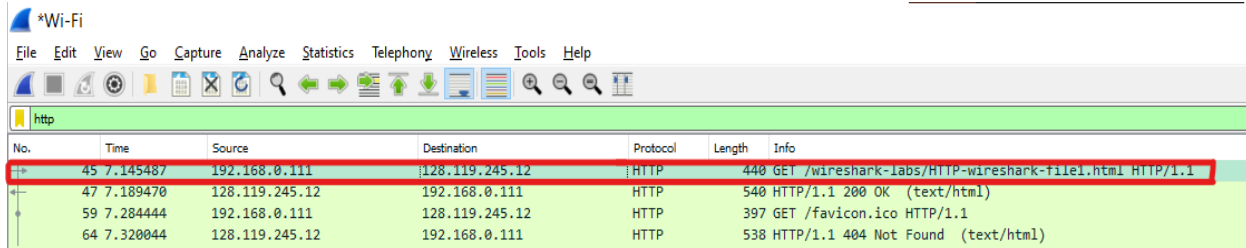


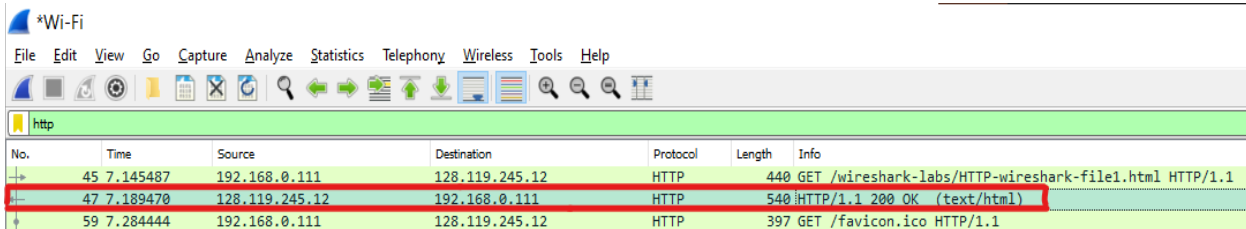
TASK 1 – Explore HTTP

1. What is the IP address of your computer? Of the *gaia.cs.umass.edu* server?
the IP Address of my machine is – 192.168.0.111
the gaia.cs.umass.edu server IP address is – 128.119.245.12



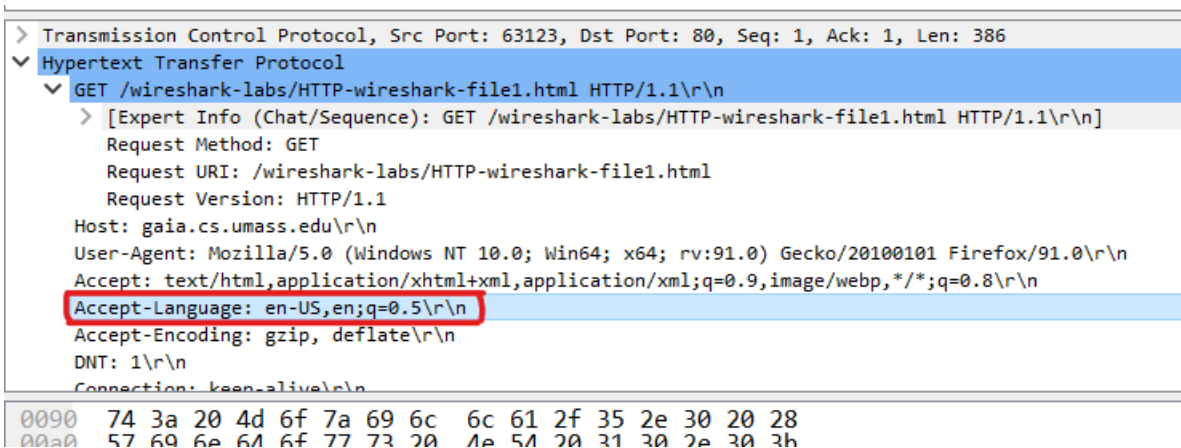
No.	Time	Source	Destination	Protocol	Length	Info
45	7.145487	192.168.0.111	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
47	7.189470	128.119.245.12	192.168.0.111	HTTP	540	HTTP/1.1 200 OK (text/html)
59	7.284444	192.168.0.111	128.119.245.12	HTTP	397	GET /favicon.ico HTTP/1.1
64	7.320444	128.119.245.12	192.168.0.111	HTTP	538	HTTP/1.1 404 Not Found (text/html)

