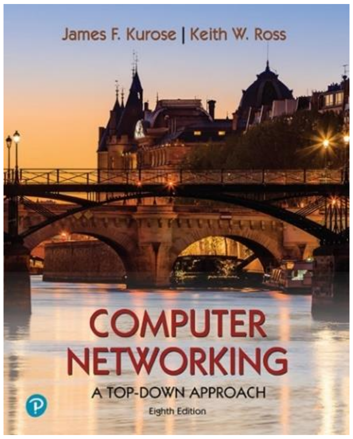
Wireshark Lab: Getting Started v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

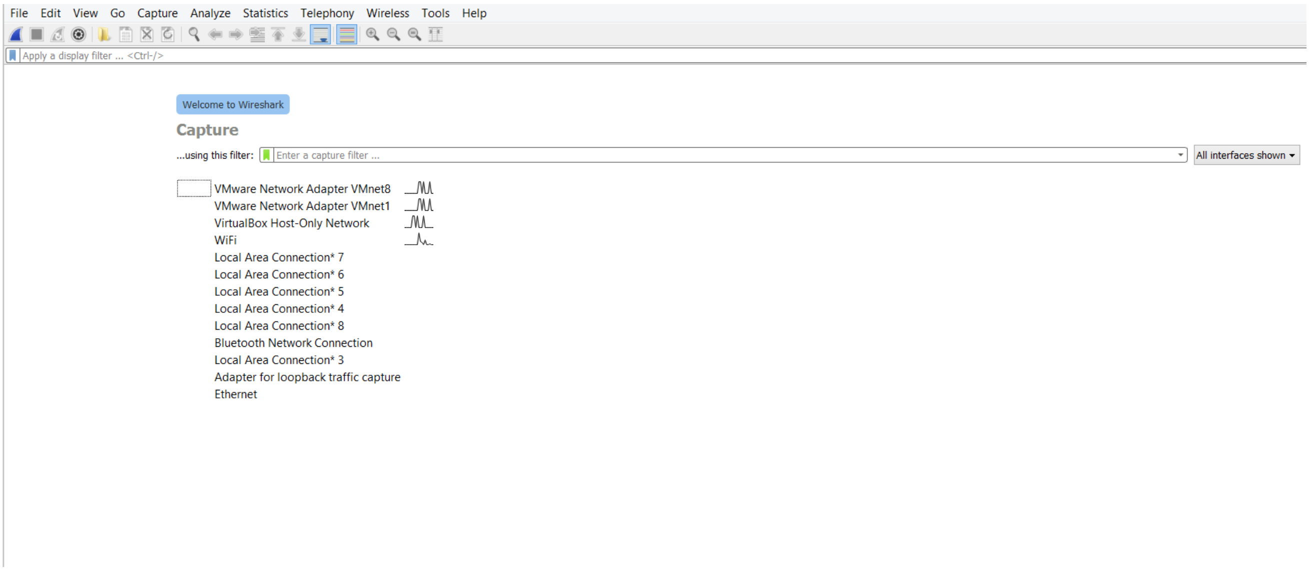
"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



Contents

What is Wireshark?

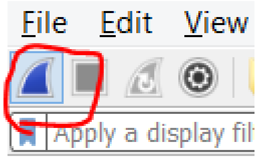
- Wireshark is a network **packet analyzer (packet sniffer)**. A network packet analyzer presents captured packet data in as much detail as possible.
- A packet sniffer program has two main components:
  - **Packet analyzer** displays the contents of all fields within a protocol message.
  - **Packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer over a given interface.
- When you open Wireshark, you will get a list of interfaces.

