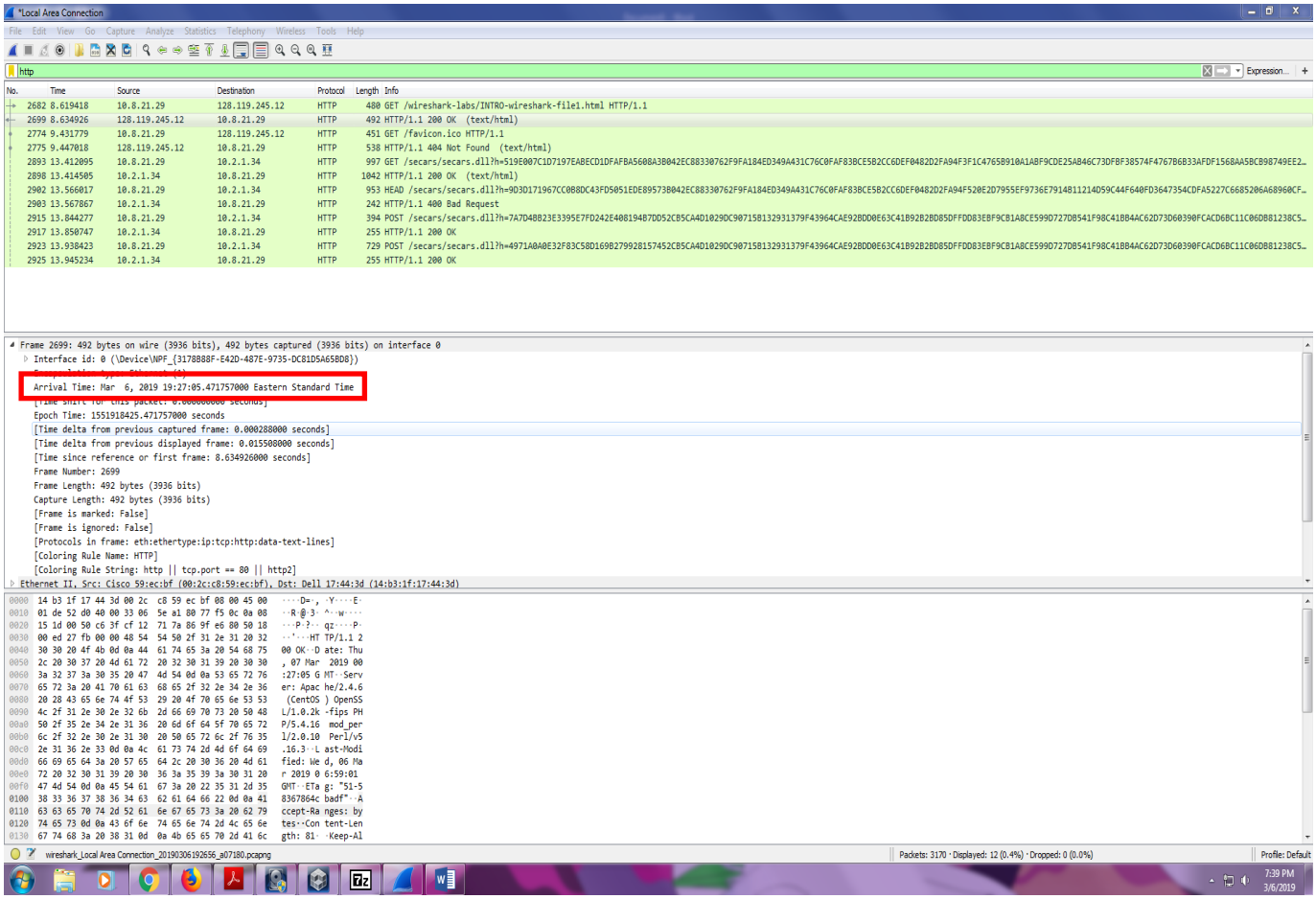


2) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

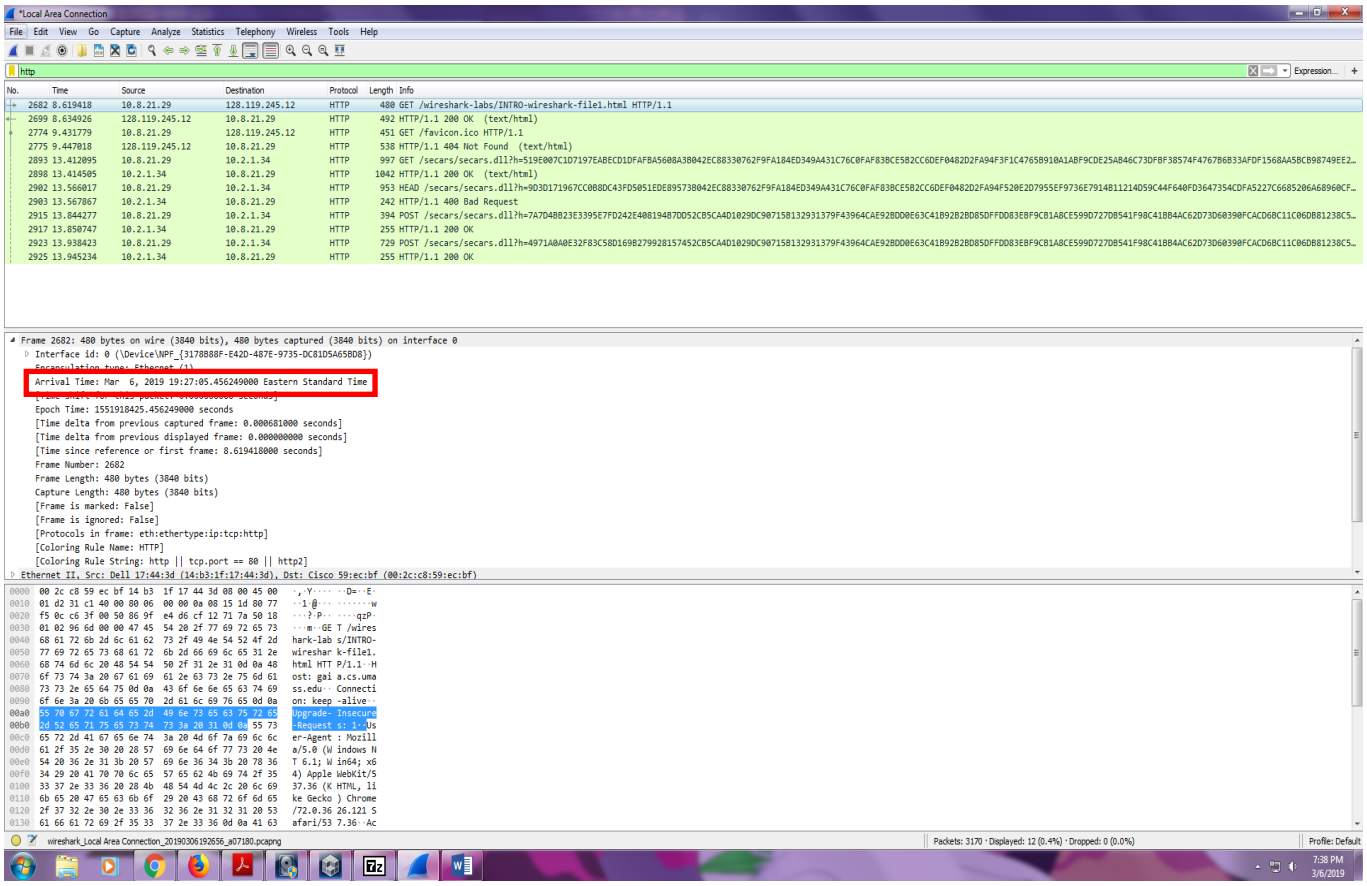
The three different protocols that appear in the packet listing are ARP, SSDP, AND TCP.



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 packet-listing 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*.)



