



AUBURN

UNIVERSITY

COMP 4320

Introduction to Computer Networks

Project #: Computer Network Lab 1

Logan Bolton – ldb0046

9/22/2025

Executive Summary

This lab explores the basics of networks and HTTP requests. By completing this lab, I was able to understand how my browser was able to interact with a web server.

Table of Contents

Table of Contents

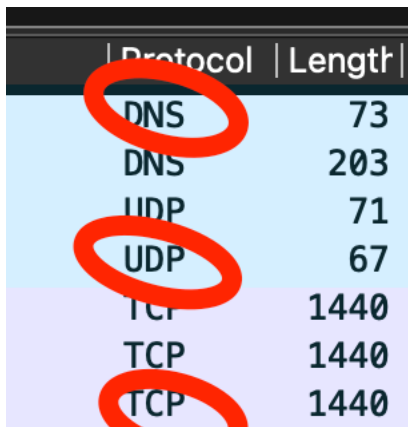
Executive Summary	2
Table of Contents	2
1 Part (1)	3
1.1 Wireshark Basics.....	3
1.1 Login Packets	6
2 Part (2)	7
2.1 2a) DNS & Name Resolution.....	7
2.2 2) HTTP	9
2.2.1 HTTP Basics.....	9
2.2.2 Additional HTTP Information	10
2.2.3 HTTP Conditionals.....	13
2.2.4 Retrieving Long Documents	17
2.2.5 HTML Documents with Embedded Objects	19
2.2.6 HTTP Authentication	20
3 AI Use Reflation Statement.....	21

1 Part (1)

1.1 Wireshark Basics

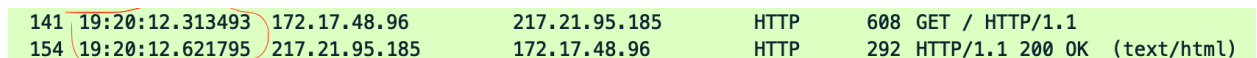
1. List 3 different protocols that appear in the protocol column in the *unfiltered* packet-listing window.

DNS, TCP and TLSv1.2 are all protocols that are listed in Wireshark.



	Protocol	Length
	DNS	73
	DNS	203
	UDP	71
	UDP	67
	TCP	1440
	TCP	1440
	TCP	1440

2. How long did it take from when the HTTP GET message was sent until the first HTTP 200 OK reply was received? (By default, the Time column shows seconds since capture start. To display time-of-day, use *View → Time Display Format → Time of Day*.)

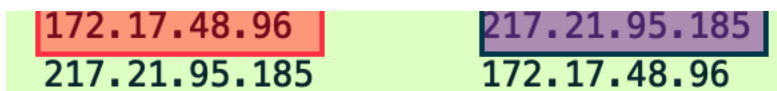


141	19:20:12.313493	172.17.48.96	217.21.95.185	HTTP	608	GET / HTTP/1.1
154	19:20:12.621795	217.21.95.185	172.17.48.96	HTTP	292	HTTP/1.1 200 OK (text/html)

It took approximately **0.308302000 seconds** for the 200 OK reply to be received.

3. What is the Internet address of your computer? What is the Internet address of the *server you accessed*?

The internet address of my computer is **172.16.0.12**. The address of the server I accessed was **217.21.95.185**



172.17.48.96	217.21.95.185
217.21.95.185	172.17.48.96

4. Print the two HTTP messages (GET and OK) referred to above. Select *File → Print*, choose “Selected Packet Only” and “Print as displayed,” then click OK.

/var/folders/kp/vdv61pd97vd0x29b257r8h7h0000gn/T/wireshark_Wi-Fi4ARUC3.pcapng 340 total packets, 2 shown

No.	Time	Source	Destination
124	15:41:38.568843	172.16.0.12	217.21.95.185

HTTP
528 GET / HTTP/
1.1
Frame 124: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface en0, id 0
Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: Netgear_5a:71:18 (9c:c9:eb:5a:71:18)
Internet Protocol Version 4, Src: 172.16.0.12, Dst: 217.21.95.185
Transmission Control Protocol, Src Port: 65341, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: cybernetlab.org\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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 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=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n

No.

