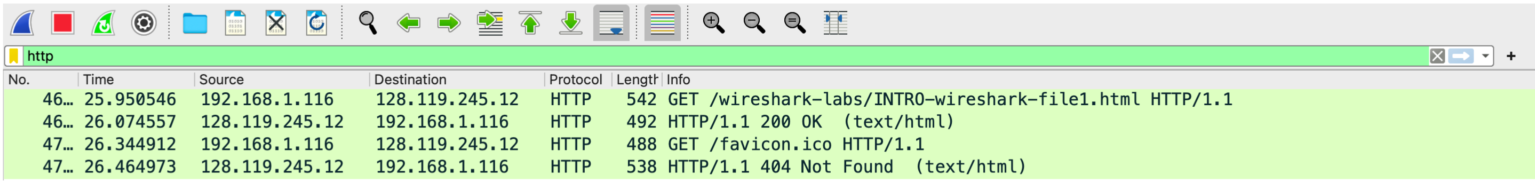
Author Ruben Ortega

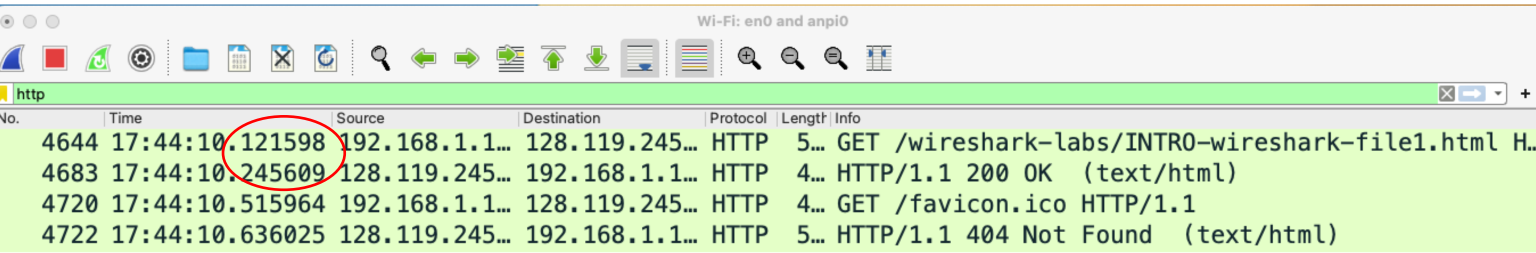
Screen shot of Wireshark after clicking the link to umass



```
http
No.     Time        Source          Destination     Protocol  Length  Info
  46…   25.950546   192.168.1.116   128.119.245.12  HTTP      542  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  46…   26.074557   128.119.245.12  192.168.1.116   HTTP      492  HTTP/1.1 200 OK  (text/html)
  47…   26.344912   192.168.1.116   128.119.245.12  HTTP      488  GET /favicon.ico HTTP/1.1
  47…   26.464973   128.119.245.12  192.168.1.116   HTTP      538  HTTP/1.1 404 Not Found  (text/html)
```

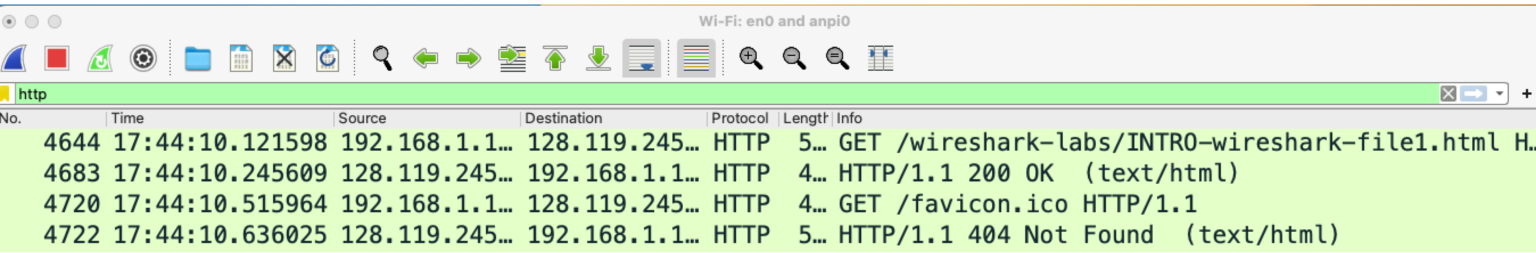
1. The protocols that are shown in the trace file are just HTTP. Since we were instructed to filter HTTP in the previous step. If it wasn't filtered I saw all the protocols listed.

