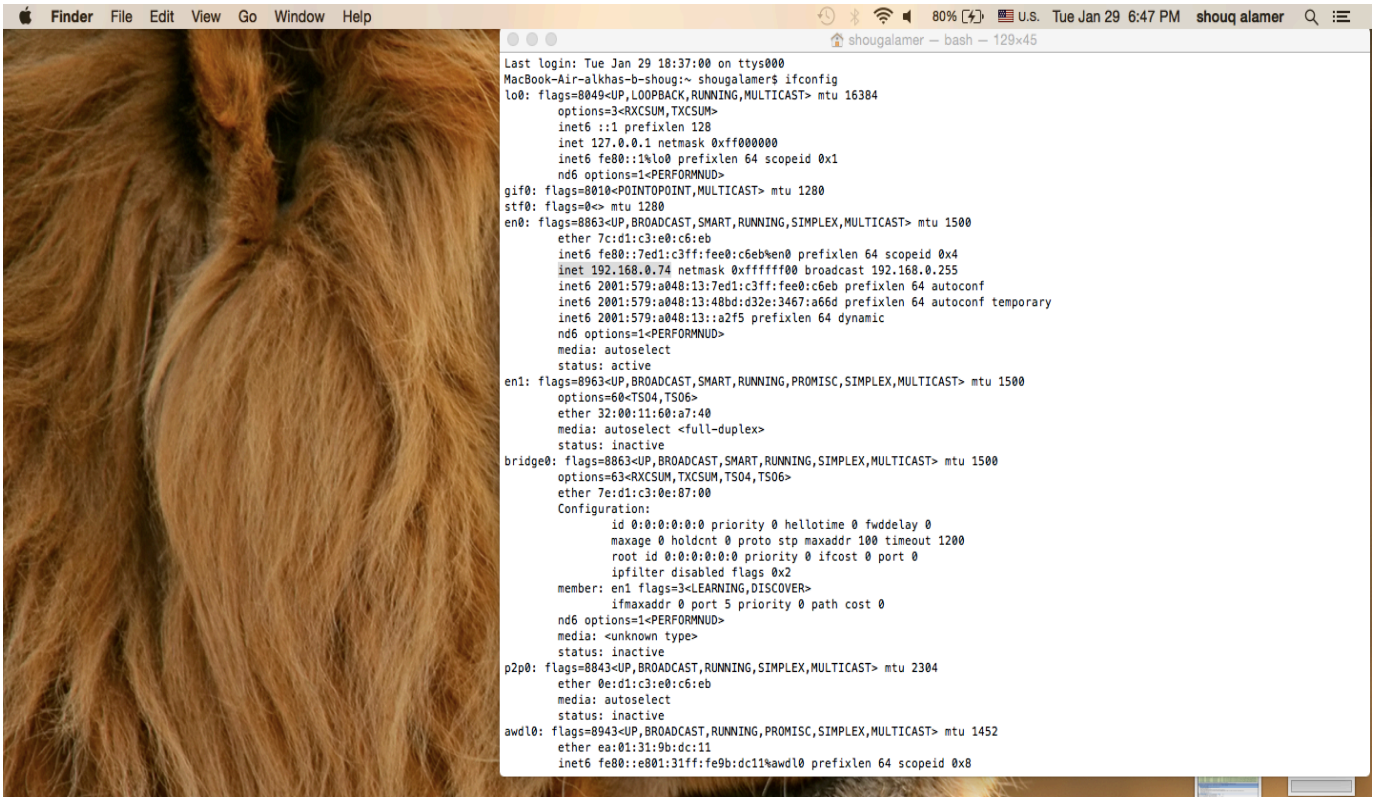