[Response in frame: 128]
[Full request URI: http://cybernetlab.org/]
Time Source
128 15:41:38.929687 217.21.95.185
Destination
172.16.0.12
Protocol Length Info
HTTP 218 HTTP/1.1
200 OK (text/html)
Frame 128: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface en0, id 0
Ethernet II, Src: Netgear_5a:71:18 (9c:c9:eb:5a:71:18), Dst: Apple_33:36:98 (80:a9:97:33:36:98)
Internet Protocol Version 4, Src: 217.21.95.185, Dst: 172.16.0.12
Transmission Control Protocol, Src Port: 80, Dst Port: 65341, Seq: 1449, Ack: 463, Len: 152
[2 Reassembled TCP Segments (1600 bytes): #127(1448), #128(152)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Connection: Keep-Alive\r\n

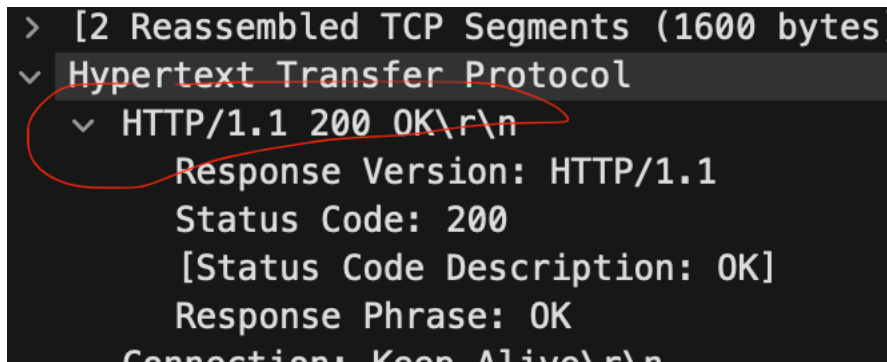
```

Keep-Alive: timeout=5, max=100\r\n
Content-Type: text/html\r\n
Last-Modified: Fri, 05 Sep 2025 20:02:49 GMT\r\n
Etag: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
Accept-Ranges: bytes\r\n
Content-Encoding: gzip\r\n
Vary: Accept-Encoding\r\n
Content-Length: 1229\r\n
Date: Sat, 20 Sep 2025 20:41:38 GMT\r\n
Server: LiteSpeed\r\n
platform: hostinger\r\n
panel: hpanel\r\n
\r\n
[Request in frame: 124]
[Time since request: 0.360844000 seconds]
[Request URI: /]
[Full request URI: http://cybernetlab.org/]
Content-encoded entity body (gzip): 1229 bytes -> 2974 bytes
File Data: 2974 bytes
Line-based text data: text/html (94 lines)

```

5. What was the HTTP status code in the HTTP response?

The HTTP status code was 200.



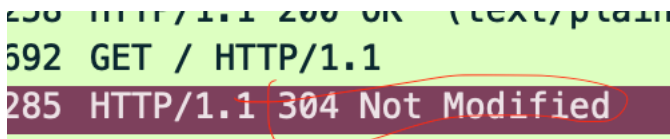
```

> [2 Reassembled TCP Segments (1600 bytes)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Connection: Keep-Alive\r\n

```

6. Refresh the website (<http://cybernetlab.org>), is the HTTP response code still the same? If not, what is the new HTTP status code and why is there a difference?

The HTTP status code changed to 304. Since the website did not change since the last time it was loaded, a cached version of the page was shown.



```

250 HTTP/1.1 200 OK (text/plain)
592 GET / HTTP/1.1
285 HTTP/1.1 304 Not Modified

```

7. Which field in the HTTP request indicates the OS used? And what is the value of that field?

The User-Agent field indicates the OS used. The OS value is Mac OS X 10_15_7.

```
Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzIwbnV0d29ya3M=\r\n
Credentials: network-labs:comp4320networks
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/140.0.0.0 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.
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
If-Modified-Since: Fri, 05 Sep 2025 20:02:49 GMT\r\n
\r\n
[Response in frame: 270]
```

