

Izaan Mohtashim

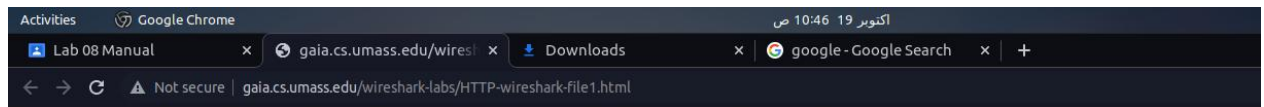
P20-0613

Sec 5A

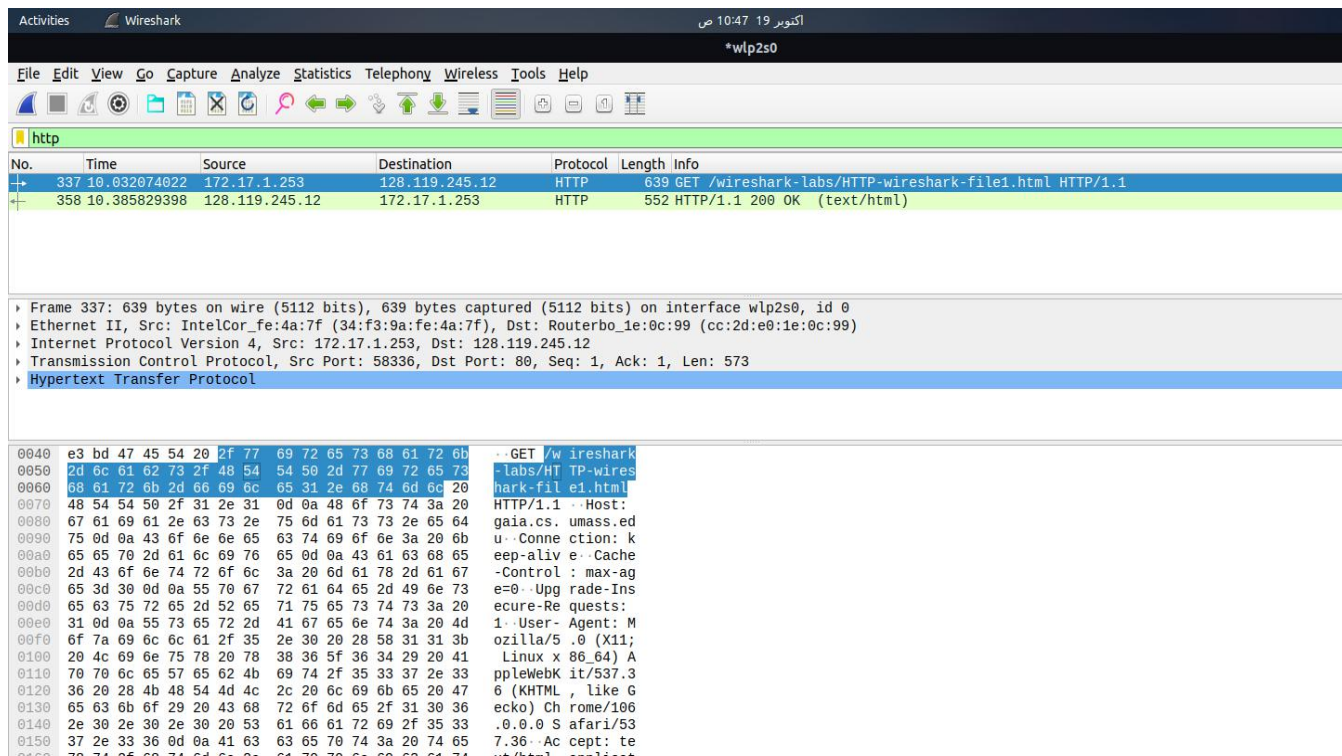
Computer Networks

Lab Task8

Task 1



Congratulations. You've downloaded the file <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>!



