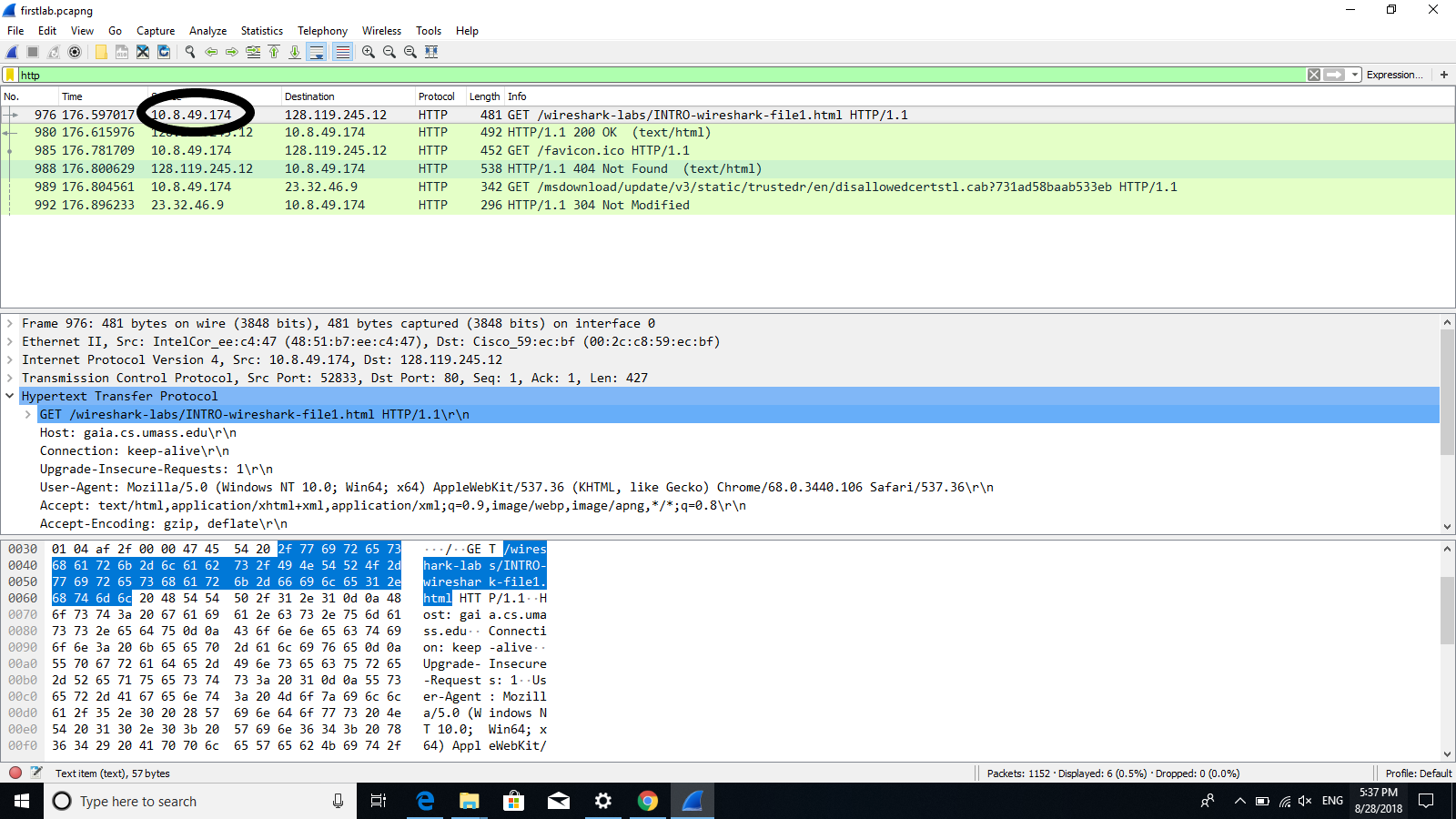
Abdalrhman Abdalla

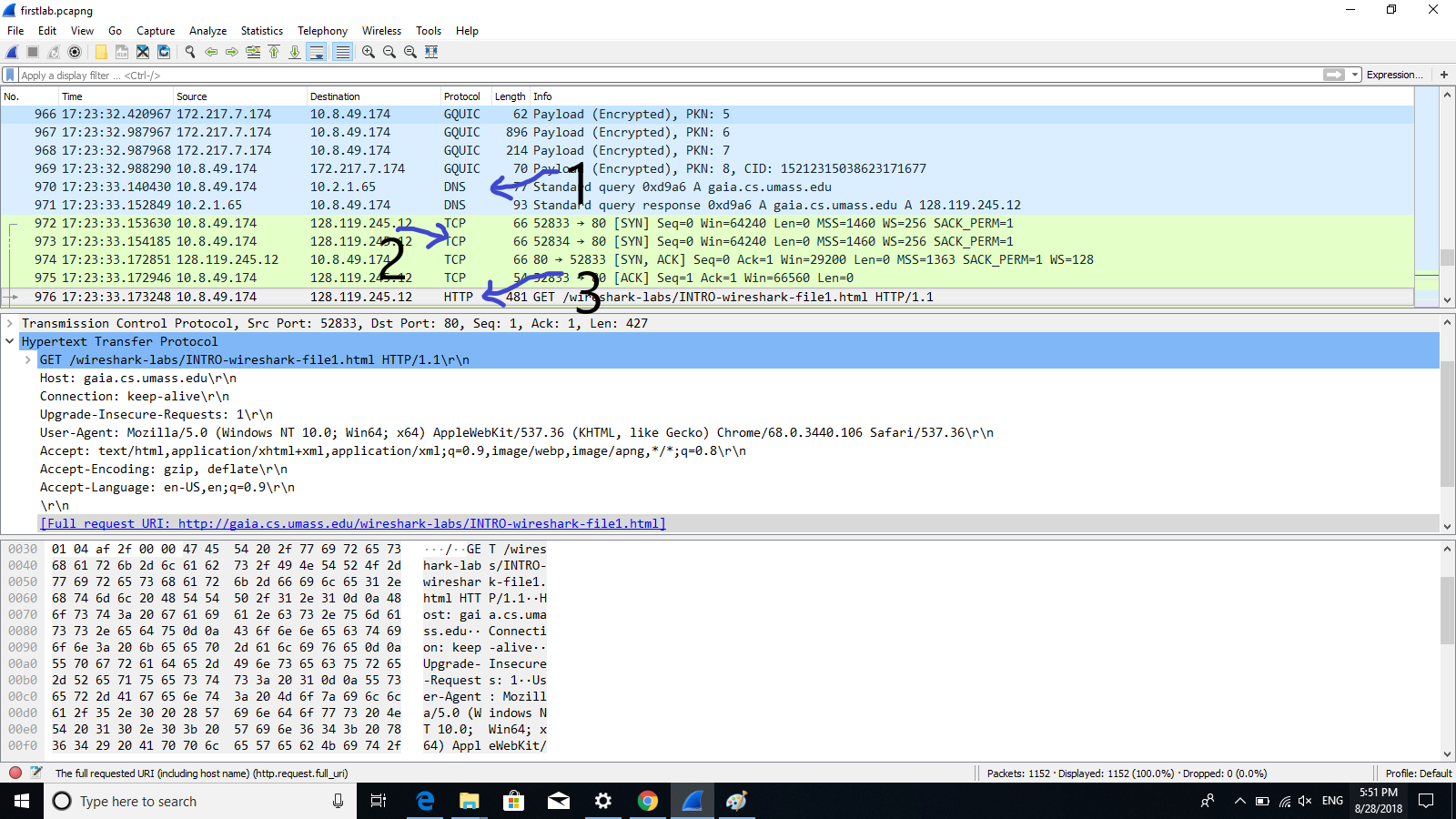
1. 1. What is the Internet address of your computer?

10.8.49.174



2. List 3 different protocols that appear in the protocol column in the unfiltered

packet-listing window in step 7 above.

