Catalina Cisneros

**Lab: Wireshark Lab: HTTP**

**1. The Basic HTTP GET/response interaction**

Start up your web browser.

A screenshot of a computer

AI-generated content may be incorrect.

Start Wireshark and wait 2 minutes

A screenshot of a computer

AI-generated content may be incorrect.

Enter on my browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

A screenshot of a computer

AI-generated content may be incorrect.

Stop packet capture

A screenshot of a computer

AI-generated content may be incorrect.

**Questions**

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

🡪 Both browser and server are running HTTP/1.1

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 Browser can accept Spanish (es, es-419), French (fr-FR, fr)

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 Source IP (my computer): 10.108.109.206

🡪 Destination IP: 128.119.245.12

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪The server returned 200 OK.

A screenshot of a computer

AI-generated content may be incorrect.

1. When was the HTML file that you are retrieving last modified at the server?  
   🡪 the HTML file was last modified on Fri, 03 Oct 2025 05:59:01 GMT = 01:59:01 EST  
   A screenshot of a computer

   AI-generated content may be incorrect.
2. How many bytes of content are being returned to your browser?  
   🡪 128 bytes of content were returned.  
   A screenshot of a computer

   AI-generated content may be incorrect.
3. 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.  
   🡪Example not shown in main list but visible in raw data is Connection: Keep-Alive

A screenshot of a computer

AI-generated content may be incorrect.

**2. The HTTP CONDITIONAL GET/response interaction**

Start up my web browser and Wireshark

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Enter the given URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html twice in the browser

A screenshot of a computer

AI-generated content may be incorrect.

Stop packet capture and filter by http

A screenshot of a computer

AI-generated content may be incorrect.

**Questions**

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 GET did not include an “If-Modified-Since” line.

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 Yes, the server returned the file. The “200 OK” status and the presence of a Content-Length field confirm it.

A screenshot of a computer

AI-generated content may be incorrect.

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 GET6? If so, what information follows the “IF-MODIFIED-SINCE:” header?

🡪 Yes, the second GET includes “If-Modified-Since: Sun, 05 Oct 2025 05:59:01 GMT\r\n”

A screenshot of a computer

AI-generated content may be incorrect.

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.

🡪 The server replied 304 Not Modified, meaning it did not resend the file and the browser used the cached version.

A screenshot of a computer

AI-generated content may be incorrect.

**3. Retrieving Long Documents**

Restart my web browser (cache + history cleared) and Wireshark

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

A screenshot of a computer

AI-generated content may be incorrect.

Stop Wireshark and filter by http

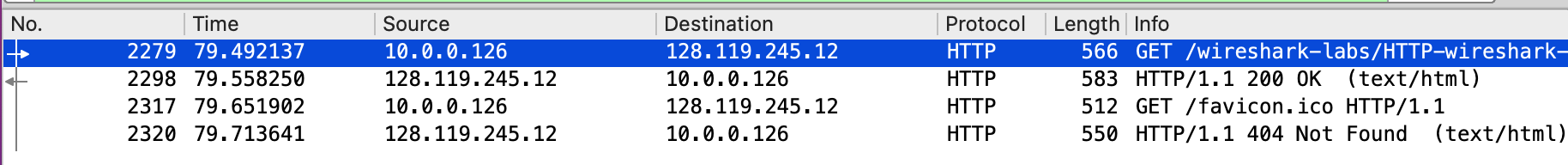
A screenshot of a computer

AI-generated content may be incorrect.

**Questions:**

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?

🡪 My browser sent 2 GET requests (one for file3.html and one for favicon.ico). The GET for the Bill of Rights is in packet 2279



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

🡪The response with the status code appears in packet 2298



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

🡪HTTP/1.1 200 OK.

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The HTTP response needed 4 data-containing TCP segments:

*14 Reassembled TCP Segments (4861 bytes):*

*[Frame: 2292, payload: 0-1447 (1448 bytes)]*

*[Frame: 2294, payload: 1448-2895 (1448 bytes)]*

*[Frame: 2296, payload: 2896-4343 (1448 bytes)]*

*[Frame: 2298, payload: 4344-4860 (517 bytes)]*

*[Segment count: 4]*

*Reassembled TCP length: 48611*

A screenshot of a computer

AI-generated content may be incorrect.

**4. HTML Documents with Embedded Objects**

Restart my web browser (cache + history cleared) and Wireshark

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

A screenshot of a computer

AI-generated content may be incorrect.

Stop Wireshark and filter by http

A screenshot of a computer

AI-generated content may be incorrect.

**Questions**

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

🡪 My browser sent 4 HTTP GET requests.

* /wireshark-labs/HTTP-wireshark-file4.html 🡪 128.119.245.12
* /pearson.png 🡪 128.119.245.12
* /8E\_cover\_small.jpg 🡪 178.79.137.164
* /favicon.ico 🡪 128.119.245.12

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 The two images were downloaded in parallel.

🡪 The GET for pearson.png was sent to 128.119.245.12 at 21.468 s, and the GET for 8E\_cover\_small.jpg was sent to 178.79.137.164 at 21.826 s. Only about 0.36 seconds of different. Because the browser initiated both requests to different servers nearly simultaneously, it retrieved the two images in parallel rather than serially.

A screenshot of a computer

AI-generated content may be incorrect.

**5 HTTP Authentication**

Restart my web browser (cache + history cleared) and Wireshark

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

A screenshot of a computer

AI-generated content may be incorrect.

Enter username and password

* Username: wireshark-students
* Password: network

A screenshot of a chat

AI-generated content may be incorrect.

Stop Wireshark and filter by http

A screenshot of a computer

AI-generated content may be incorrect.

**Questions**

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

🡪 The server replied with HTTP/1.1 401 Unauthorized, meaning the page is protected and my browser didn’t have the authorization needed to access it.

A screenshot of a computer

AI-generated content may be incorrect.

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

🡪 When my browser sent the second GET request, it added an Authorization field that included my login credentials encoded in Base64.

A screenshot of a computer

AI-generated content may be incorrect.

🡪 Decoding the credentials

A screenshot of a chat

AI-generated content may be incorrect.