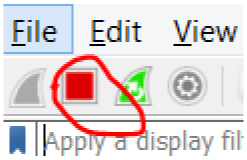

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown

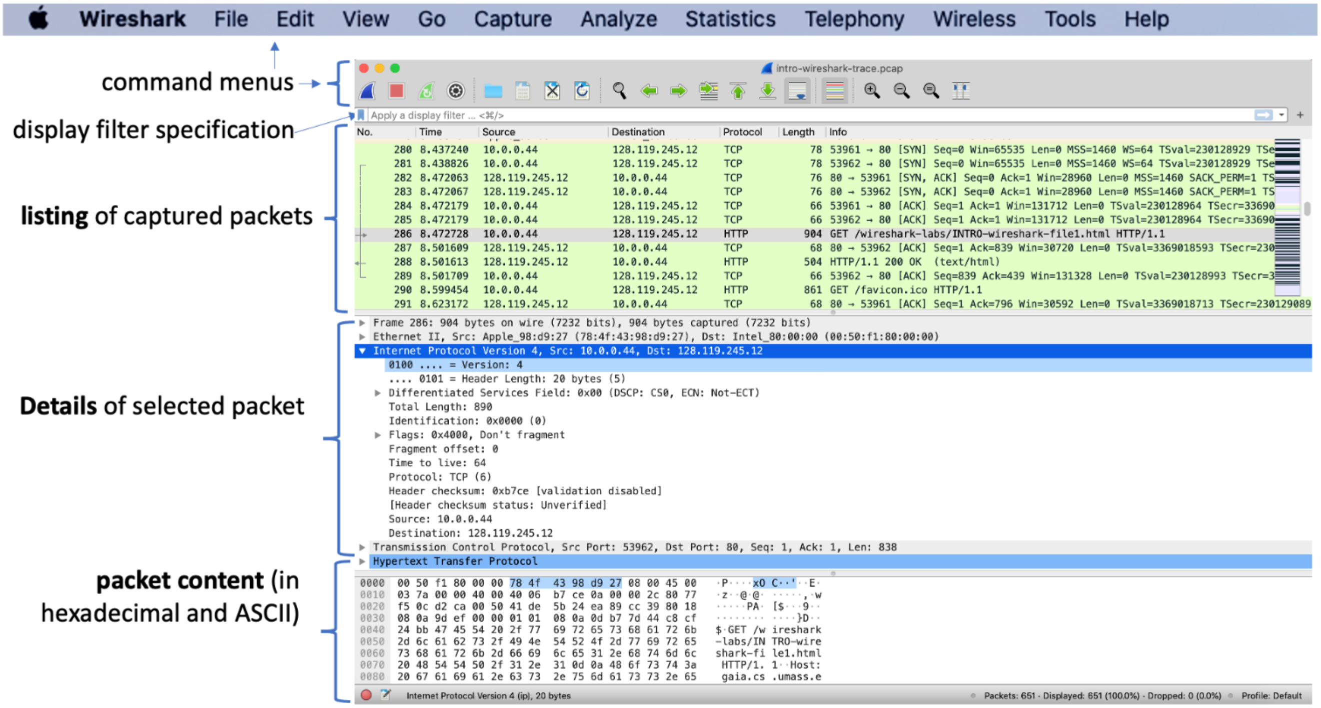
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
WiFi
Local Area Connection* 7
Local Area Connection* 6
Local Area Connection* 5
Local Area Connection* 4
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 3
Adapter for loopback traffic capture
Ethernet

Wireshark Interface

- Select the appropriate interface (WiFi or Ethernet).
- Double click on the interface or press on the start capturing button.
- You can stop capturing packets by clicking on the stop button.
- A screen like the one below will be displayed, showing information about the packets being captured.






Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
command menus
display filter specification
listing of captured packets
Details of selected packet
packet content (in hexadecimal and ASCII)
intro-wireshark-trace.pcap
Apply a display filter ... <⌘/>

```
No.   Time      Source          Destination     Protocol Length Info
  280 8.437240  10.0.0.44       128.119.245.12  TCP        78 53961 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=230128929 TSe
  281 8.438826  10.0.0.44       128.119.245.12  TCP        78 53962 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=230128929 TSe
  282 8.472063  128.119.245.12  10.0.0.44       TCP        76 80 → 53961 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
  283 8.472067  128.119.245.12  10.0.0.44       TCP        76 80 → 53962 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
  284 8.472179  10.0.0.44       128.119.245.12  TCP        66 53961 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=230128964 TSecr=33690
  285 8.472179  10.0.0.44       128.119.245.12  TCP        66 53962 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=230128964 TSecr=33690
  286 8.472728  10.0.0.44       128.119.245.12  HTTP      904 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  287 8.501609  128.119.245.12  10.0.0.44       TCP        68 80 → 53962 [ACK] Seq=1 Ack=839 Win=30720 Len=0 TSval=3369018593 TSecr=230
  288 8.501613  128.119.245.12  10.0.0.44       HTTP      504 HTTP/1.1 200 OK  (text/html)
  289 8.501709  10.0.0.44       128.119.245.12  TCP        66 53962 → 80 [ACK] Seq=839 Ack=439 Win=131328 Len=0 TSval=230128993 TSecr=3
  290 8.599454  10.0.0.44       128.119.245.12  HTTP      861 GET /favicon.ico HTTP/1.1
  291 8.623172  128.119.245.12  10.0.0.44       TCP        68 80 → 53961 [ACK] Seq=1 Ack=796 Win=30592 Len=0 TSval=3369018713 TSecr=230129089
```

```
▶ Frame 286: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits)
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Intel_80:00:00 (00:50:f1:80:00:00)
▼ Internet Protocol Version 4, Src: 10.0.0.44, 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: 890
    Identification: 0x0000 (0)
  ▶ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xb7ce [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.44
    Destination: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 53962, Dst Port: 80, Seq: 1, Ack: 1, Len: 838
▶ Hypertext Transfer Protocol
```

```
0000  00 50 f1 80 00 00 78 4f  43 98 d9 27 08 00 45 00   ·P····xO C··'··E·
0010  03 7a 00 00 40 00 40 06  b7 ce 0a 00 00 2c 80 77   ·z··@·@· ·····,·w
0020  f5 0c d2 ca 00 50 41 de  5b 24 ea 89 cc 39 80 18   ·····PA· [$···9··
0030  08 0a 9d ef 00 00 01 01  08 0a 0d b7 7d 44 c8 cf   ········ ····}D··
0040  24 bb 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   $·GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
```

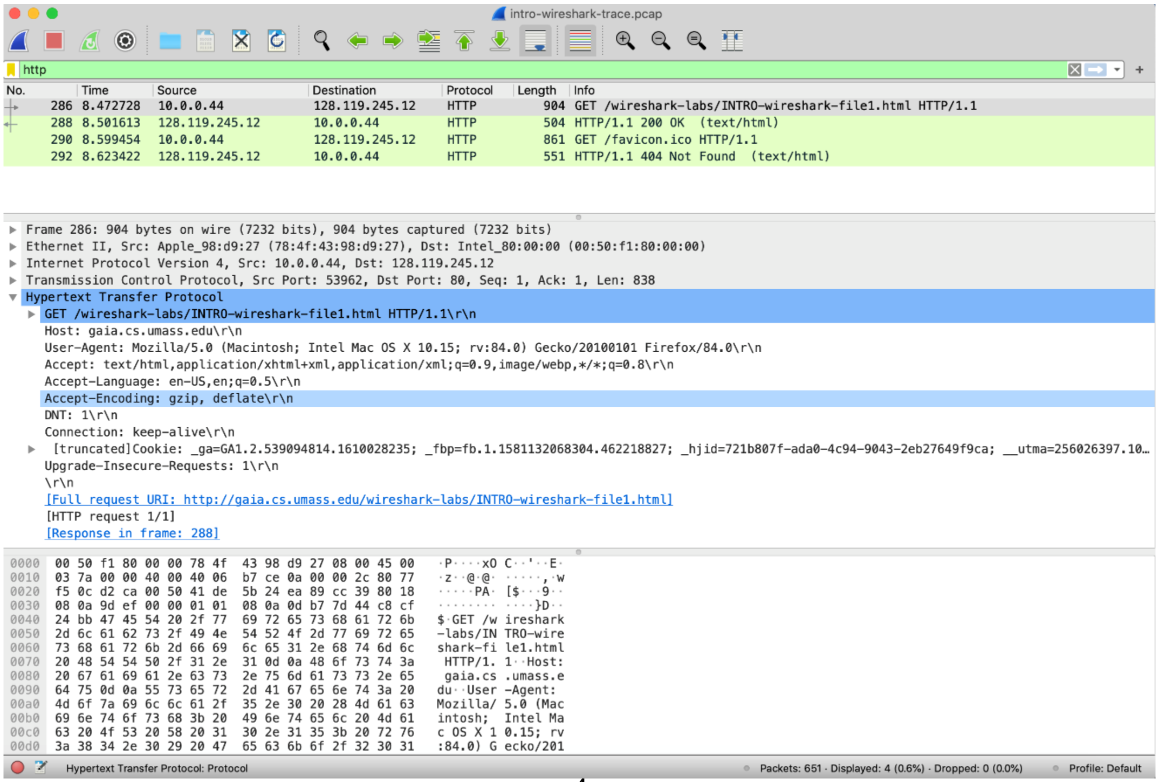
Internet Protocol Version 4 (ip), 20 bytes   Packets: 651 · Displayed: 651 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