Task 2

1. Is your browser running HTTP version 1.0, 1.1, or 2?

Yes it is running 1.1

The screenshot shows a Wireshark capture of an HTTP response. The packet list shows a GET request from 128.119.245.12 to 172.17.1.253. The packet details pane shows the response is HTTP/1.1 200 OK. The response headers include: Date: Wed, 19 Oct 2022 05:38:11 GMT, Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3, Last-Modified: Wed, 19 Oct 2022 05:38:02 GMT, ETag: "80-5eb5c9cb2eb2e", Accept-Ranges: bytes, Content-Length: 128, Keep-Alive: timeout=5, max=100, Connection: Keep-Alive, Content-Type: text/html; charset=UTF-8.

2. What version of HTTP is the server running?

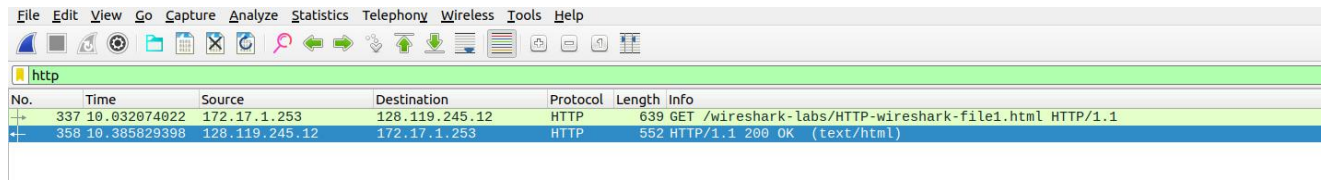
The screenshot shows the packet details pane for the HTTP response. It indicates the response is HTTP/1.1 200 OK. The status code is 200, and the status code description is OK. The response phrase is OK.

3. What languages (if any) does your browser indicate that it can accept to the server?

The screenshot shows the packet details pane for the browser's request. The Accept-Language header is set to en-US;q=0.9. The full request URI is http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html.

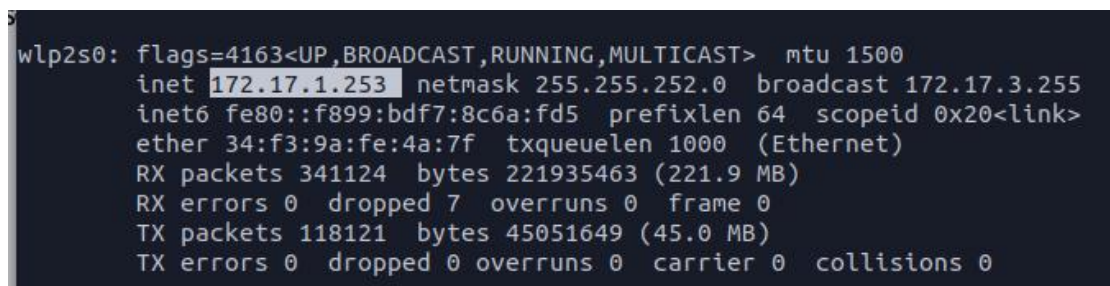
4. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?

compterip-> 172.17.1.253
gaia.cs.umass.edu server-> 128.119.245.12



The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first packet is an HTTP GET request from 172.17.1.253 to 128.119.245.12. The second packet is the corresponding HTTP 200 OK response from 128.119.245.12 to 172.17.1.253.

No.	Time	Source	Destination	Protocol	Length	Info
337	10.032074022	172.17.1.253	128.119.245.12	HTTP	639	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
358	10.385829398	128.119.245.12	172.17.1.253	HTTP	552	HTTP/1.1 200 OK (text/html)