8. Which field in the HTTP request indicates the browser used? And what is the value of that field?

The User-Agent field also indicates the browser used. The value of the browser field is Chrome/140.0.0.0.

```
Cache-Control: max-age=0\r\n
Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzIwbnV0d29ya3M=\r\n
Credentials: network-labs:comp4320networks
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/140.0.0.0 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=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
If-Modified-Since: Fri, 05 Sep 2025 20:02:49 GMT\r\n
\r\n
```

1.1 Login Packets

1. Were there any additional HTTP GET requests? If so, what pages were fetched?

Yes, the login.html page was fetched through a GET request.

IP	Protocol	Port	Request	Status	Response
217.21.95.185	HTTP	575	GET /login.html HTTP/1.1	200	OK (text/html)
172.17.48.96	HTTP	1238	HTTP/1.1	200	OK (text/html)

2. Put in your Auburn username, and password MUST be notsafepassword and click on Submit. After doing this, what type of HTTP request is sent? [GET, POST, PUT, DELETE, PATCH]

IP	Protocol	Port	Request	Status	Response
172.17.48.96	HTTP	258	HTTP/1.1	200	OK (text/plain)
217.21.95.185	HTTP	575	GET /login.html HTTP/1.1	200	OK (text/html)
172.17.48.96	HTTP	1238	HTTP/1.1	200	OK (text/html)
217.21.95.185	HTTP	787	POST /login.php HTTP/1.1	200	OK (application/x-www-form-urlencoded)
172.17.48.96	HTTP	849	HTTP/1.1	200	OK (text/html)

A POST request was sent.

3. Do you see the credentials that you have just put in on Wireshark? If so, in which packet and which field do you see them?

The POST request packet contains the unencrypted username and password. They are in “HTML Form URL Encoded: application/x-www-form-urlencoded” in form item “username” and “password”.

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Response in frame: 462]
[Full request URI: http://cybernetlab.org/login.php]
File Data: 41 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "ldb0046"
  Form item: "password" = "notsafepassword"
```

2 Part (2)

2.1 2a) DNS & Name Resolution

1. What is the Transaction ID of the DNS query and corresponding response?

The transaction ID for both was “0x7063”.

Destination	Protocol	Length	Info
131.204.253.205	DNS	87	Standard query 0x6444 A www-apple-com.v.aaplimg.com
172.17.48.96	DNS	179	Standard query response 0x6444 A www-apple-com.v.aaplimg.com CNAME www.apple.com.edgekey.net
131.204.253.205	DNS	75	Standard query 0x7063 A cybernetlab.org
131.204.253.205	DNS	75	Standard query response 0x612f HTTPS cybernetlab.org
172.17.48.96	DNS	75	Standard query response 0x612f HTTPS cybernetlab.org
172.17.48.96	DNS	91	Standard query response 0x7063 A cybernetlab.org A 217.21.95.185
131.204.253.205	DNS	81	Standard query 0xc164 A captive.g.aaplimg.com
172.17.48.96	DNS	113	Standard query response 0xc164 A captive.g.aaplimg.com A 17.253.7.135 A 17.253.7.131
131.204.253.205	DNS	79	Standard query 0x00c1 A a1961.g2.akamai.net
172.17.48.96	DNS	111	Standard query response 0x00c1 A a1961.g2.akamai.net A 104.120.129.69 A 104.120.129.80

2. Which record types are returned (A, AAAA)? List the answer IP(s).

The record type was A. The answer IP was 217.21.95.185.

```

Domain Name System (Response)
Transaction ID: 0x7063
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
✓ Queries
  ✓ cybernetlab.org: type A, class IN
    Name: cybernetlab.org
    [Name Length: 15]
    [Label Count: 2]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
  ✓ Answers
    ✓ cybernetlab.org: type A, class IN, addr 217.21.95.185
      Name: cybernetlab.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 4
      Address: 217.21.95.185
\[Request In: 6\]
[Time: 0.081544000 seconds]

```

3. What is the TTL for the returned record(s)?

The TTL for the returned record was 1800 (30 minutes).