2. The delay was .124011 seconds 17:44:10.245609 - 17:44:10.121598

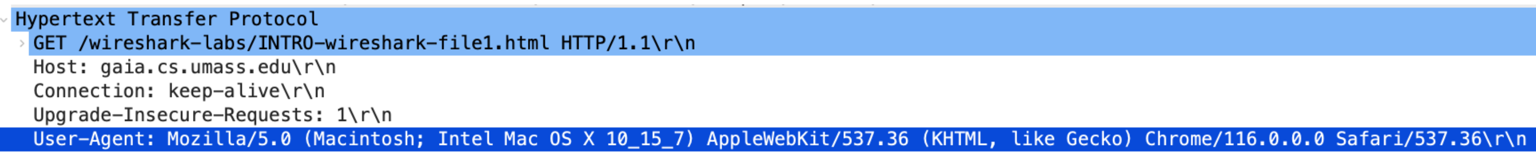


```
Wi-Fi: en0 and anpi0
http
No.   Time             Source       Destination  Protocol  Length  Info
 4644 17:44:10.121598 192.168.1.1… 128.119.245… HTTP  5… GET /wireshark-labs/INTRO-wireshark-file1.html H…
 4683 17:44:10.245609 128.119.245… 192.168.1.1… HTTP  4… HTTP/1.1 200 OK  (text/html)
 4720 17:44:10.515964 192.168.1.1… 128.119.245… HTTP  4… GET /favicon.ico HTTP/1.1
 4722 17:44:10.636025 128.119.245… 192.168.1.1… HTTP  5… HTTP/1.1 404 Not Found  (text/html)
```

