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

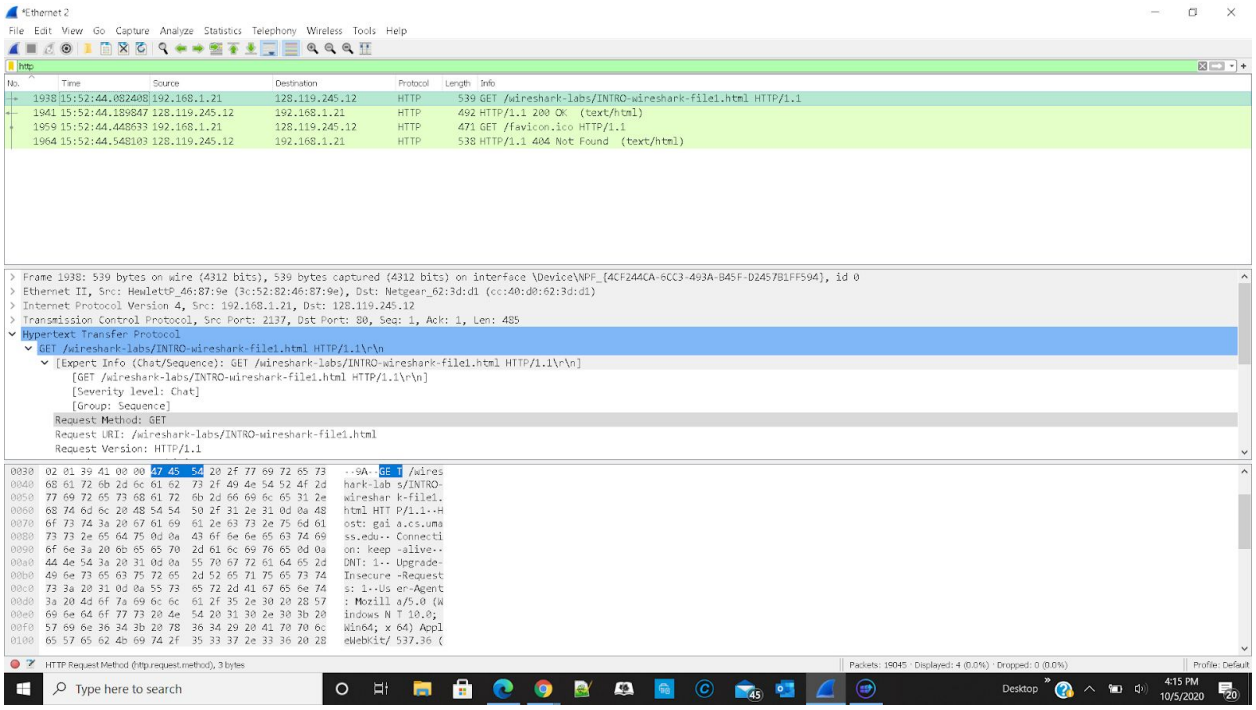
There were many different types of packet listings I saw. To name three of the protocols from the unfiltered packet-listing, I saw TCP, HTTP, and QUIC.

2. 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.)

