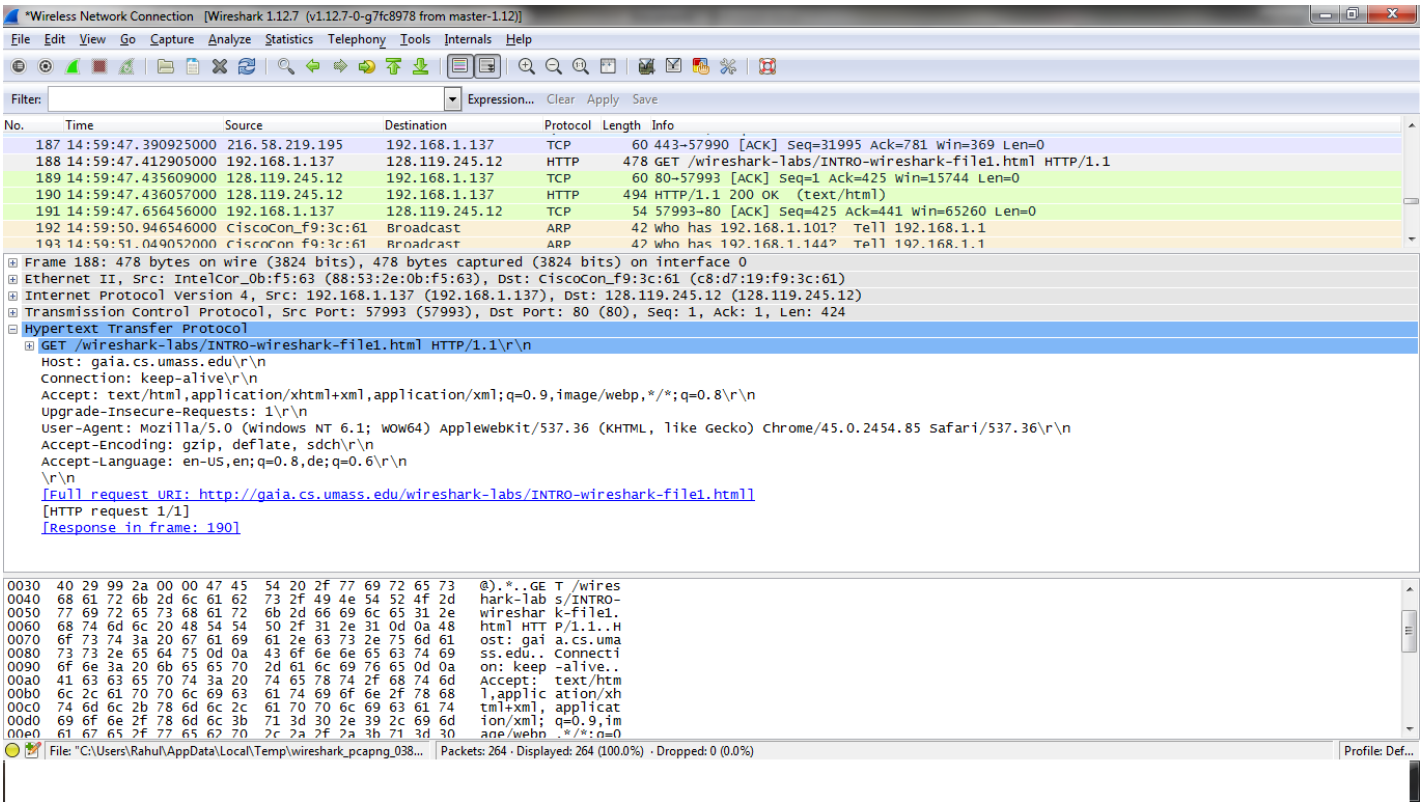
Assignment 1 - Wireshark Lab: Getting Started

Answer 1:

The three different protocols in the protocol column are:

1. HTTP – Hypertext Transfer Protocol
2. TCP – Transmission Control Protocol
3. ARP – Address Resolution Protocol

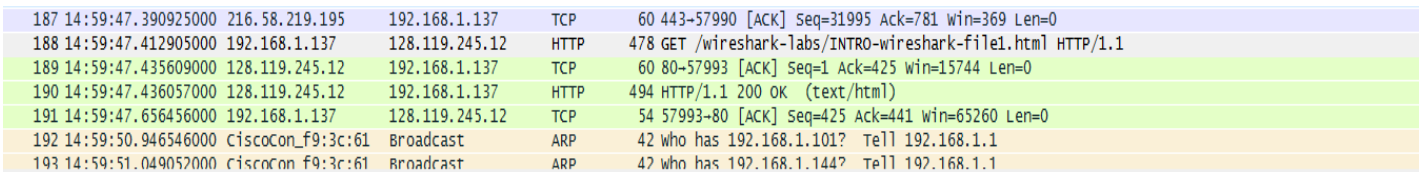


Answer 2:

The time at which the HTTP GET message was sent is = **14:59:47.412905000**

The time at which the HTTP OK reply was received is = **14:59:47.436057000**

The time elapsed between these two is = **0.023152** seconds

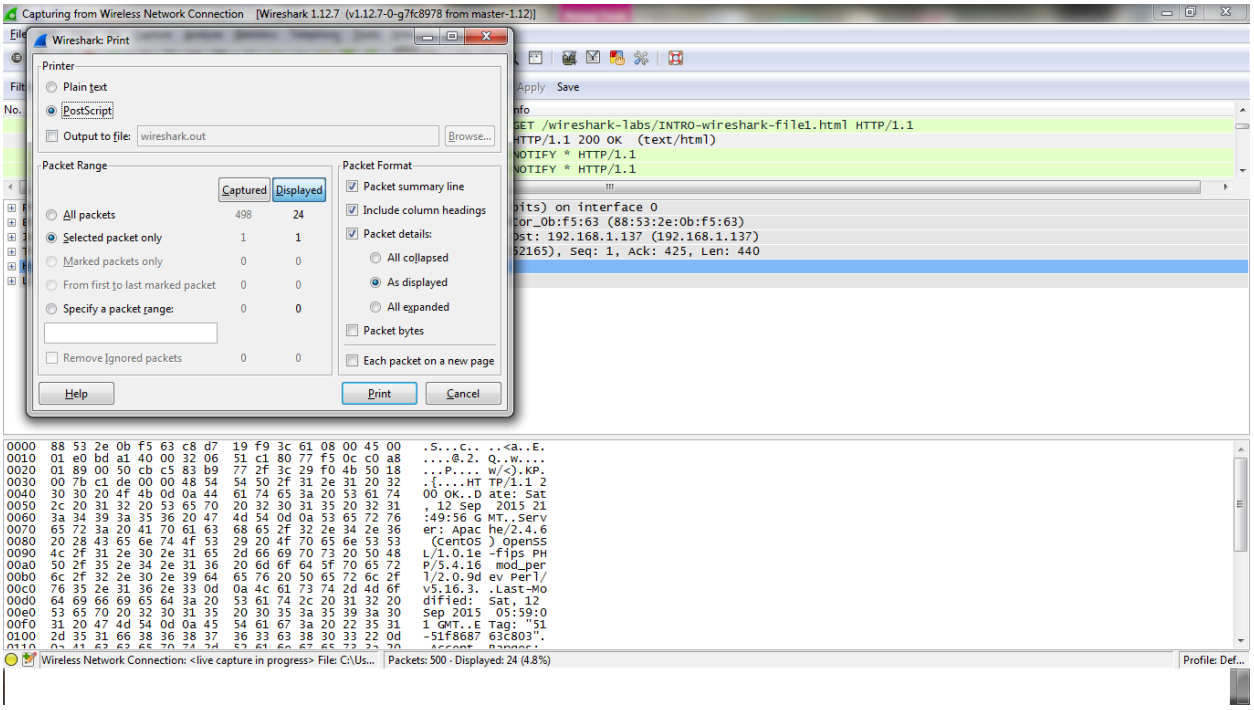


Answer3:

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

The Internet Address of my computer is **192.168.1.137**

Answer4:



The two messages are shown below:

1. **Packet Print of GET message –**

```
No.     Time               Source                Destination           Protocol Length Info
    188 14:59:47.412905000 192.168.1.137         128.119.245.12        HTTP     478    GET /wireshark-labs/INTRO
-wireshark-file1.html HTTP/1.1

Frame 188: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
Ethernet II, Src: IntelCor 0b:f5:63 (88:53:2e:0b:f5:63), Dst: CiscoCon f9:3c:61 (c8:d7:19:f9:3c:61)
Internet Protocol Version 4, Src: 192.168.1.137 (192.168.1.137), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 57993 (57993), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 424
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
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85 Safar
  i/537.36\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: en-US,en;q=0.8,de;q=0.6\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: 190]
```

2. **Packet print of OK Reply:**

```
No.     Time               Source                Destination           Protocol Length Info
    190 14:59:47.436057000 128.119.245.12        192.168.1.137         HTTP     494    HTTP/1.1 200 OK  (text/ht
ml)

Frame 190: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0
Ethernet II, Src: CiscoCon f9:3c:61 (c8:d7:19:f9:3c:61), Dst: IntelCor 0b:f5:63 (88:53:2e:0b:f5:63)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.137 (192.168.1.137)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 57993 (57993), Seq: 1, Ack: 425, Len: 440
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 11 Sep 2015 18:59:08 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
  Last-Modified: Fri, 11 Sep 2015 05:59:01 GMT\r\n
  ETag: "51-51f726991b1de"\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: 0.023152000 seconds]
  [Request in frame: 188]
Line-based text data: text/html
  <html>\n
  Congratulations!  You've downloaded the first Wireshark lab file!\n
  </html>\n
```