```

[Label Count: 2]
Type: A (1) (Host Address)
Class: IN (0x0001)
✓ Answers
  ✓ cybernetlab.org: type A, class IN, addr 217.21.95.185
    Name: cybernetlab.org
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 4
    Address: 217.21.95.185
\[Request In: 6\]
[Time: 0.081544000 seconds]

```


- Measure the DNS response time: response timestamp minus query timestamp.

6	19:36:48.738269	172.17.48.96	131.204.253.205	DNS	75	Standard query 0x7063 A cybernetlab.org
7	19:36:48.738340	172.17.48.96	131.204.253.205	DNS	75	Standard query 0x612f HTTPS cybernetlab.org
8	19:36:48.762152	131.204.253.205	172.17.48.96	DNS	75	Standard query response 0x612f HTTPS cybernetlab.org
9	19:36:48.819813	131.204.253.205	172.17.48.96	DNS	91	Standard query response 0x7063 A cybernetlab.org
11	19:36:48.821020	172.17.48.96	131.204.253.205	DNS	81	Standard query response 0x612f HTTPS cybernetlab.org

The response – query time was 0.081544000 seconds

- Verify that the HTTP connection later uses one of the returned IP addresses (clear the display filter and check the IP used by the HTTP packet pair).

It uses the same 217.21.95.185 address.

172.17.48.96	217.21.95.185	HTTP	565	GET / HTTP/1.1
217.21.95.185	172.17.48.96	HTTP	292	HTTP/1.1 200 OK (text/html)

2.2 2) HTTP

2.2.1 HTTP Basics

- What HTTP version does the GET use? What version is reported in the server response?

The response and the GET request both use HTTP 1.1

172.17.48.96	217.21.95.185	HTTP	565	GET / HTTP/1.1
217.21.95.185	172.17.48.96	HTTP	292	HTTP/1.1 200 OK (text/html)

- What is the request–response latency? (time from GET to first 200 OK packet)

The request-response latency was 0.348563000seconds.

```

Date: Mon, 22 Sep 2025 00:48:28 GMT\r\n
Server: LiteSpeed\r\n
platform: hostinger\r\n
panel: hpanel\r\n
\r\n
[Request in frame: 48]
[Time since request: 0.348563000 seconds]
[Request URI: /]

```

- What is your host IP and the server IP used for the HTTP exchange?

My host IP was 172.16.0.12 and the server IP was 217.21.95.185.

172.17.48.96	217.21.95.185	HTTP	608 GET / HTTP/1.1
217.21.95.185	172.17.48.96	HTTP	292 HTTP/1.1 200 OK (text/html)

- What headers are present in the request and in the response (list at least 3 from each)?

“Host”, “User-Agent”, and “Connection” were all in the request. “Connection”, “Server” and “Date” were present in the response.

```

v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: cybernetlab.org\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
  v Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzZl\r\n
    Credentials: network-labs:comp4320networks
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Response in frame: 54]
  [Full request URI: http://cybernetlab.org/]

```

```

v 12 Reassembled TCP Segments (1000 bytes) [0-1000]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html\r\n
    Last-Modified: Fri, 05 Sep 2025 20:02:49 GMT\r\n
    Etag: "b9e-68bb41e9-d0b55a139fbd97a;gz"\r\n
    Accept-Ranges: bytes\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
    Content-Length: 1229\r\n
    Date: Mon, 22 Sep 2025 00:48:28 GMT\r\n
    Server: LiteSpeed\r\n
    platform: hostinger\r\n
    panel: hpanel\r\n
  \r\n
  [Request in frame: 48]
  [Time since request: 0.348563000 seconds]

```

2.2.2 Additional HTTP Information

- Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Both the browser and the server use HTTP/1.1.

HTTP	258	HTTP/1.1	200	OK	(text/plain)
HTTP	608	GET /	HTTP/1.1		
HTTP	292	HTTP/1.1	200	OK	(text/html)

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

The request Accept-Language header has the value “en-US” which indicates that it accepts English.