The GET request was arrived at Mar 6,2019 19:27:05.471757000

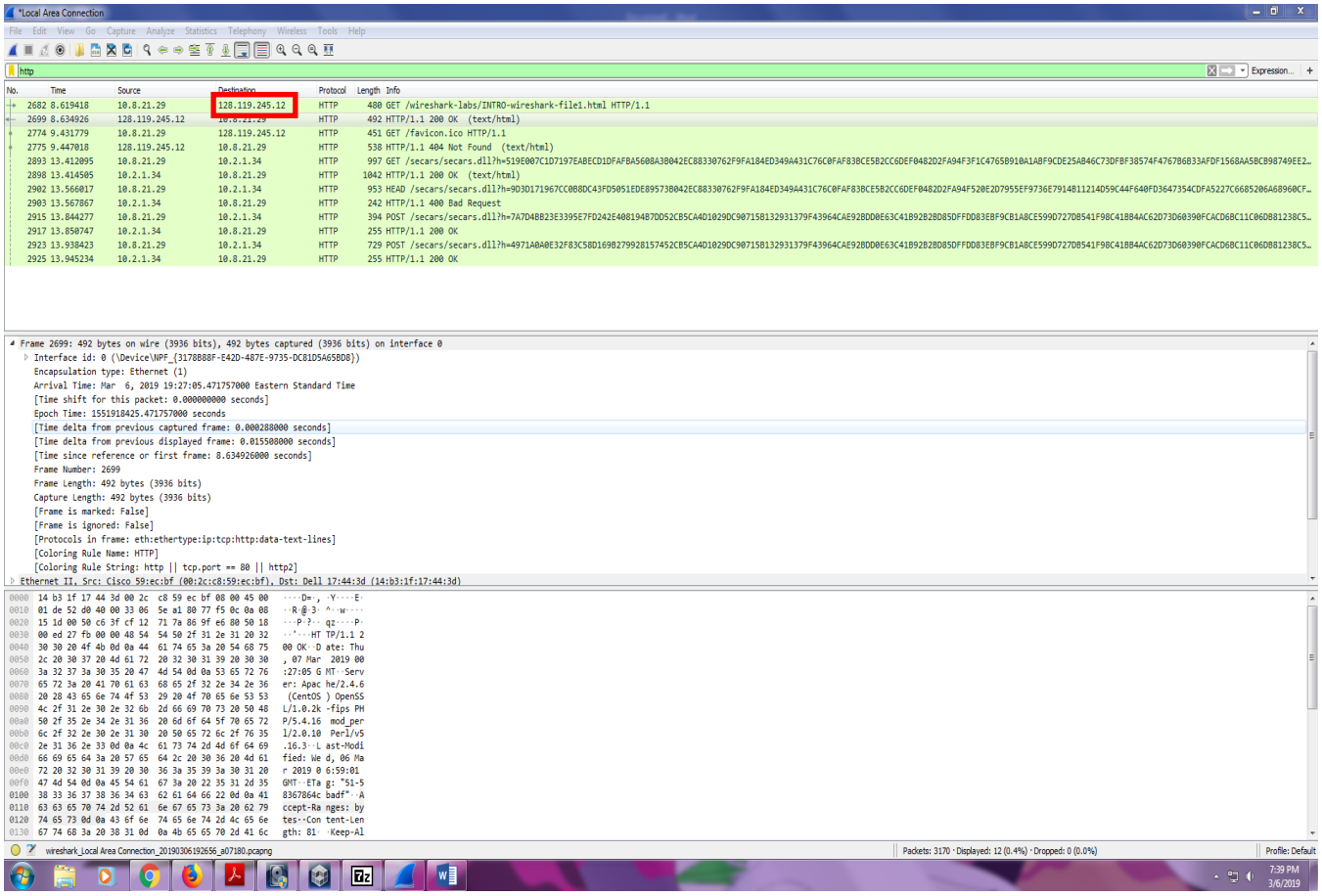


The HTTP OK is arrived at Mar 6, 2019 19:27:05.456249000

So the time took from HTTP GET TO HTTP OK is .456249000 - .471757000 = 0.015508

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

The Internet Address of gaia.cs.umass.edu is 128.119.245.12



HTTP MESSAGE GET

C:\Users\Saints\AppData\Local\Temp\wireshark_Local Area Connection_20190306192656_a07180.pcapng 3170 total packets, 12 shown

No. Time Source Destination Protocol Length Info

2682 8.619418 10.8.21.29 128.119.245.12 HTTP 480 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 2682: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0

Interface id: 0 (\Device\NPF_{3178B88F-E42D-487E-9735-DC81D5A65BD8})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2019 19:27:05.456249000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1551918425.456249000 seconds

[Time delta from previous captured frame: 0.000681000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 8.619418000 seconds]

Frame Number: 2682

Frame Length: 480 bytes (3840 bits)

Capture Length: 480 bytes (3840 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: Dell_17:44:3d (14:b3:1f:17:44:3d), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)

Internet Protocol Version 4, Src: 10.8.21.29, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50751, Dst Port: 80, Seq:
1, Ack: 1, Len: 426 Hypertext Transfer Protocol

HTTP MESSAGE OK

C:\Users\Saints\AppData\Local\Temp\wireshark_Local Area Connection_20190306192656_a07180.pcapng 3170 total packets, 12 shown

No. Time Source Destination Protocol Length Info

2699 8.634926 128.119.245.12 10.8.21.29 HTTP 492 HTTP/1.1 200 OK (text/html)

Frame 2699: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0

Interface id: 0 (\Device\NPF_{3178B88F-E42D-487E-9735-DC81D5A65BD8})

Encapsulation type: Ethernet (1)

Arrival Time: Mar 6, 2019 19:27:05.471757000 Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1551918425.471757000 seconds

[Time delta from previous captured frame: 0.000288000 seconds]

[Time delta from previous displayed frame: 0.015508000 seconds]

[Time since reference or first frame: 8.634926000 seconds]

Frame Number: 2699

Frame Length: 492 bytes (3936 bits)

Capture Length: 492 bytes (3936 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: Cisco_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell_17:44:3d (14:b3:1f:17:44:3d)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.21.29

Transmission Control Protocol, Src Port: 80, Dst Port: 50751, Seq: 1, Ack: 427, Len: 438

Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)