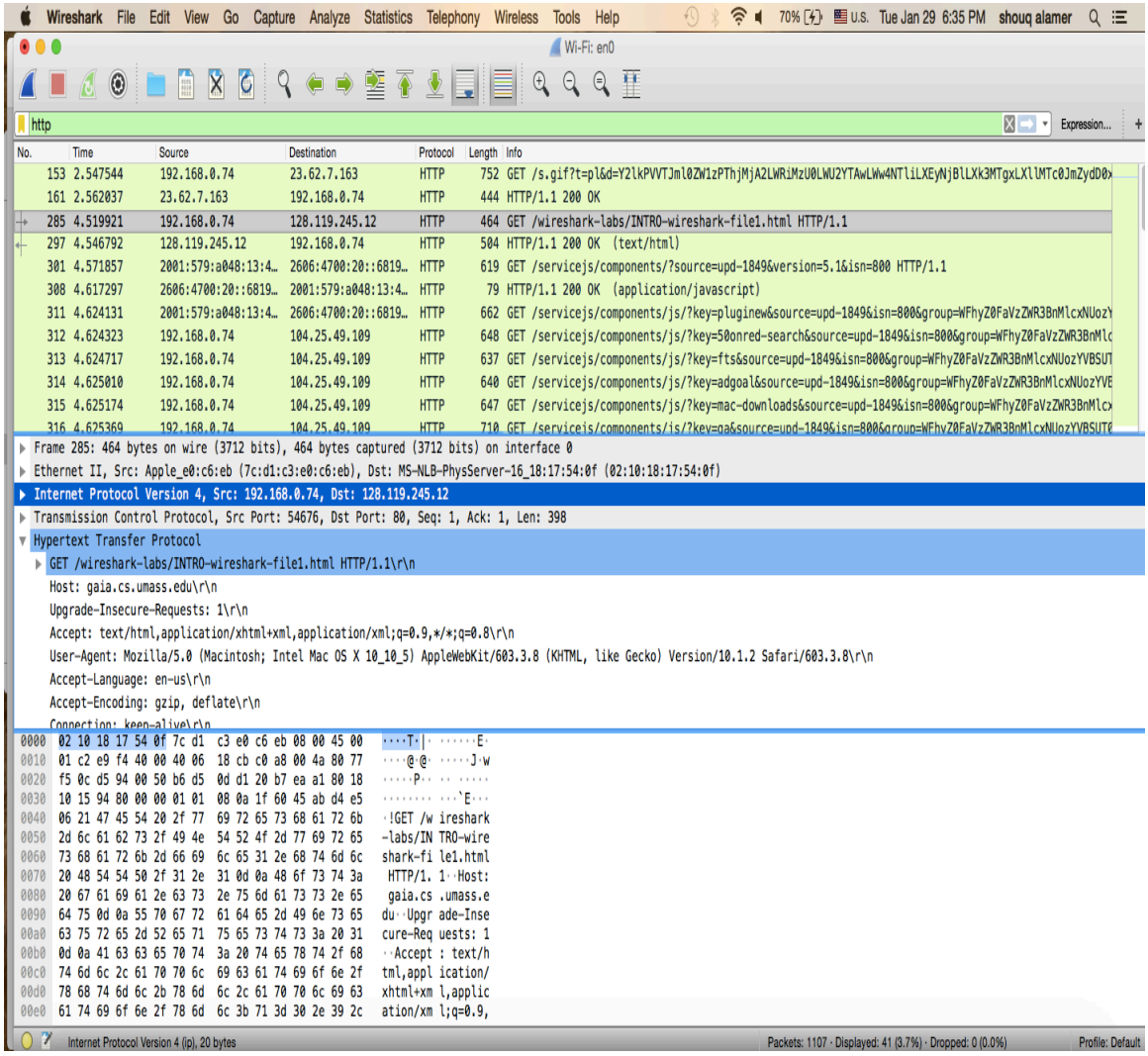
Shouq Alamer
IT-520-LAB1
Jan 31 2019