2. What is the status code and phrase returned from the server to your browser?
the server responded to the browser with - 200 OK as status code and phrase



No.	Time	Source	Destination	Protocol	Length	Info
45	7.145487	192.168.0.111	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
47	7.189470	128.119.245.12	192.168.0.111	HTTP	540	HTTP/1.1 200 OK (text/html)
59	7.284444	192.168.0.111	128.119.245.12	HTTP	397	GET /favicon.ico HTTP/1.1

3. What languages does your browser indicate to the server that it can accept? Which header line is used to indicate this information?
my Firefox browser indicates that it will accept en-US (English-US) and en (English) language from the server

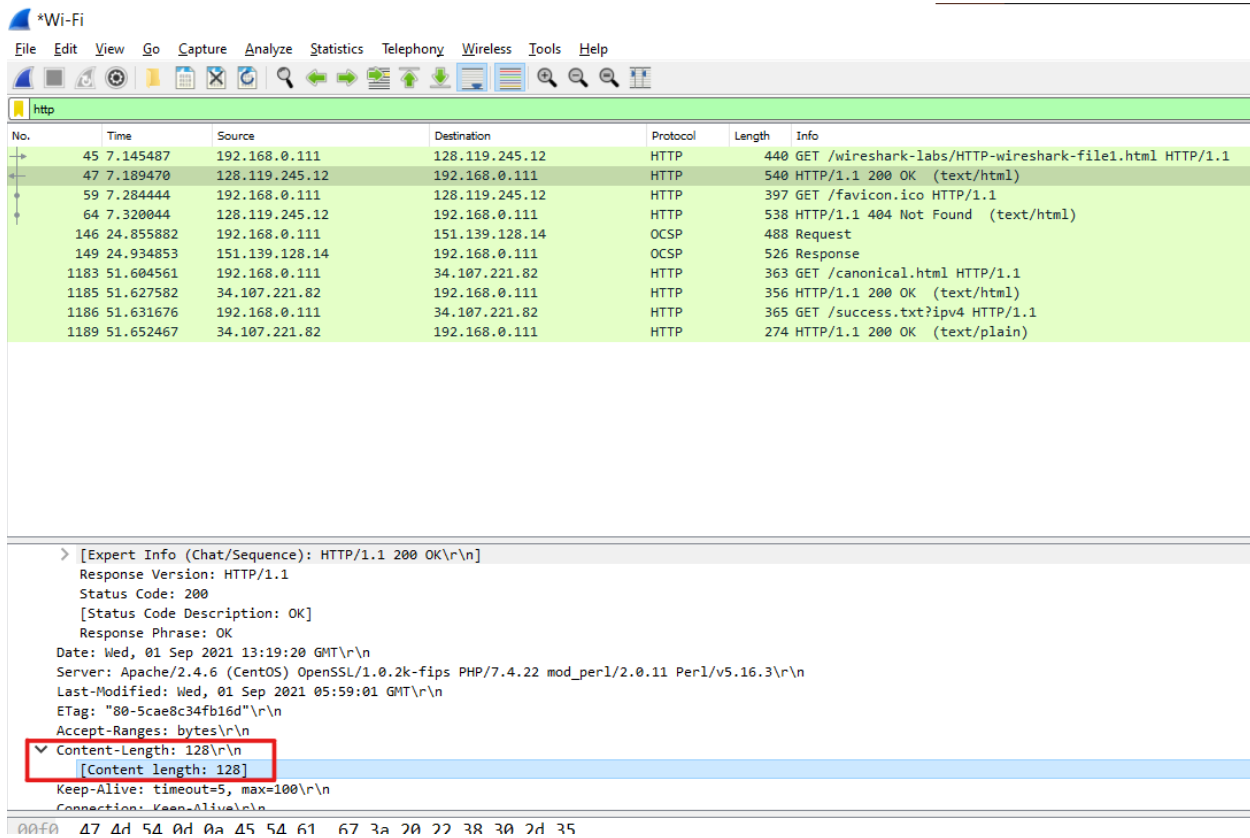


> Transmission Control Protocol, Src Port: 63123, Dst Port: 80, Seq: 1, Ack: 1, Len: 386	
▼ Hypertext Transfer Protocol	
▼ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n	
> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]	
Request Method: GET	
Request URI: /wireshark-labs/HTTP-wireshark-file1.html	
Request Version: HTTP/1.1	
Host: gaia.cs.umass.edu\r\n	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0\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	

0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
00a0 57 60 6e 6d 6f 77 73 20 1e 5d 20 31 30 2e 30 20

4. How many bytes of content (size of file) are returned to your browser? Which header line is used to indicate this information?