3. The internet address of gaia.cs.umass.edu is 128.119.245.12 and the internet address of my computer is 192.168.1.116



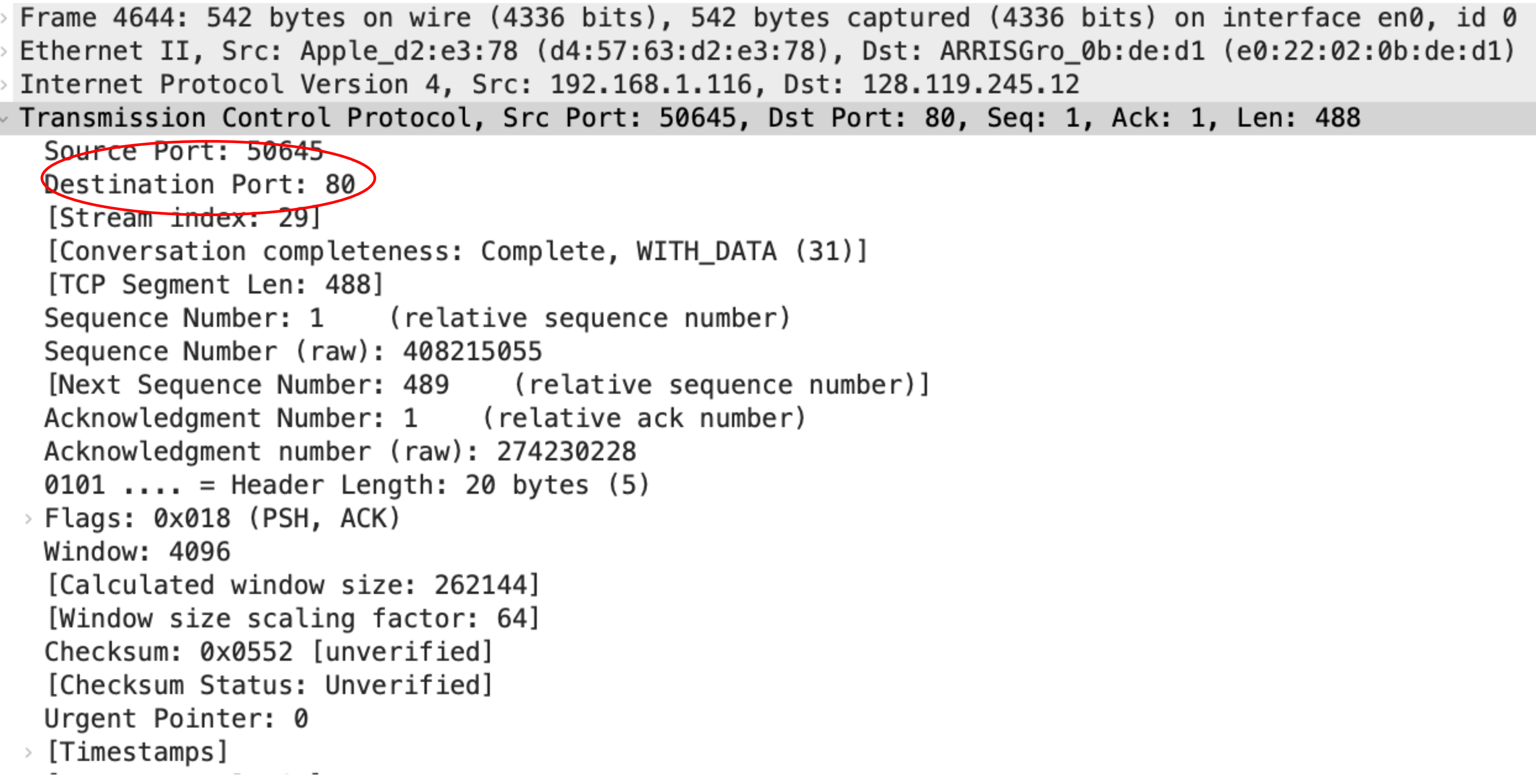
```
Wi-Fi: en0 and anpi0
http
No.   Time             Source       Destination  Protocol  Length  Info
 4644 17:44:10.121598 192.168.1.1… 128.119.245… HTTP  5… GET /wireshark-labs/INTRO-wireshark-file1.html H…
 4683 17:44:10.245609 128.119.245… 192.168.1.1… HTTP  4… HTTP/1.1 200 OK  (text/html)
 4720 17:44:10.515964 192.168.1.1… 128.119.245… HTTP  4… GET /favicon.ico HTTP/1.1
 4722 17:44:10.636025 128.119.245… 192.168.1.1… HTTP  5… HTTP/1.1 404 Not Found  (text/html)
```



```
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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36\r\n
```

