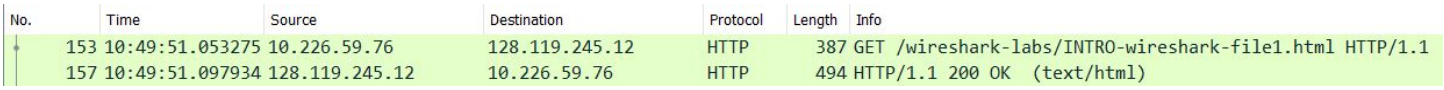
Sterling Price - U49743231
Matthew Kramer - U20891900
CNT 4004.001 - Wireshark Lab 1

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

1. ARP
2. HTTP
3. TCP
4. TLSv1.2

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.)

It took ~40 milliseconds from when the HTTP GET message was sent until the HTTP OK reply was received.



No.	Time	Source	Destination	Protocol	Length	Info
153	10:49:51.053275	10.226.59.76	128.119.245.12	HTTP	387	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
157	10:49:51.097934	128.119.245.12	10.226.59.76	HTTP	494	HTTP/1.1 200 OK (text/html)

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

The Internet address of the gaia.cs.umass.edu server is **128.119.245.12** (*destination* for HTTP GET message, *source* for HTTP OK reply). The internet address of our computer is **10.226.59.76** (*source* for HTTP GET message, *destination* for HTTP OK reply).

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.

```
210 total packets, 6 shown
153 10:49:51.053275     10.226.59.76      128.119.245.12    HTTP        387
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 153: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface 0
Ethernet II, Src: LiteonTe_27:75:37 (c8:ff:28:27:75:37), Dst: CiscoInc_9f:f0:00
      (00:00:0c:9f:f0:00)
Internet Protocol Version 4, Src: 10.226.59.76, Dst: 128.119.245.12
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 373
      Identification: 0x2ba4 (11172)
      Flags: 0x02 (Don't Fragment)
      Fragment offset: 0
      Time to live: 128
      Protocol: TCP (6)
      Header checksum: 0x122d [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.226.59.76
      Destination: 128.119.245.12
```

```
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 63847, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
      Source Port: 63847
      Destination Port: 80
      [Stream index: 5]
      [TCP Segment Len: 333]
      Sequence number: 1 (relative sequence number)
      [Next sequence number: 334 (relative sequence number)]
      Acknowledgment number: 1 (relative ack number)
      Header Length: 20 bytes
      Flags: 0x018 (PSH, ACK)
      Window size value: 256
      [Calculated window size: 65536]
      [Window size scaling factor: 256]
      Checksum: 0x7379 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
      [SEQ/ACK analysis]
Hypertext Transfer Protocol
      GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101
      Firefox/47.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\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 1/3]
      [Response in frame: 157]
      [Next request in frame: 171]

157 10:49:51.097934     128.119.245.12    10.226.59.76      HTTP 494          HTTP/1.1
200 OK (text/html)
Frame 157: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0
Ethernet II, Src: CiscoInc_21:88:c1 (40:55:39:21:88:c1), Dst: LiteonTe_27:75:37
      (c8:ff:28:27:75:37)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.226.59.76
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 480
      Identification: 0x5b9a (23450)
      Flags: 0x02 (Don't Fragment)
      Fragment offset: 0
      Time to live: 46
      Protocol: TCP (6)
      Header checksum: 0x33cc [validation disabled]
```

```
      [Header checksum status: Unverified]
      Source: 128.119.245.12
      Destination: 10.226.59.76
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 63847, Seq: 1, Ack: 334, Len: 440
      Source Port: 80
      Destination Port: 63847
      [Stream index: 5]
      [TCP Segment Len: 440]
      Sequence number: 1 (relative sequence number)
      [Next sequence number: 441 (relative sequence number)]
      Acknowledgment number: 334 (relative ack number)
      Header Length: 20 bytes
      Flags: 0x018 (PSH, ACK)
      Window size value: 237
      [Calculated window size: 30336]
      [Window size scaling factor: 128]
      Checksum: 0x2a0d [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
      [SEQ/ACK analysis]
Hypertext Transfer Protocol
      HTTP/1.1 200 OK\r\n
```