- The **command menus** are standard pulldown menus located at the top of the Wireshark window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data and exit the Wireshark application. The Capture menu allows you to begin packet capture.
- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; note that this is not a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
- The **packet-header details** window provides details about the packet selected (highlighted) in the packet-listing window. These details include information about the Ethernet frame and IP datagram that contains this packet.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

- Towards the top of the Wireshark graphical user interface, is the **packet display filter** field, into which a protocol name or other information can be entered to filter the information displayed in the packet-listing window.

Running Wireshark

1. Start Wireshark.
2. Select the appropriate interface.
3. Start packet capturing.
4. Open the web browser, go to http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
5. Stop packet capturing.
6. Wireshark now has packet data that contains all protocol messages exchanged between your computer and other network entities.
    a. The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well.
7. Type in “http” into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”) or just hit Enter.
    a. This will cause only HTTP messages to be displayed in the packet-listing window.



http

```
No.    Time      Source          Destination     Protocol  Length  Info
   286 8.472728  10.0.0.44       128.119.245.12  HTTP         904  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   288 8.501613  128.119.245.12  10.0.0.44       HTTP         504  HTTP/1.1 200 OK  (text/html)
   290 8.599454  10.0.0.44       128.119.245.12  HTTP         861  GET /favicon.ico HTTP/1.1
   292 8.623422  128.119.245.12  10.0.0.44       HTTP         551  HTTP/1.1 404 Not Found  (text/html)
```

```
▶ Frame 286: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits)
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Intel_80:00:00 (00:50:f1:80:00:00)
▶ Internet Protocol Version 4, Src: 10.0.0.44, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 53962, Dst Port: 80, Seq: 1, Ack: 1, Len: 838
▼ 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 (Macintosh; Intel Mac OS X 10.15; rv:84.0) Gecko/20100101 Firefox/84.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
  ▶  [truncated]Cookie: _ga=GA1.2.539094814.1610028235; _fbp=fb.1.1581132068304.462218827; _hjid=721b807f-ada0-4c94-9043-2eb27649f9ca; __utma=256026397.10…
    Upgrade-Insecure-Requests: 1\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: 288]
```

```
0000  00 50 f1 80 00 00 78 4f  43 98 d9 27 08 00 45 00   ·P····xO C··'··E·
0010  03 7a 00 00 40 00 40 06  b7 ce 0a 00 00 2c 80 77   ·z··@·@· ·····,·w
0020  f5 0c d2 ca 00 50 41 de  5b 24 ea 89 cc 39 80 18   ·····PA· [$···9··
0030  08 0a 9d ef 00 00 01 01  08 0a 0d b7 7d 44 c8 cf   ········ ····}D··
0040  24 bb 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   $·GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
0090  64 75 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   du··User -Agent: 
00a0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 4d 61 63   Mozilla/ 5.0 (Mac
00b0  69 6e 74 6f 73 68 3b 20  49 6e 74 65 6c 20 4d 61   intosh;  Intel Ma
00c0  63 20 4f 53 20 58 20 31  30 2e 31 35 3b 20 72 76   c OS X 1 0.15; rv
00d0  3a 38 34 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   :84.0) G ecko/201
```

Hypertext Transfer Protocol: Protocol

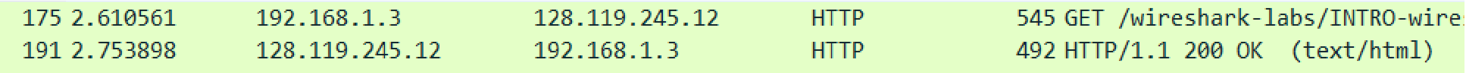
Packets: 651 · Displayed: 4 (0.6%) · Dropped: 0 (0.0%)

Profile: Default

8. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server.
   a. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window.