DNS, TCP, HTTP

3. How long did it take from when the HTTP GET message was sent until the HTTP

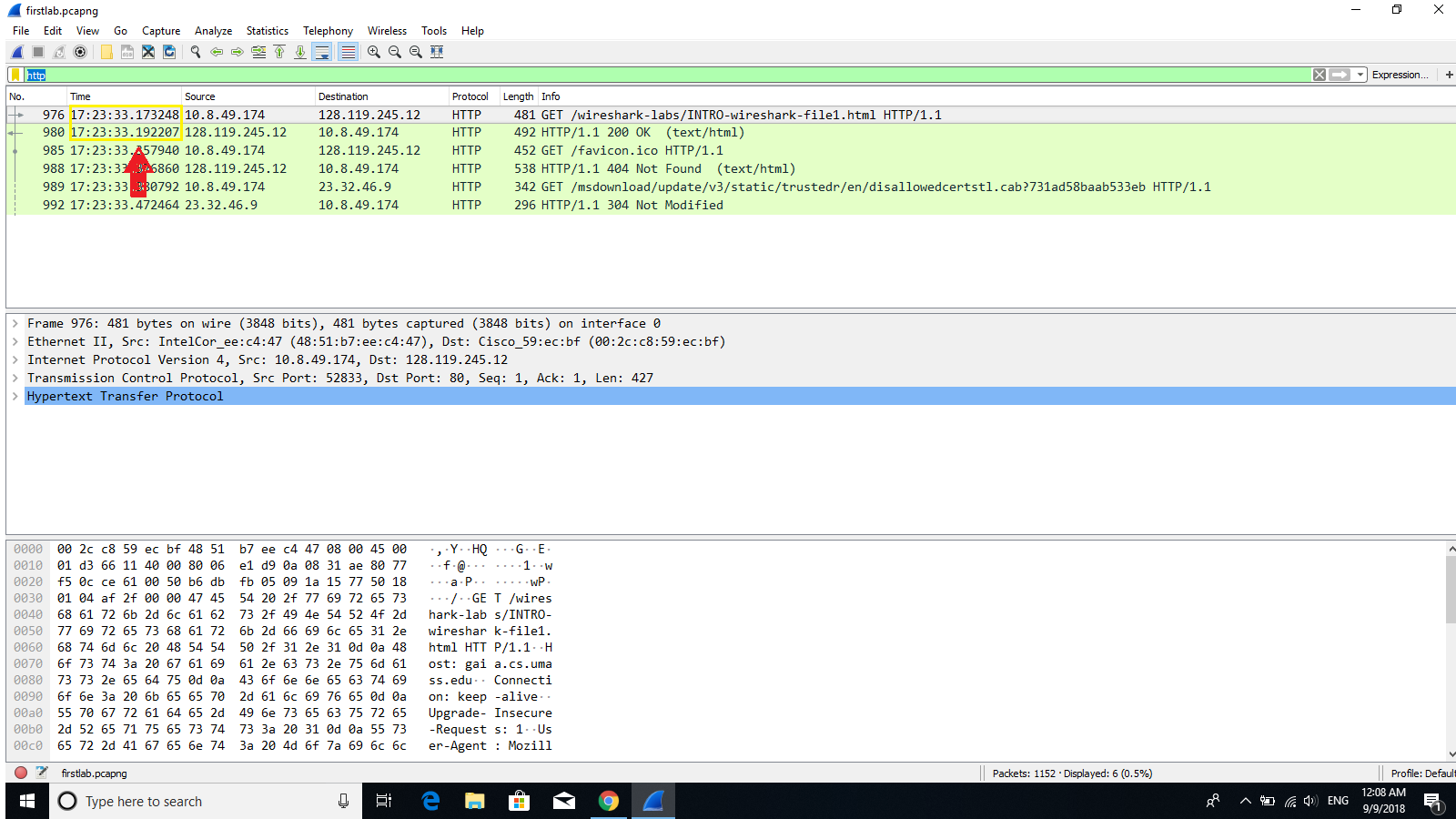
OK reply was received? (By default, the value of the Time column in the packetlisting