Questions:

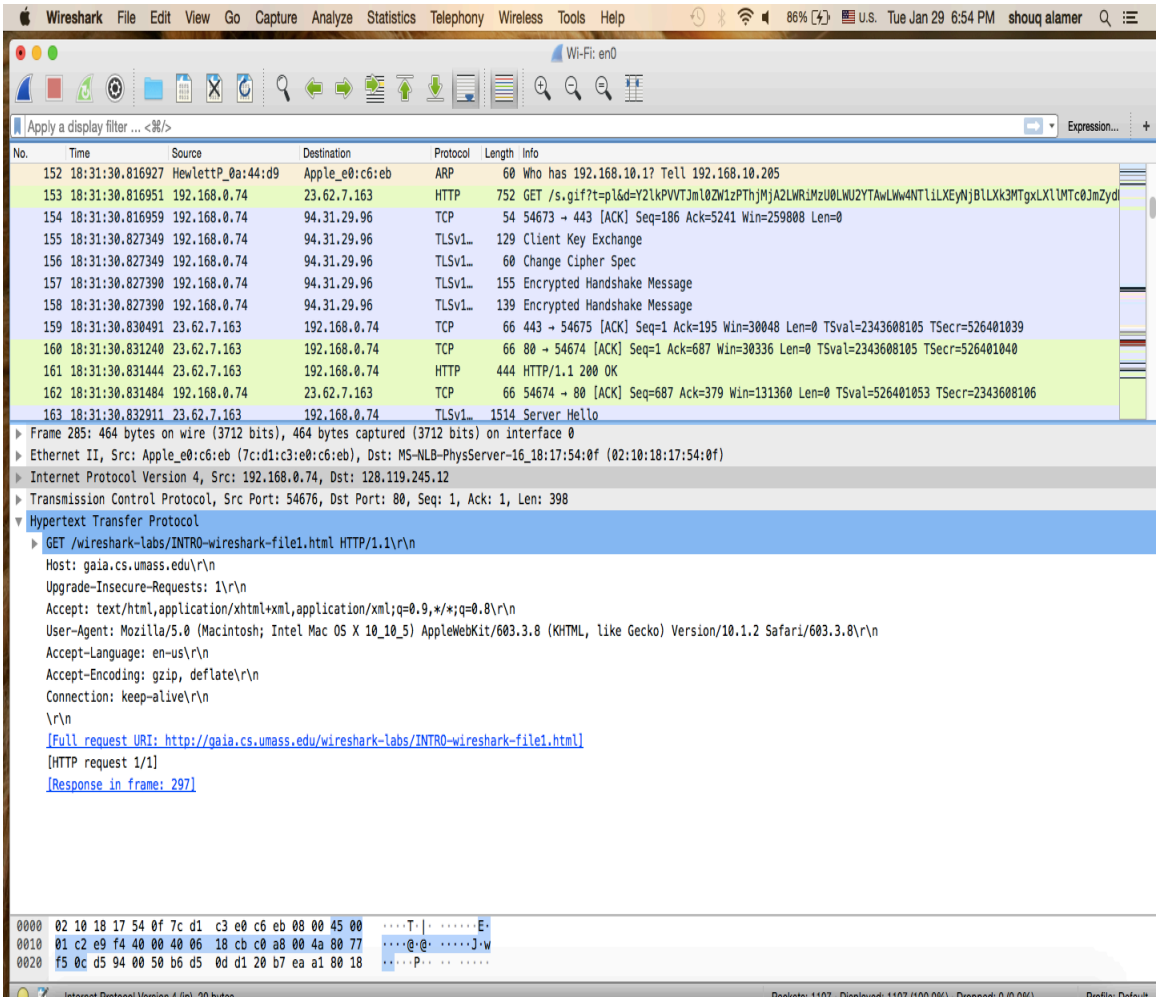
1. What is the Internet address of your computer?