Exercises

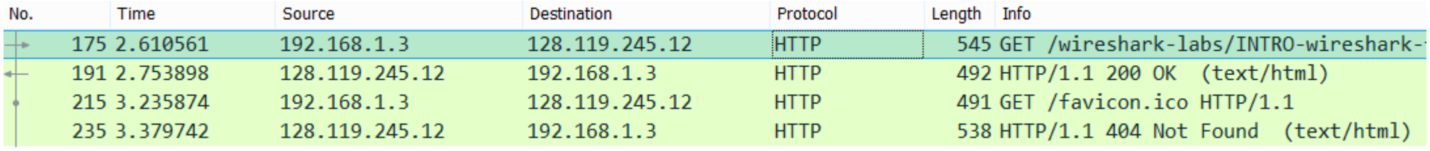
1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?



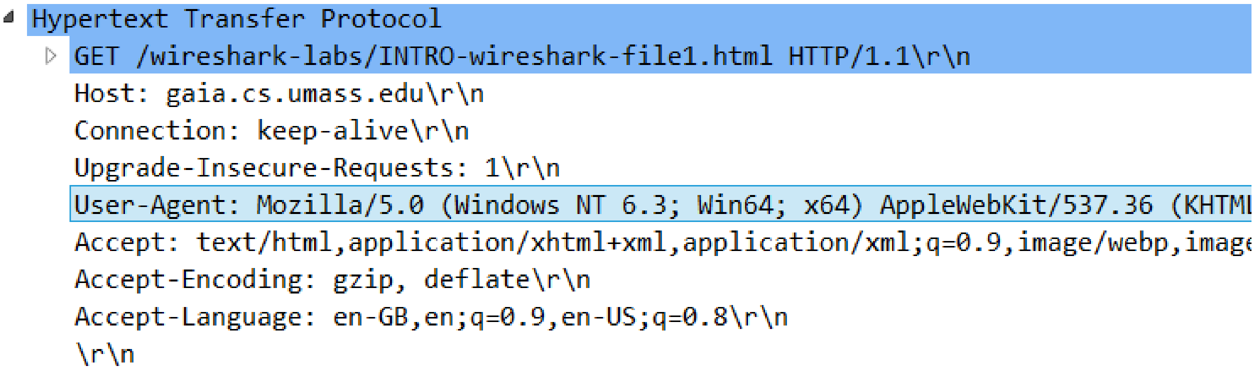
```
175 2.610561    192.168.1.3       128.119.245.12    HTTP     545 GET /wireshark-labs/INTRO-wire
191 2.753898    128.119.245.12    192.168.1.3       HTTP     492 HTTP/1.1 200 OK  (text/html)
```

It is 2.75 – 2.61 ≈ 0.1 seconds

2. What is the Internet address of the gaia.cs.umass.edu What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?
   gaia.cs.umass.edu → 128.119.245.12
   my computer → 192.168.1.3
3. What type of Web browser issued the HTTP request?



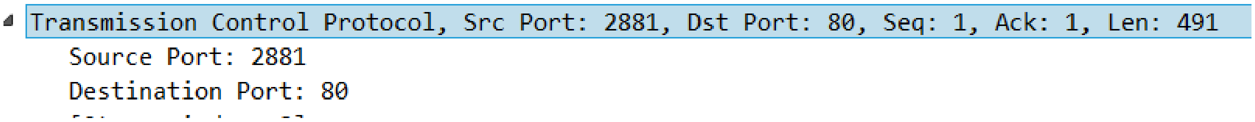
```
No.   Time          Source           Destination       Protocol   Length  Info
  175 2.610561      192.168.1.3      128.119.245.12    HTTP         545 GET /wireshark-labs/INTRO-wireshark-
  191 2.753898      128.119.245.12   192.168.1.3       HTTP         492 HTTP/1.1 200 OK  (text/html)
  215 3.235874      192.168.1.3      128.119.245.12    HTTP         491 GET /favicon.ico HTTP/1.1
  235 3.379742      128.119.245.12   192.168.1.3       HTTP         538 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 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTMl
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9,en-US;q=0.8\r\n
    \r\n
```

Select the "GET" request from the captured packets window
Expand the "hypertext transfer protocol" section
Look for the "user-agent" field
Match the content of the field with the strings in
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent

4. What is the destination port number to which this HTTP request is being sent?



```
◢ Transmission Control Protocol, Src Port: 2881, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
    Source Port: 2881
    Destination Port: 80
```

Select a packet

Select the “Transmission Control Protocol”

The source port is 2881

The destination port is 80