

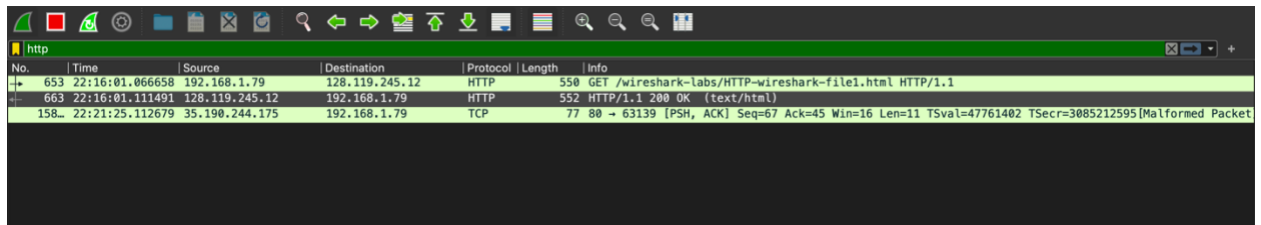
Name: VINAYAKA GADAG

Email: vgadag@iu.edu

TASK-1

1. What is the IP address of your computer? Of the *gaia.cs.umass.edu* server?

- IP address of computer – 192.168.1.79
- Server IP address – 128.119.245.12



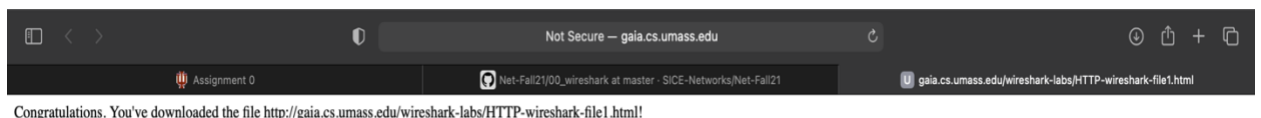
The image shows a Wireshark packet capture window. The top bar is green and labeled 'http'. The packet list on the left shows three packets. The first packet is selected, showing details in the right pane. The details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
653	22:16:01.066658	192.168.1.79	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
663	22:16:01.111491	128.119.245.12	192.168.1.79	HTTP	552	HTTP/1.1 200 OK (text/html)
158...	22:21:25.112679	35.190.244.175	192.168.1.79	TCP	77	80 → 63139 [PSH, ACK] Seq=67 Ack=45 Win=16 Len=11 TSval=47761402 TSecr=3085212595 [Malformed Packet]

2. What is the status code and phrase returned from the server to your browser?

- Status Code - HTTP/1.1 200 OK
- Phrase - Congratulations. You've downloaded the file
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!>
- Response Phrase: OK

Protocol	Length	Info
HTTP	550	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
HTTP	552	HTTP/1.1 200 OK (text/html)



3. What languages does your browser indicate to the server that it can accept?
Which header line is used to indicate this information?

- Language - en-US,en;q=0.9
- Header-line – Accept-language

```
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
If-Modified-Since: Fri, 27 Aug 2021 05:59:01 GMT\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15
Accept-Language: en-us\r\n
```

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

- Content length - 128 bytes
- Header line – Content-Length
- Folder Data – 128 bytes

```
Content-Length: 128\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: 0.044833000 seconds]
[Request in frame: 653]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

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.)

- Time taken - 0.0448 seconds