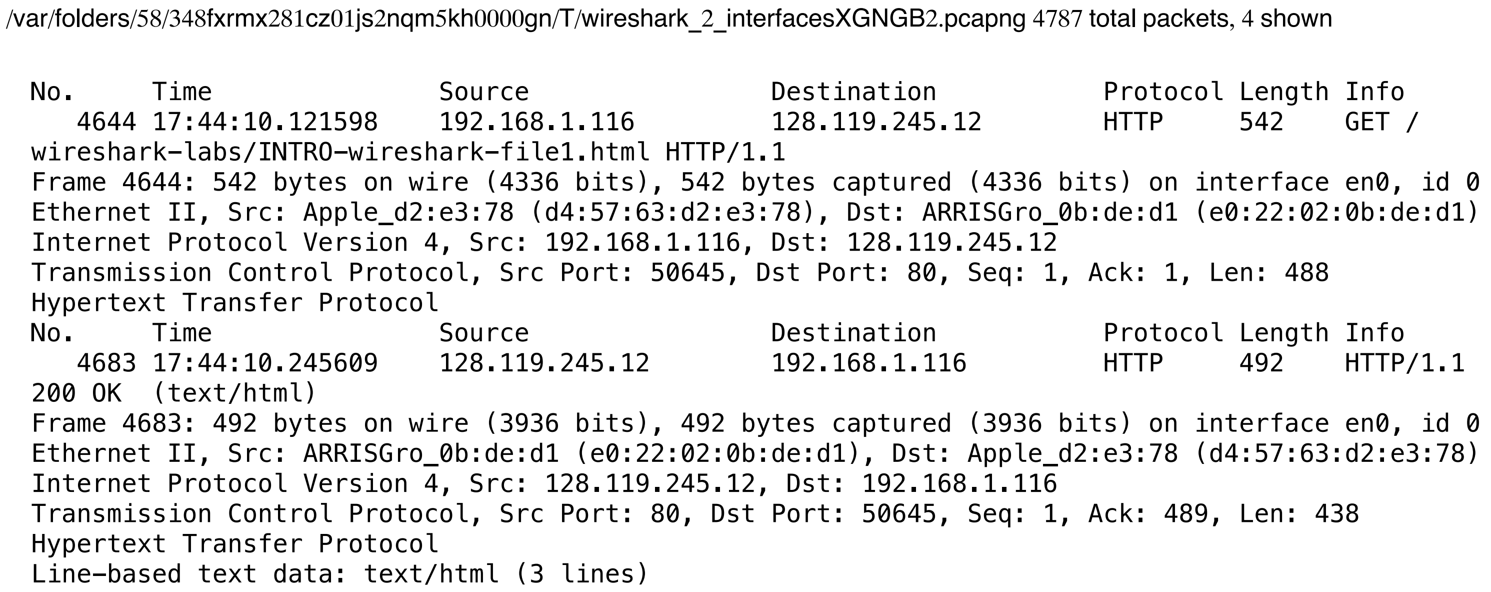
4. The browser that issued the request is built with software components of Mozilla and Apple's Webkit and that is Google Chrome.

5. The destination port is port 80



```
Frame 4644: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface en0, id 0
Ethernet II, Src: Apple_d2:e3:78 (d4:57:63:d2:e3:78), Dst: ARRISGro_0b:de:d1 (e0:22:02:0b:de:d1)
Internet Protocol Version 4, Src: 192.168.1.116, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50645, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
  Source Port: 50645
  Destination Port: 80
  [Stream index: 29]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 488]
  Sequence Number: 1    (relative sequence number)
  Sequence Number (raw): 408215055
  [Next Sequence Number: 489    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 274230228
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 4096
  [Calculated window size: 262144]
  [Window size scaling factor: 64]
  Checksum: 0x0552 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
```

6. Print the two HTTP messages (GET and OK)



/var/folders/58/348fxrmx281cz01js2nqm5kh0000gn/T/wireshark_2_interfacesXGNGB2.pcapng 4787 total packets, 4 shown

```
No.     Time               Source                Destination           Protocol Length Info
   4644 17:44:10.121598    192.168.1.116         128.119.245.12        HTTP     542    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 4644: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface en0, id 0
Ethernet II, Src: Apple_d2:e3:78 (d4:57:63:d2:e3:78), Dst: ARRISGro_0b:de:d1 (e0:22:02:0b:de:d1)
Internet Protocol Version 4, Src: 192.168.1.116, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50645, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
   4683 17:44:10.245609    128.119.245.12        192.168.1.116         HTTP     492    HTTP/1.1
200 OK  (text/html)
Frame 4683: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0
Ethernet II, Src: ARRISGro_0b:de:d1 (e0:22:02:0b:de:d1), Dst: Apple_d2:e3:78 (d4:57:63:d2:e3:78)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.116
Transmission Control Protocol, Src Port: 80, Dst Port: 50645, Seq: 1, Ack: 489, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```