128 bytes of content size are returned to my Firefox browser



Wireshark packet capture showing an HTTP GET request and response. The response packet (No. 47) is selected, and the 'Content-Length: 128' header is highlighted in the packet details pane.

No.	Time	Source	Destination	Protocol	Length	Info
45	7.145487	192.168.0.111	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
47	7.189470	128.119.245.12	192.168.0.111	HTTP	540	HTTP/1.1 200 OK (text/html)
59	7.284444	192.168.0.111	128.119.245.12	HTTP	397	GET /favicon.ico HTTP/1.1
64	7.320044	128.119.245.12	192.168.0.111	HTTP	538	HTTP/1.1 404 Not Found (text/html)
146	24.855882	192.168.0.111	151.139.128.14	OCSP	488	Request
149	24.934853	151.139.128.14	192.168.0.111	OCSP	526	Response
1183	51.604561	192.168.0.111	34.107.221.82	HTTP	363	GET /canonical.html HTTP/1.1
1185	51.627582	34.107.221.82	192.168.0.111	HTTP	356	HTTP/1.1 200 OK (text/html)
1186	51.631676	192.168.0.111	34.107.221.82	HTTP	365	GET /success.txt?ip=4 HTTP/1.1
1189	51.652467	34.107.221.82	192.168.0.111	HTTP	274	HTTP/1.1 200 OK (text/plain)

Packet details for selected packet (No. 47):

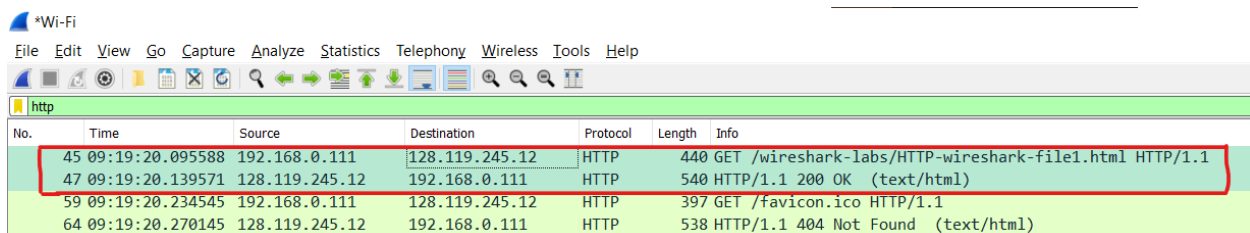
- [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Wed, 01 Sep 2021 13:19:20 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
- Last-Modified: Wed, 01 Sep 2021 05:59:01 GMT\r\n
- Etag: "80-5cae8c34fb16d"\r\n
- Accept-Ranges: bytes\r\n
- Content-Length: 128\r\n
- [Content length: 128]
- Keep-Alive: timeout=5, max=100\r\n
- Connection: Keep-Alive\r\n

5. 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 **43.983ms** from when the HTTP GET message was sent until the HTTP OK reply was received

The result was calculated in (Time Display Format hh-mm-ss)

09:19:20.139571 - 09:19:20.095588

= 0.043983 seconds (43.983 milliseconds)



Wireshark packet capture showing an HTTP GET request and response. The response packet (No. 47) is selected, and the 'Content-Length: 128' header is highlighted in the packet details pane.

No.	Time	Source	Destination	Protocol	Length	Info
45	09:19:20.095588	192.168.0.111	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
47	09:19:20.139571	128.119.245.12	192.168.0.111	HTTP	540	HTTP/1.1 200 OK (text/html)
59	09:19:20.234545	192.168.0.111	128.119.245.12	HTTP	397	GET /favicon.ico HTTP/1.1
64	09:19:20.270145	128.119.245.12	192.168.0.111	HTTP	538	HTTP/1.1 404 Not Found (text/html)