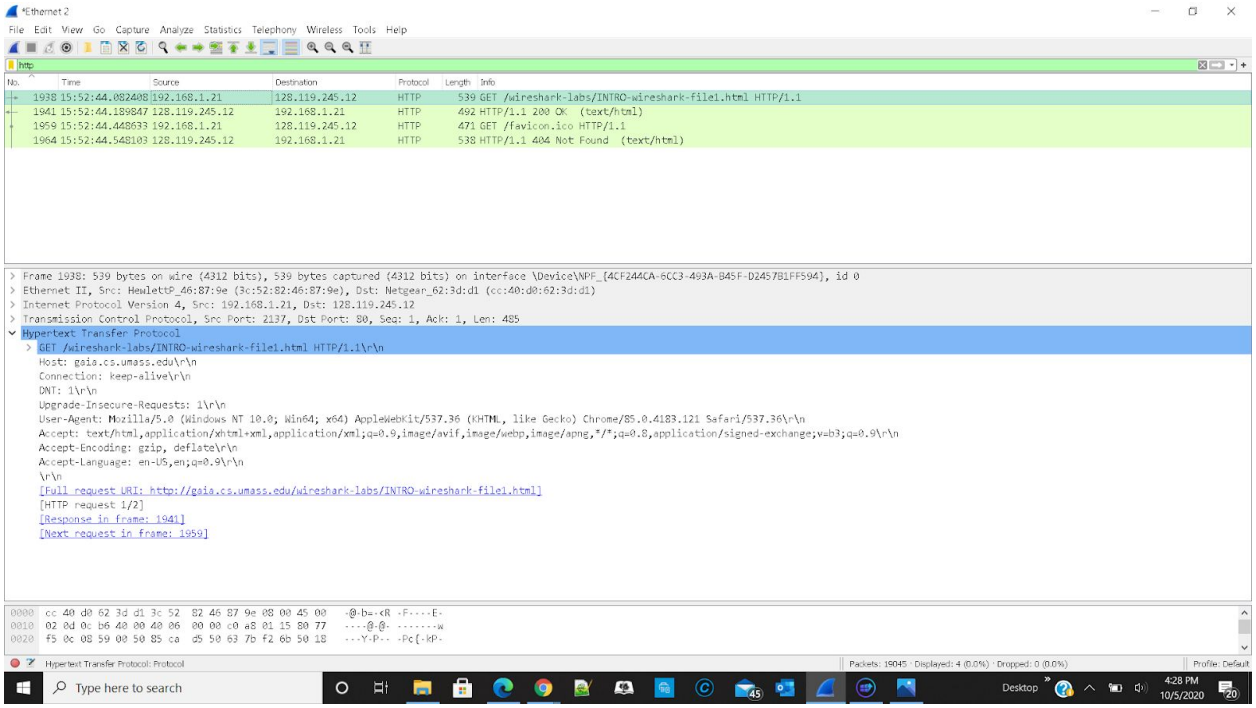
The time of the GET message was 15:52:44.082408. The time of the OK message was 15:52:44.189847.

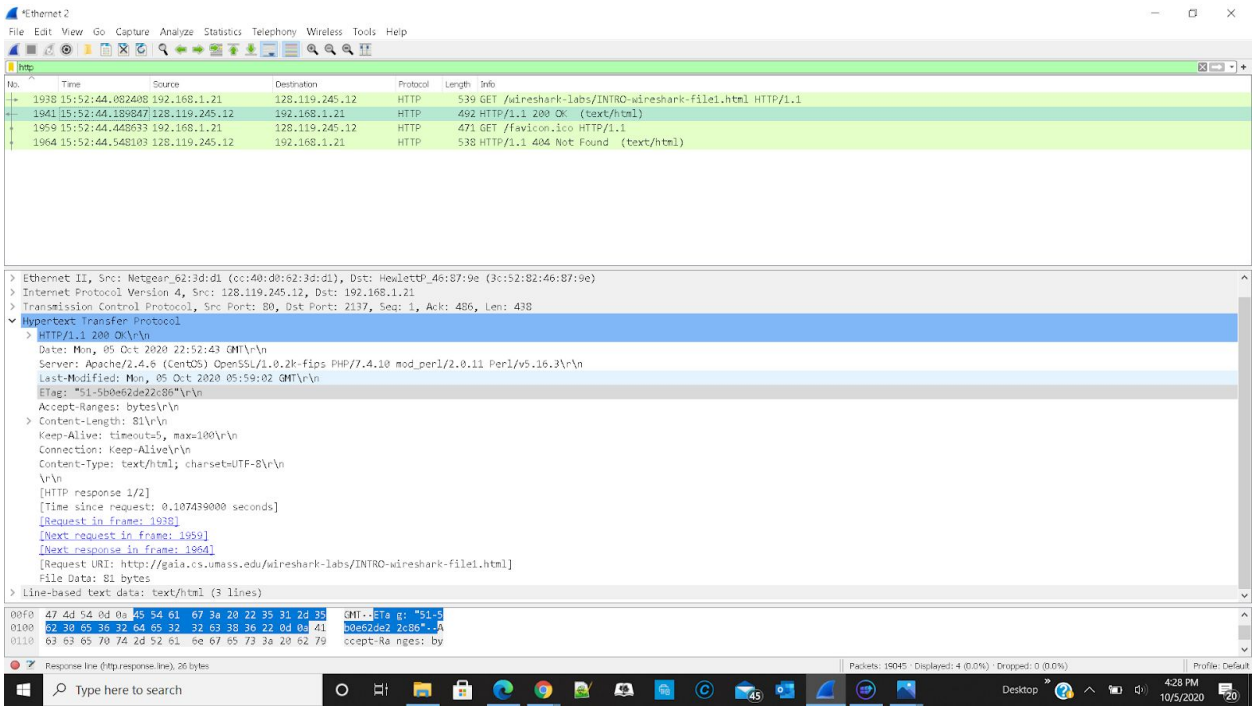
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