192.168.0.74



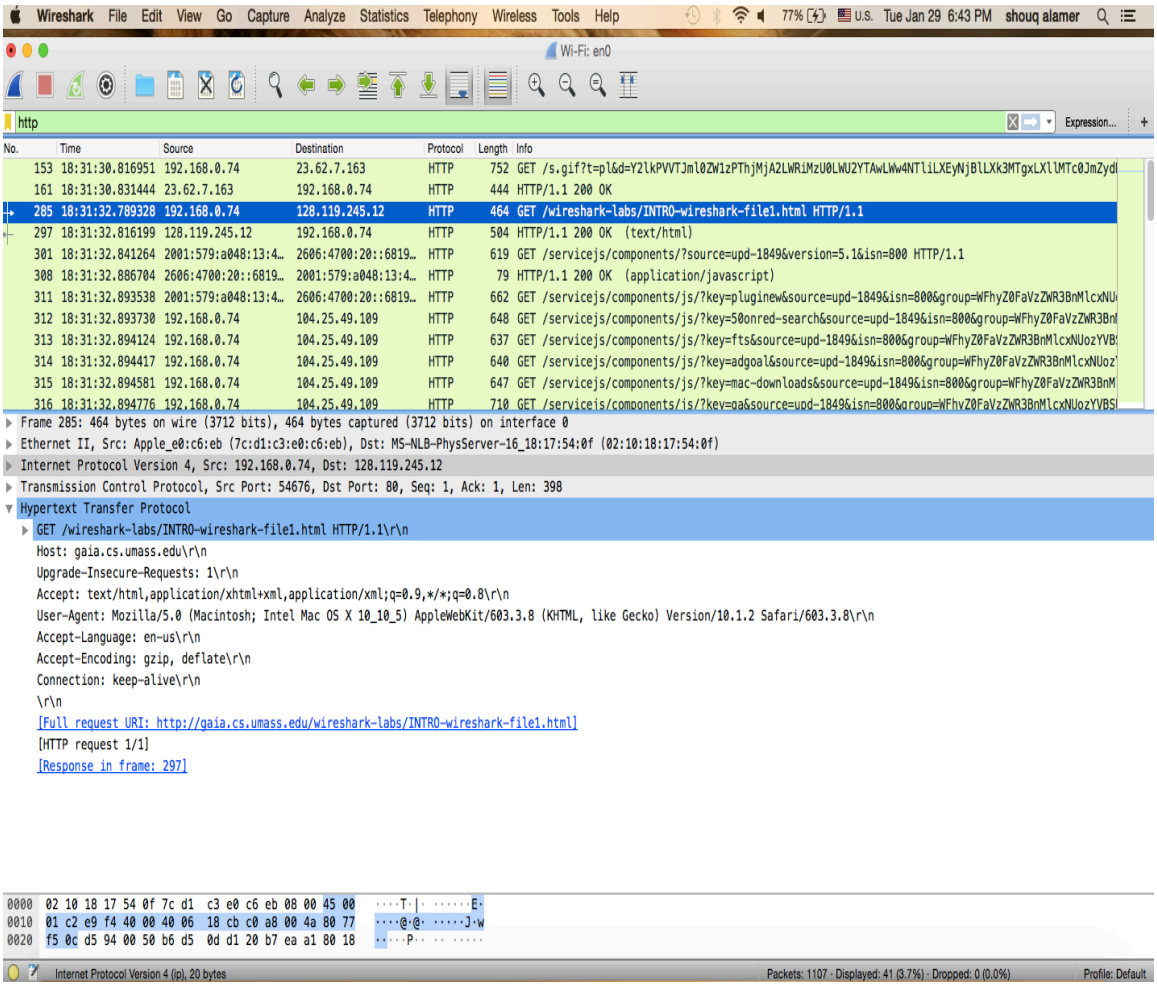
2. List 3 different protocols that appear in the protocol column in the unfiltered packet- listing window in step 7 above.