```
[HTTP response 1/1]
[Time since request: 0.044833000 seconds]
```

TASK-2

1. 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.

No.	Time	Source	Destination	Protocol	Length	Info
36	22:54:01.666100	192.168.1.254	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
41	22:54:01.679362	192.168.1.254	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
43	22:54:01.683846	192.168.1.254	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
45	22:54:01.689291	45.16.200.1	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
47	22:54:01.695396	45.16.200.1	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
49	22:54:01.700514	45.16.200.1	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
51	22:54:01.708502	71.152.199.226	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
55	22:54:01.721652	71.152.199.226	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
57	22:54:01.728962	71.152.199.226	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
133	22:54:04.373528	192.168.1.79	192.168.1.254	ICMP	70	Destination unreachable (Port unreachable)
266	22:54:11.743849	75.19.192.70	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
273	22:54:11.951308	12.83.79.17	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
275	22:54:11.962469	12.83.79.1	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
277	22:54:11.975144	12.83.79.17	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
279	22:54:11.990812	12.122.132.197	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
281	22:54:12.010332	12.122.132.197	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
283	22:54:12.026545	12.122.132.197	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
285	22:54:12.040362	213.248.87.253	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
287	22:54:12.055339	213.248.87.253	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
289	22:54:12.070230	213.248.87.253	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
296	22:54:12.084365	62.115.122.194	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
299	22:54:12.098385	62.115.122.194	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
303	22:54:12.111593	62.115.122.194	192.168.1.79	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
307	22:54:12.127217	62.115.61.126	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
309	22:54:12.142412	62.115.61.126	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
311	22:54:12.155977	62.115.61.126	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
313	22:54:12.183677	209.191.64.214	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
317	22:54:12.171463	209.191.64.212	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
331	22:54:12.680714	209.191.64.212	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
333	22:54:12.719315	216.115.105.25	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
339	22:54:12.821052	216.115.105.31	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
343	22:54:12.910096	216.115.105.29	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
372	22:54:13.029561	98.138.97.63	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
375	22:54:13.072842	98.138.97.71	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
381	22:54:13.117350	98.138.97.73	192.168.1.79	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
384	22:54:13.159643	98.138.51.0	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
389	22:54:13.228903	98.138.51.5	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
402	22:54:13.495480	98.138.51.3	192.168.1.79	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)

```

1. > traceroute yahoo.com
2. traceroute: Warning: yahoo.com has multiple addresses; using 74.6.231.21
3. traceroute to yahoo.com (74.6.231.21), 64 hops max, 52 byte packets
4.  1  dsldevice (192.168.1.254)  4.029 ms  3.937 ms  3.573 ms
5.  2  45-16-200-1.lightspeed.iplsin.sbcglobal.net (45.16.200.1)  4.602 ms  4.350 ms  4.382 ms
6.  3  71.152.199.226 (71.152.199.226)  7.251 ms  7.482 ms  7.054 ms
7.  4  * * *
8.  5  * 12.83.79.17 (12.83.79.17)  19.542 ms
9.  12.83.79.1 (12.83.79.1)  8.782 ms
10. 6  cgcil402igs.ip.att.net (12.122.132.197)  15.990 ms  13.481 ms  16.429 ms
11. 7  chi-b2-link.ip.twelve99.net (213.248.87.253)  13.237 ms  14.027 ms  13.371 ms
12. 8  chi-b23-link.ip.twelve99.net (62.115.122.194)  12.861 ms  12.910 ms  13.735 ms
13. 9  yahoo-ic314777-chi-b23.ip.twelve99-cust.net (62.115.61.126)  13.186 ms  13.862 ms
14. 266 ms
14. 10 ae-7.pat2.nez.yahoo.com (209.191.64.214)  27.765 ms
15. ae-5.pat1.nez.yahoo.com (209.191.64.212)  48.547 ms  39.677 ms
16. 11 et-0-0-0.msr2.ne1.yahoo.com (216.115.105.179)  40.666 ms  39.379 ms
17. et-18-1-0.msr1.ne1.yahoo.com (216.115.105.31)  26.985 ms
18. 12 et-1-0-0.clr2-a-gdc.ne1.yahoo.com (98.138.97.73)  41.330 ms
19. et-0-0-0.clr1-a-gdc.ne1.yahoo.com (98.138.97.61)  25.543 ms
20. et-1-1-0.clr1-a-gdc.ne1.yahoo.com (98.138.97.63)  38.681 ms
21. 13 lo0.fab2-2-gdc.ne1.yahoo.com (98.138.51.1)  54.203 ms
22. lo0.fab6-2-gdc.ne1.yahoo.com (98.138.51.5)  25.999 ms
23. lo0.fab5-2-gdc.ne1.yahoo.com (98.138.51.4)  25.957 ms
24. 14 usw2-1-lbd.ne1.yahoo.com (98.138.97.157)  23.631 ms
25. usw1-1-lbd.ne1.yahoo.com (98.138.97.156)  68.687 ms  23.993 ms

```

26.	15	media-router-fp74.prod.media.vip.ne1.yahoo.com (74.6.231.21)	40.851 ms	38.086 ms
27.			40.438 ms	