The internet address of the gaia.cs.umass.edu was 128.119.245.12. The internet address of my computer is 192.168.1.21.



4. 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


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1938 15:52:44.082408 192.168.1.21 128.119.245.12 HTTP 539 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1941 15:52:44.189847 128.119.245.12 192.168.1.21 HTTP 492 HTTP/1.1 200 OK (text/html)
1959 15:52:44.448633 192.168.1.21 128.119.245.12 HTTP 471 GET /favicon.ico HTTP/1.1
1964 15:52:44.548103 128.119.245.12 192.168.1.21 HTTP 538 HTTP/1.1 404 Not Found (text/html)
Frame 1938: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{4CF244CA-6CC3-493A-B45F-D2457B1FF594}, id 0
Ethernet II, Src: HewlettP_46:87:9e (3c:52:82:46:87:9e), Dst: Netgear_62:3d:d1 (cc:40:d0:62:3d:d1)
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 2137, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 1941]
[Next request in frame: 1959]
0000 cc 40 d0 62 3d d1 3c 52 82 46 87 9e 08 00 45 00
0010 02 0d 0c b6 40 00 40 06 00 00 c0 a8 01 15 80 77
0020 f5 0c 08 59 00 50 85 ca d5 50 63 7b f2 6b 50 18
Hypertext Transfer Protocol: Protocol
Packets: 19045 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Desktop
4:28 PM
10/5/2020


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1938 15:52:44.082408 192.168.1.21 128.119.245.12 HTTP 539 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1941 15:52:44.189847 128.119.245.12 192.168.1.21 HTTP 492 HTTP/1.1 200 OK (text/html)
1959 15:52:44.448633 192.168.1.21 128.119.245.12 HTTP 471 GET /favicon.ico HTTP/1.1
1964 15:52:44.548103 128.119.245.12 192.168.1.21 HTTP 538 HTTP/1.1 404 Not Found (text/html)
Ethernet II, Src: Netgear_62:3d:d1 (cc:40:d0:62:3d:d1), Dst: HewlettP_46:87:9e (3c:52:82:46:87:9e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.21
Transmission Control Protocol, Src Port: 80, Dst Port: 2137, Seq: 1, Ack: 486, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 05 Oct 2020 22:52:43 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Mon, 05 Oct 2020 05:59:02 GMT\r\n
ETag: "51-5b0e62de22c86"\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 1/2]
[Time since request: 0.107439000 seconds]
[Request in frame: 1938]
[Next request in frame: 1959]
[Next response in frame: 1964]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
Line-based text data: text/html (3 lines)
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 35
0100 62 30 65 36 32 64 65 32 32 63 38 36 22 0d 0a 41
0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79
Response line (http.response.line), 26 bytes
Packets: 19045 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Desktop
4:28 PM
10/5/2020