ARP
HTTP
TCP



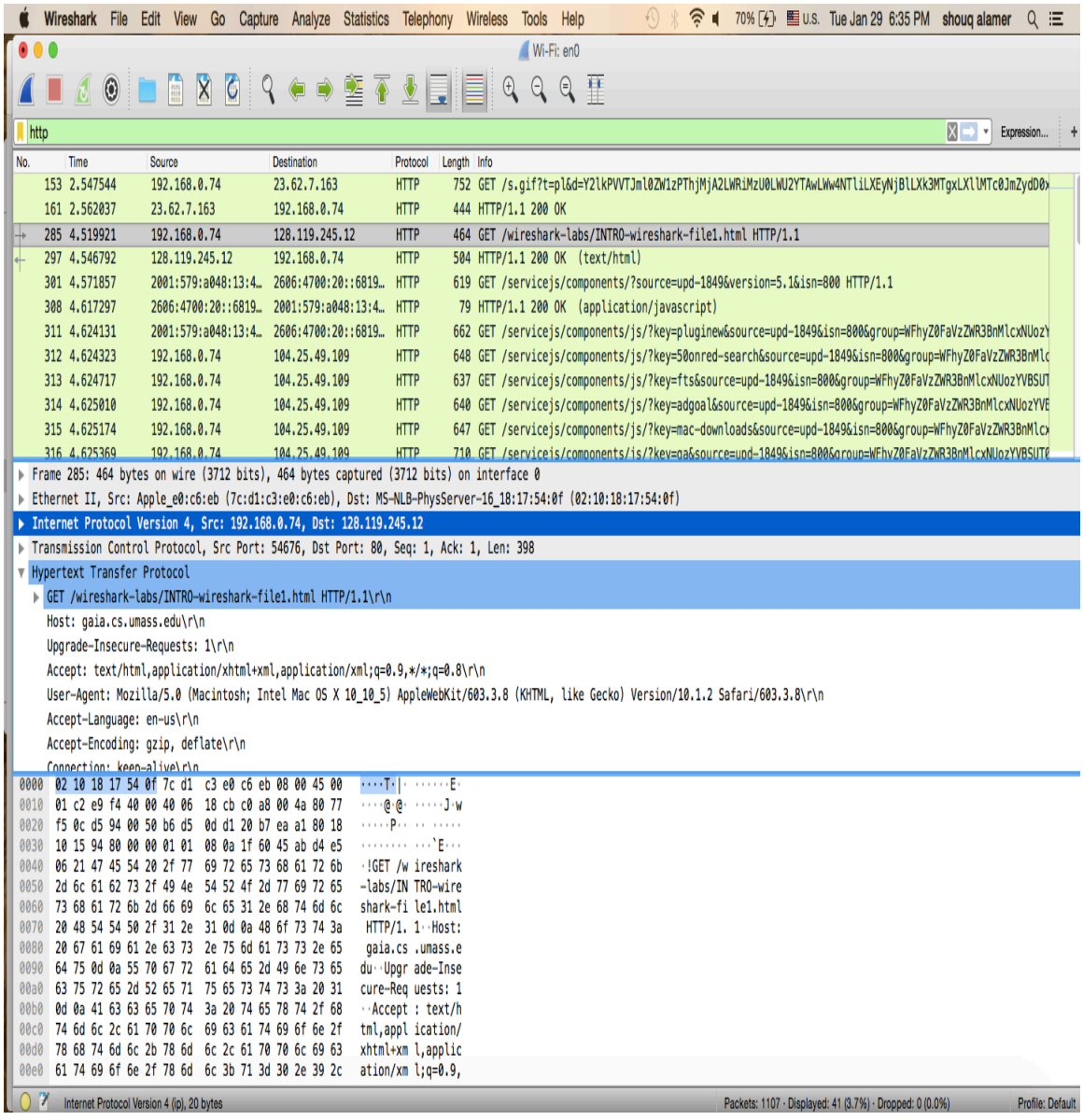
3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark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

GET = 18:31:32:789328
OK = 18:31:32:816199
DIFFRENCE= 00:00:00:026871



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

128.119.245.12



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.

GET

/var/folders/2p/1gs3fhtn08ncl7wj3dnnprn00000gn/T//wireshark_en0_20190129183128_mZfOFI.pcapng 1107 total packets, 41 shown

```
No.     Time               Source                Destination           Protocol Length Info
    285 18:31:32.789328    192.168.0.74          128.119.245.12        HTTP     464    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 285: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
Ethernet II, Src: Apple_e0:c6:eb (7c:d1:c3:e0:c6:eb), Dst: MS-NLB-PhysServer-16_18:17:54:0f
(02:10:18:17:54:0f)
Internet Protocol Version 4, Src: 192.168.0.74, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54676, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/603.3.8 (KHTML, like
Gecko) Version/10.1.2 Safari/603.3.8\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 297]
```

OK

/var/folders/2p/1gs3fhtn08ncl7wj3dnnprn00000gn/T//wireshark_en0_20190129183128_mZfOFI.pcapng 1107 total packets, 41 shown

```
No.     Time               Source                Destination           Protocol Length Info
    297 18:31:32.816199    128.119.245.12        192.168.0.74          HTTP     504    HTTP/1.1
200 OK  (text/html)
Frame 297: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
Ethernet II, Src: MS-NLB-PhysServer-16_18:17:54:0f (02:10:18:17:54:0f), Dst: Apple_e0:c6:eb
(7c:d1:c3:e0:c6:eb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.74
Transmission Control Protocol, Src Port: 80, Dst Port: 54676, Seq: 1, Ack: 399, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 29 Jan 2019 23:31:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 29 Jan 2019 06:59:01 GMT\r\n
    ETag: "51-580935402e3a9"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.026871000 seconds]
    [Request in frame: 285]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```