```
Authorization: Basic bmV0d29yay1SYWJ2OmlNVjBxAg==
Credentials: network-labs:comp4320networks
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Response in frame: 54]
```

3. What is the IP address of your computer? What is the IP address of the server you accessed (e.g., <http://cybernetlab.org>)?

My computer's IP address is 172.17.48.96 and the server's is 217.21.95.185.

172.17.48.96	217.21.95.185	HTTP
217.21.95.185	172.17.48.96	HTTP
172.17.48.96	217.21.95.185	HTTP
217.21.95.185	172.17.48.96	HTTP

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

The status code was 200 OK.

```
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

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

The last time it was modified was Fri, 05 Sep 2025 20:02:49 GMT.

```
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
Content-Type: text/html\r\n
Last-Modified: Fri, 05 Sep 2025 20:02:49 GMT\r\n
Etag: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
Accept-Ranges: bytes\r\n
```

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

1229 bytes were returned for this exchange.

```
[request URI: /]
[Full request URI: http://cybernetlab.org/]
Content-encoded entity body (gzip): 1229 bytes -> 2974 bytes
File Data: 2974 bytes
```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Yes. For example, the request includes “Accept-Language: en-US,en;q=0.9”

40	19:48:28.603290	104.120.129.80	172.17.48.96	HTTP	258	HTTP/1.1 200 OK (text/plain)
48	19:48:28.644477	172.17.48.96	217.21.95.185	HTTP	608	GET / HTTP/1.1
54	19:48:28.993040	217.21.95.185	172.17.48.96	HTTP	292	HTTP/1.1 200 OK (text/html)
202	19:48:29.115013	172.17.48.96	217.21.95.185	HTTP	552	GET /favicon.ico HTTP/1.1
208	19:48:29.422081	217.21.95.185	172.17.48.96	HTTP	974	HTTP/1.1 404 Not Found (text/html)
232	19:48:30.039334	172.17.48.96	217.21.95.185	HTTP	692	GET / HTTP/1.1
238	19:48:30.345698	217.21.95.185	172.17.48.96	HTTP	285	HTTP/1.1 304 Not Modified


```

> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (542 bytes)
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: cybernetlab.org\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
  v Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzIwbnV0d29ya3M=\r\n
    Credentials: network-labs:comp4320networks
    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) Chrom
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n

```

2.2.3 HTTP Conditionals

1. Inspect the headers in the second and third requests. Do you observe If-Modified-Since or If-None-Match? Copy the line if present.

Yes, they are both present:

If-None-Match: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n

If-Modified-Since: Fri, 05 Sep 2025 20:02:49 GMT\r\n

493	20:07:05.007043	172.17.48.96	217.21.95.185	HTTP	692	GET / HTTP/1.1
494	20:07:05.362867	217.21.95.185	172.17.48.96	HTTP	285	HTTP/1.1 304 Not Modified
499	20:07:05.741117	172.17.48.96	217.21.95.185	HTTP	692	GET / HTTP/1.1
500	20:07:06.080458	217.21.95.185	172.17.48.96	HTTP	285	HTTP/1.1 304 Not Modified
504	20:07:06.262650	172.17.48.96	217.21.95.185	HTTP	692	GET / HTTP/1.1
505	20:07:06.592284	217.21.95.185	172.17.48.96	HTTP	285	HTTP/1.1 304 Not Modified


```

Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: Cisco_9f:f2:bf (00:00:0c:9f:f2:bf)
Internet Protocol Version 4, Src: 172.17.48.96, Dst: 217.21.95.185
Transmission Control Protocol, Src Port: 64648, Dst Port: 80, Seq: 1655, Ack: 4102, Len: 626
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: cybernetlab.org\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzIwbmV0d29ya3M=\r\n
    Credentials: network-labs:comp4320networks
    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/90.0.4431.24 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\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
    If-Modified-Since: Fri, 05 Sep 2025 20:02:49 GMT\r\n
  
```

2. What status code is returned to the cached request (304 Not Modified vs 200 OK)? Explain the meaning of the code.

The first status code was 200 OK. The second response was 304 Not Modified. This is because the original request returned the file from a server while the second request returned the cached file.

```

  Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
  
```

3. Compare payload sizes between the first request and the cached request(s). Did the server resend the entire page or did the browser use its cache?