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

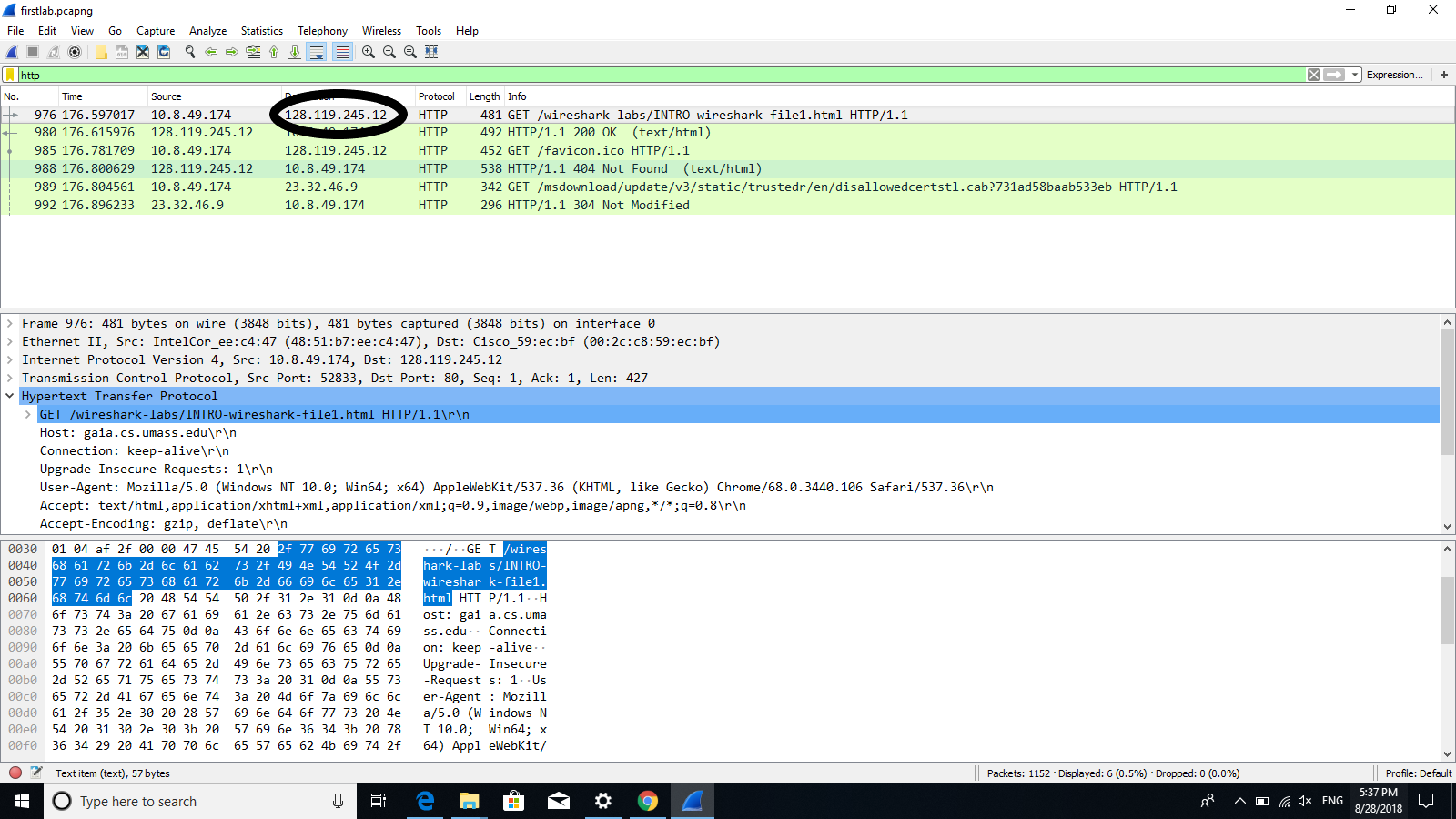
down menu, then select Time Display Format, then select Time-of-day.)

.018959 second



4. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.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 C :\U sers\A bdalrhman\D ocuments\firstlab.pcapng 1152 total packets, 6 show n

No. Time Source Destination Protocol Length Info

976 176.597017 10.8.49.174 128.119.245.12 HTTP 481 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/

1.1

Frame 976: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0

Ethernet II, Src: IntelCor\_ee:c4:47 (48:51:b7:ee:c4:47), Dst: Cisco\_59:ec:bf (00:2c:c8:59:ec:bf)

Internet Protocol Version 4, Src: 10.8.49.174, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 52833, Dst Port: 80, Seq: 1, Ack: 1, Len: 427

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

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8\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: 980]

1. [Next request in frame: 985]

OK C :\U sers\A bdalrhman\D ocuments\firstlab.pcapng 1152 total packets, 6 show n

No. Time Source Destination Protocol Length Info

980 176.615976 128.119.245.12 10.8.49.174 HTTP 492 HTTP/1.1 200 OK (text/html)

Frame 980: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0

Ethernet II, Src: Cisco\_59:ec:bf (00:2c:c8:59:ec:bf), Dst: IntelCor\_ee:c4:47 (48:51:b7:ee:c4:47)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.49.174

Transmission Control Protocol, Src Port: 80, Dst Port: 52833, Seq: 1, Ack: 428, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 28 Aug 2018 21:23:32 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, 28 Aug 2018 05:59:01 GMT\r\n

ETag: "51-5747889e2ab23"\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: 0.018959000 seconds]

[Request in frame: 976]

[Next request in frame: 985]

[Next response in frame: 988]

File Data: 81 bytes

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