TASK 2 – Capture a traceroute

1. Start a new packet capture in Wireshark.
2. Open a “terminal window” on Mac or Linux, a “Command Prompt” on Windows
3. Use the “tracert” command on Windows to determine path and intermediate devices between your host and yahoo.com. On Linux or Macintosh, the command is “traceroute”. You should see results of the traceroute command in your terminal/command window, as well as in the wireshark packets list. For example:
4. Type “icmp” into the “filter” window and then click the “apply” button to narrow down the types of packets shown in the list.
5. Stop the Wireshark trace. Packets should no longer be collected.
6. Take a screen shot of the wireshark window showing the ICMP packets. Depending on the number of hops between where you are on the Internet and Yahoo, you might not be able to fit all the ICMP packets on the screen. That’s OK, just make the Wireshark window as “tall” as you can, and perhaps uncheck the “packet bytes” and “packet details” sections under the “View” menu. Notice the IP addresses match up to the output from the traceroute command in your terminal window.

traceroute command on windows terminal -

```
C:\windows\system32>tracert yahoo.com
```

```
Tracing route to yahoo.com [2001:4998:44:3507::8001]  
over a maximum of 30 hops:
```

1	19 ms	25 ms	20 ms	ae-20.2231.cr5.blc.net.uits.iu.edu [2001:18e8:2:28b7::2]
2	4 ms	3 ms	2 ms	ae-15.0.br2.blc.net.uits.iu.edu [2001:18e8:3:f016::2]
3	7 ms	7 ms	5 ms	2001:18e8:ff00:90::1
4	15 ms	11 ms	14 ms	2001:18e8:ffff:7::4
5	13 ms	13 ms	10 ms	2001:18e8:ffff:11::2
6	13 ms	9 ms	10 ms	r-equinix-isp-ae0-2274.wiscnet.net [2001:4e0:0:21c::219]
7	*	*	*	Request timed out.
8	26 ms	38 ms	20 ms	ae-0.pat2.nez.yahoo.com [2001:4998:f000:200::]
9	27 ms	24 ms	24 ms	et-1-0-0.msrl.ne1.yahoo.com [2001:4998:f000:207::1]
10	22 ms	19 ms	20 ms	et-1-1-0.clr2-a-gdc.ne1.yahoo.com [2001:4998:44:fe1d::1]
11	25 ms	21 ms	22 ms	2001:4998:44:f823::1
12	24 ms	23 ms	328 ms	et28.usw1-1-lbd.ne1.yahoo.com [2001:4998:44:c226::1]
13	24 ms	24 ms	23 ms	media-router-fp74.prod.media.vip.ne1.yahoo.com [2001:4998:44:3507::8001]

```
Trace complete.
```

traceroute command on windows terminal (screenshot) -

```
Administrator: Command Prompt
ms 9.232 ms

C:\windows\system32>tracert yahoo.com

Tracing route to yahoo.com [2001:4998:44:3507::8001]
over a maximum of 30 hops:
 0  0 ms  0 ms  ae-8.pat1.bfz.yahoo.com (216.115.101.231)  21.313 ms
 1  11 ms  19 ms  25 ms  ae-20.2231.cr5.blc.net.uits.iu.edu [2001:18e8:2:28b7::2]
 2  12 ms  4 ms  813 ms  3 ms  25 ms  ae-15.0.br2.blc.net.uits.iu.edu [2001:18e8:3:f016::2]
 3  3 ms  7 ms  35 ms  5 ms  2001:18e8:ff00:90::1
 4  15 ms  11 ms  14 ms  2001:18e8:ffff:7::4
 5  13 ms  13 ms  10 ms  2001:18e8:ffff:11::2
 6  13 ms  9 ms  10 ms  r-equinix-isp-ae0-2274.wiscnet.net [2001:4e0:0:21c::219]
 7  * * * Request timed out.
 8  26 ms  38 ms  20 ms  ae-0.pat2.nez.yahoo.com [2001:4998:f000:200::]
 9  27 ms  24 ms  24 ms  et-1-0-0.msrl.ne1.yahoo.com [2001:4998:f000:207::1]
10  22 ms  19 ms  24 ms  et-1-1-0.clr2-a-gdc.ne1.yahoo.com [2001:4998:44:fe1d::1]
11  25 ms  21 ms  22 ms  2001:4998:44:f823::1
12  24 ms  23 ms  328 ms  et28.usw1-1-lbd.ne1.yahoo.com [2001:4998:44:c226::1]
13  24 ms  24 ms  23 ms  media-router-fp74.prod.media.vip.ne1.yahoo.com [2001:4998:44:3507::8001]

Trace complete.
```

icmpv6 filter for capturing traceroute command using Wireshark -