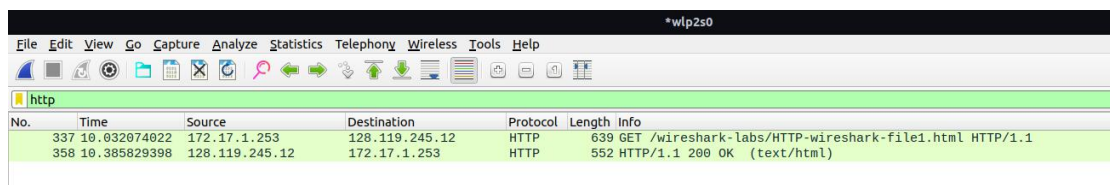


The image shows a terminal window displaying the output of the 'ifconfig' command for the wlp2s0 interface. The output shows the interface is up and running, with an IP address of 172.17.1.253 and a netmask of 255.255.252.0. It also shows statistics for RX and TX packets and bytes.

```
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.17.1.253 netmask 255.255.252.0 broadcast 172.17.3.255
inet6 fe80::f899:bdf7:8c6a:fd5 prefixlen 64 scopeid 0x20<link>
ether 34:f3:9a:fe:4a:7f txqueuelen 1000 (Ethernet)
RX packets 341124 bytes 221935463 (221.9 MB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 118121 bytes 45051649 (45.0 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

5.What is the status code returned from the server to your browser?

200..

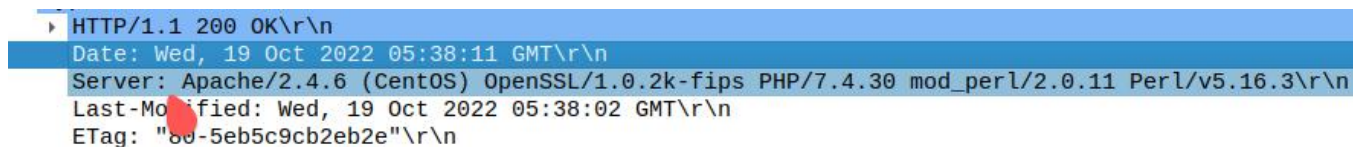


The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first packet is an HTTP GET request from 172.17.1.253 to 128.119.245.12. The second packet is the corresponding HTTP 200 OK response from 128.119.245.12 to 172.17.1.253.

No.	Time	Source	Destination	Protocol	Length	Info
337	10.032074022	172.17.1.253	128.119.245.12	HTTP	639	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
358	10.385829398	128.119.245.12	172.17.1.253	HTTP	552	HTTP/1.1 200 OK (text/html)

6. When was the HTML file that you are retrieving last modified at the server?

last modified-> Wed, 19 oct 2022

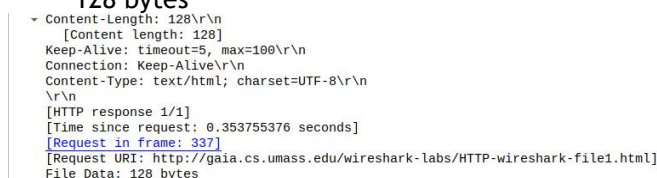


The image shows the packet details pane in Wireshark. The selected packet is the HTTP 200 OK response. The details pane shows the following information:

```
HTTP/1.1 200 OK\r\n
Date: Wed, 19 Oct 2022 05:38:11 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Wed, 19 Oct 2022 05:38:02 GMT\r\n
ETag: "80-5eb5c9cb2eb2e"\r\n
```

7. How many bytes of content are being returned to your browser?

128 bytes



The image shows the packet details pane in Wireshark. The selected packet is the HTTP 200 OK response. The details pane shows the following information:

```
Content-Length: 128\r\n
[Content length: 128]
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: 0.353755376 seconds]
[Request in frame: 337]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

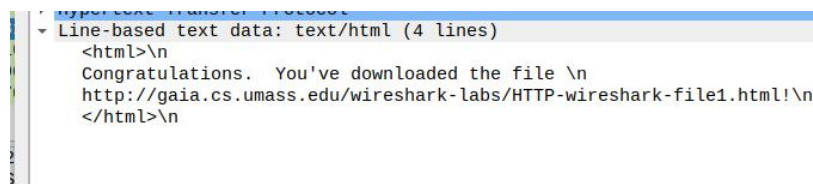
Task 3

1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No there is no IF-MODIFIED line in the HTTP GET.

2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

The contents of the file were expressly returned by the server. The "Line-Based Text Data" part of Wireshark displays what the server delivered back to my browser, more specifically, what the website displayed when I opened it up on my browser.\



```
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes, there is an IF-MODIFIED-SINCE line in the second HTTP message. The time and date that I most recently accessed the website are listed below.



```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "80-5eb5ce7c918bc"\r\n
If-Modified-Since: Wed, 19 Oct 2022 05:59:01 GMT\r\n
\r\n
[Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

4. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The HTTP status code is “304: Not Modified”