The original request returned 1229 bytes. For the cached request, no body was returned and so only the header was returned which is substantially smaller. The browser reused the cache.

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 64648, Seq: 3883, Ack: 1655, Len:
< Hypertext Transfer Protocol
  < HTTP/1.1 304 Not Modified\r\n
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Etag: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
    Date: Mon, 22 Sep 2025 01:07:05 GMT\r\n
    Server: LiteSpeed\r\n
    platform: hostinger\r\n
    panel: hpanel\r\n
    \r\n
    [Request in frame: 493]
    [Time since request: 0.355822000 seconds]
    [Request URI: /]
    [Full request URI: http://cybernetlab.org/]

```

4. 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. The first request does not include "If-Modified-Since".

```

< GET / HTTP/1.1\r\n
  Request Method: GET
  Request URI: /
  Request Version: HTTP/1.1
  Host: cybernetlab.org\r\n
  Connection: keep-alive\r\n
  Pragma: no-cache\r\n
  Cache-Control: no-cache\r\n
  Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzIwbnV
    Credentials: network-labs:comp4320networks
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 1
  Accept: text/html,application/xhtml+xml,application/
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Response in frame: 322]
  [Full request URI: http://cybernetlab.org/]

```

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

Yes. It is HTTP/1.1 200 OK with Content-Length: 1229, and Wireshark shows File Data: 2974 bytes after decompression.

```
pane1: ipanel1 (1/n
\r\n
[Request in frame: 314]
[Time since request: 0.303987000 seconds]
[Request URI: /]
[Full request URI: http://cybernetlab.org/]
Content-encoded entity body (gzip): 1229 bytes -> 2974 bytes
File Data: 2974 bytes
> Line-based text data: text/html (94 lines)
```

6. 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. It contains the information If-Modified-Since: Fri, 05 Sep 2025 20:02:49 GMT.

```
> Internet Protocol Version 4, Src: 172.17.48.96, Dst: 217.21.95.185
> Transmission Control Protocol, Src Port: 64648, Dst Port: 80, Seq: 1655, Ack
✓ Hypertext Transfer Protocol
  ✓ GET / HTTP/1.1\r\n
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: cybernetlab.org\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  ✓ Authorization: Basic bmV0d29yay1sYWJz0mNvbXA0MzIwbmV0d29ya3M=\r\n
    Credentials: network-labs:comp4320networks
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/5
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
    If-Modified-Since: Fri, 05 Sep 2025 20:02:49 GMT\r\n
  \r\n
```

7. 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.

It returned HTTP/1.1 304 Not Modified. Since no body was sent for the 304, the server did not return the file contents. The browser used the cached copy because the resource had not changed.

```
> Transmission Control Protocol, Src Port: 80, Dst Port:
  v Hypertext Transfer Protocol
    v HTTP/1.1 304 Not Modified\r\n
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
      Connection: Keep-Alive\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Etag: "b9e-68bb41e9-d0b55a139fbdf97a;gz"\r\n
      Date: Mon, 22 Sep 2025 01:07:05 GMT\r\n
      Server: LiteSpeed\r\n
      platform: hostinger\r\n
      panel: hpanel\r\n
      \r\n
      [Request in frame: 493]
      [Time since request: 0.355822000 seconds]
      [Request URI: /]
      [Full request URI: http://cybernetlab.org/]
```

2.2.4 Retrieving Long Documents

8. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

Two requests were sent. **GET /bill-of-rights** and **GET /favicon.ico** The first packet contained the Bill of Rights.

