A close up of a sign

Description automatically generated

**COMP 4320**

**Introduction to Computer Networks**

Project #: Computer Network Lab 1

Logan Bolton

9/22/2025

# Executive Summary

Format:

* Font: Arial
* Font Size: 11
* Spacing: Double

This section should begin on a new page. The executive summary should include a summary of the findings and decisions

# Table of Contents

This section should begin on a new page. The table of contents below is generated using the "References" menu.

Table of Contents

[Executive Summary 2](#_Toc208308380)

[Table of Contents 3](#_Toc208308381)

[List of Figures 4](#_Toc208308382)

[List of Tables 5](#_Toc208308383)

[1 Part (1) 6](#_Toc208308384)

[2 Part (2) 6](#_Toc208308385)

[2.1 First Subheading 6](#_Toc208308386)

[2.2 Second Subheading 6](#_Toc208308387)

[2.2.1 First Sub-subheading 6](#_Toc208308388)

[2.2.2 Second Sub-subheading 7](#_Toc208308389)

[3 Acknowledgements 7](#_Toc208308390)

[4 References 7](#_Toc208308391)

[5 AI Generated Statement 7](#_Toc208308392)

[Appendix A: Place the title of appendix here 8](#_Toc208308393)

# List of Figures

This section should begin on a new page. This should be one of the last pages to be completed. Each Figure should have a descriptive caption.

# List of Tables

This section should begin on a new page. All tables must have a caption. If no tables are needed this section can be omitted.

# 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 protocols that are listed in Wireshark.

1. 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*.)

It took approximately 0.360844 seconds for the 200 OK reply to be received.

1. 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

1. 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 Protocol Length Info

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)

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

The HTTP status code was 200.

1. 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.

1. 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.

1. 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.

## 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.

1. 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]

A POST request was sent.

1. 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”.

# 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 was 0xa897. The response was in frame 66 and was “cybernetlab.org: type A, class IN, addr 217.21.95.185”.

1. 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.

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

The TTL for the returned record was 225 (3 minutes, 45 seconds).

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

The DNS response time was 2.83 ms.

1. 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.

## 2.2 2) HTTP

### 2.2.1 HTTP Basics

1. 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

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

The request-response latency was 0.007301000 seconds.

1. 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.

1. 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.

### 2.2.2 Additional HTTP Information

1. 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.

1. 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.

1. 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 is172.17.48.96 and the server’s is 217.21.95.185.

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

The status code was 304 Not Modified.

1. 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.

1. How many bytes of content are being returned to your browser?   
     
   0 bytes were returned for this exchange.
2. 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”

### 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

1. 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.

1. 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 2974 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.

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. The first request does not include “If-Modified-Since”.

1. 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.

1. 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.

1. 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 its cached copy because the resource had not changed.

### 2.2.4 Retrieving Long Documents

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
3. What is the status code and phrase in the response?
4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

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

### 2.2.6 HTTP Authentication

1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
2. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

# 3 Acknowledgements

This section allows authors to acknowledge contributors and other sources that are not appropriate to list in the references section.

# 4 References

This is the last section of the report, prior to any appendices. The references should not be double-spaced, but single-spaced. For a technical report, use the CSE style.

[1] Reference 1 information.

[2] Reference 2 information.

[3] Reference 3 information.

# 5 AI Use Reflation Statement

As part of this assignment, you are required to explain how Artificial Intelligence (AI) tools were used in your work. For this you need to describe:

* Purpose of Use – Why you chose to use AI (for example: brainstorming, outlining, checking grammar, simplifying complex ideas, or generating examples).
* Extent of Use – To what degree AI contributed (for example: “I used AI to help refine my outline, but the analysis and arguments were entirely my own”).
* My Contribution – How I ensured the final assignment represents my own original thinking, understanding, and interpretation.

Reflections – What I found useful, what limitations I noticed, and how AI influenced my learning process.

**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.**