```
HTTP 258 HTTP/1.1 200 OK (text/plain)
HTTP 627 GET /bill-of-rights.html HTTP/1.1
HTTP 1505 HTTP/1.1 200 OK (text/html)
HTTP 571 GET /favicon.ico HTTP/1.1
HTTP 674 HTTP/1.1 404 Not Found (text/html)
```

9. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Frame 95 contained the response for the Bill of Rights request.

95	20:12:43.592564	217.21.95.185	172.17.48.96	HTTP	1305 HTTP/1.1 200 OK (text/html)
181	20:12:43.660973	172.17.48.96	217.21.95.185	HTTP	571 GET /favicon.ico HTTP/1.1
189	20:12:43.956659	217.21.95.185	172.17.48.96	HTTP	974 HTTP/1.1 404 Not Found (text/html)
205	20:12:44.936674	172.17.48.96	217.21.95.185	HTTP	712 GET /bill-of-rights.html HTTP/1.1
208	20:12:45.230658	217.21.95.185	172.17.48.96	HTTP	286 HTTP/1.1 304 Not Modified

Frame 95: 1305 bytes on wire (10440 bits), 1305 bytes captured (10440 bits) on interface en0, id 0
Ethernet II, Src: Cisco_5c:a5:cf (74:8f:c2:5c:a5:cf), Dst: Apple_33:36:98 (80:a9:97:33:36:98)
Internet Protocol Version 4, Src: 217.21.95.185, Dst: 172.17.48.96
Transmission Control Protocol, Src Port: 80, Dst Port: 49846, Seq: 1375, Ack: 562, Len: 1239
[2 Reassembled TCP Segments (2613 bytes): #94(1374), #95(1239)]
Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Response Version: HTTP/1.1
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK
 Connection: Keep-Alive\r\n
 Keep-Alive: timeout=5, max=100\r\n
 Content-Type: text/html\r\n
 Last-Modified: Sat, 06 Sep 2025 15:46:34 GMT\r\n
 Etag: "14a2-68bc575a-42518ef6f6840272;gz"\r\n
 Accept-Ranges: bytes\r\n
 Content-Encoding: gzip\r\n
 Vary: Accept-Encoding\r\n
 Content-Length: 2241\r\n
 Date: Mon, 22 Sep 2025 01:12:43 GMT\r\n
 Server: LiteSpeed\r\n
 platform: hostinger\r\n

0000 4
0010 0
0020 7
0030 6
0040 6
0050 2
0060 0
0070 2
0080 3
0090 4
00a0 3
00b0 3
00c0 7
00d0 0
00e0 6
00f0 6
0100 4
0110 3
0120 2
0130 3
0140 7
0150 6
0160 7
0170 0
0180 d
0190 1
Frame (1

10. What is the status code and phrase in the response?

The response was 200 OK.

95	20:12:43.592564	217.21.95.185	172.17.48.96	HTTP	1305 HTTP/1.1 200 OK (text/html)
181	20:12:43.660973	172.17.48.96	217.21.95.185	HTTP	571 GET /favicon.ico HTTP/1.1
189	20:12:43.956659	217.21.95.185	172.17.48.96	HTTP	974 HTTP/1.1 404 Not Found (text/html)
205	20:12:44.936674	172.17.48.96	217.21.95.185	HTTP	712 GET /bill-of-rights.html HTTP/1.1
208	20:12:45.230658	217.21.95.185	172.17.48.96	HTTP	286 HTTP/1.1 304 Not Modified


```

Frame 95: 1305 bytes on wire (10440 bits), 1305 bytes captured (10440 bits) on interface en0, id 0
Ethernet II, Src: Cisco_5c:a5:cf (74:8f:c2:5c:a5:cf), Dst: Apple_33:36:98 (80:a9:97:33:36:98)
Internet Protocol Version 4, Src: 217.21.95.185, Dst: 172.17.48.96
Transmission Control Protocol, Src Port: 80, Dst Port: 49846, Seq: 1375, Ack: 562, Len: 1239
[2 Reassembled TCP Segments (2613 bytes): #94(1374), #95(1239)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html\r\n
    Last-Modified: Sat, 06 Sep 2025 15:46:34 GMT\r\n
    Etag: "14a2-68bc575a-42518ef6f6840272;gz"\r\n
    Accept-Ranges: bytes\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
  > Content-Length: 2241\r\n
    Date: Mon, 22 Sep 2025 01:12:43 GMT\r\n
    Server: LiteSpeed\r\n
    platform: hostinger\r\n

```

11. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

It needed 2 segments. The segments were #94 (1374) and #95 (1239).

> Transmission Control Protocol, Src Port: 80, Dst Port: 49846, Seq: 1375, A
> [2 Reassembled TCP Segments (2613 bytes): #94(1374), #95(1239)]
> Hypertext Transfer Protocol

2.2.5 HTML Documents with Embedded Objects

1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

I observed 2 requests. The requests were HTTP GET for the page: "GET /recommended-textbook.html" and "GET /favicon.ico".

105	20:17:13.269362	172.17.48.96	217.21.95.185	HTTP	63	GET /recommended-textbook.html HTTP/1.1
165	20:17:13.569945	217.21.95.185	172.17.48.96	HTTP	549	HTTP/1.1 200 OK (text/html)
165	20:17:13.721496	172.17.48.96	217.21.95.185	HTTP	57	GET /favicon.ico HTTP/1.1
168	20:17:14.035595	217.21.95.185	172.17.48.96	HTTP	974	HTTP/1.1 404 Not Found (text/html)

- Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

By looking at the TLS information, I can see that each of the image requests started within a few microseconds of each other. This indicates that they were downloaded in parallel.

Info	ws.col.info	relative	Source	Destination	Protocol	Length	Info
	53	18:16:59.68...	172.17.48.96	217.21.95.185	TLSv1...	513	Client Hello (SNI=cybernetlab.org)
	74	18:17:00.09...	172.17.48.96	217.21.95.185	TLSv1...	481	Client Hello (SNI=cybernetlab.org)
	83	18:17:00.39...	172.17.48.96	217.21.95.185	TLSv1...	449	Client Hello (SNI=cybernetlab.org)
	98	18:17:02.02...	172.17.48.96	35.186.224.9	QUIC	1292	Initial, DCID=b4041618e19b2189, PKN:
	141	18:17:02.66...	172.17.48.96	35.186.224.24	QUIC	1292	Initial, DCID=8676d2948c378ee0, PKN:
	171	18:17:02.69...	172.17.48.96	35.186.224.24	QUIC	1292	Initial, DCID=162e004e03a89604, PKN:
	175	18:17:02.69...	172.17.48.96	35.186.224.24	QUIC	1292	Initial, DCID=47204611f4e81c93, PKN:
	204	18:17:02.71...	172.17.48.96	23.0.162.231	TLSv1...	812	Client Hello (SNI=i.scdn.co)
	272	18:17:02.86...	172.17.48.96	131.204.138.170	TLSv1...	508	Client Hello (SNI=auburn.edu)
	297	18:17:02.88...	172.17.48.96	23.7.33.70	TLSv1...	481	Client Hello (SNI=www.pearson.com)
	303	18:17:02.89...	172.17.48.96	151.101.65.229	TLSv1...	482	Client Hello (SNI=cdn.jsdelivr.net)
	365	18:17:02.89...	172.17.48.96	151.101.65.229	TLSv1...	418	Client Hello (SNI=cdn.jsdelivr.net)

2.2.6 HTTP Authentication

- What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

The initial response was HTTP/1.1 401 Unauthorized.

HTTP	258	HTTP/1.1 200 OK (text/plain)
HTTP	504	HTTP/1.1 401 Unauthorized (text/html)
HTTP	443	GET /protected.php HTTP/1.1
HTTP	504	HTTP/1.1 401 Unauthorized (text/html)

- When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

In the second GET message, it contains the header "Authorization" with the username and password in plain text.

Accept-Encoding: gzip, deflate\r\n
Authorization: Basic bmV0d29yay1sYWJzOmNvbXA0MzIwbmV0d29ya3M=\r\n
Credentials: network-labs:comp4320networks

3 AI Use Reflation Statement

I used ChatGPT to help understand the basics of Wireshark. I also used it to help clarify my writing for the report. The actual lab and the core ideas in the analysis were completed by me. I found ChatGPT to be very helpful for explaining core networks ideas.

By writing this reflection, I acknowledge that AI is a support tool, not a substitute for my own effort, and I take full responsibility for the final submission.