

Wireshark 2

Due Feb 5 at 11am **Points** 40 **Questions** 20 **Time Limit** None
Allowed Attempts Unlimited

Instructions

TODO

[Original Instructions and background](https://www-net.cs.umass.edu/wireshark-labs/Wireshark_HTTP_v7.0.pdf)

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	40 minutes	0 out of 40 *


* Some questions not yet graded

Score for this attempt: **0** out of 40 *

Submitted Feb 2 at 11:48am

This attempt took 40 minutes.

Part 1 - The Basic HTTP GET/response interaction

- Make sure to clear your cache first. Although I recommend using an icognito-type window.
- Url to request during the trace (make sure it's *NOT* HTTPS):
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>  (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>)

Question 1**Not yet graded / 2 pts**

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

Your Answer:

1.1, 1.1

Question 2**Not yet graded / 2 pts**

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

Your Answer:

en-US

Question 3**Not yet graded / 2 pts**

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

Your Answer:

144.38.233.98 (my computer)

128.119.245.12 (server)

Question 4**Not yet graded / 2 pts**

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

Your Answer:

200

Question 5

Not yet graded / 2 pts

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

Your Answer:

Fri, 02 Feb 2024 06:59:02 GMT

Unanswered

Question 6

Not yet graded / 2 pts

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

Your Answer:

Question 7


Not yet graded / 2 pts

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

Your Answer:

no

Part 2 - The HTTP CONDITIONAL GET/response interaction

- Make sure to clear your cache first. Although I recommend using an icognito-type window.
- Url to request during the trace (make sure it's *NOT* HTTPS):
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>  (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>)

Unanswered

Question 8

Not yet graded / 2 pts

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?

Your Answer:

Unanswered

Question 9

Not yet graded / 2 pts

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

Your Answer:

Unanswered

Question 10

Not yet graded / 2 pts

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?

Your Answer:

Unanswered


Question 11

Not yet graded / 2 pts

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.

Your Answer:

Part 3 - Retrieving Long Documents

- Make sure to clear your cache first. Although I recommend using an incognito-type window.
- Url to request during the trace (make sure it's *NOT* HTTPS):
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>  (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>)

Unanswered

Question 12

Not yet graded / 2 pts

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?

Your Answer:

Unanswered

Question 13

Not yet graded / 2 pts

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

Your Answer:

Unanswered

Question 14

Not yet graded / 2 pts

What is the status code and phrase in the response?

Your Answer:

Unanswered

Question 15

Not yet graded / 2 pts

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

Your Answer:

Part 4 - HTML Documents with Embedded Objects

- Make sure to clear your cache first. Although I recommend using an incognito-type window.

- Url to request during the trace (make sure it's *NOT* HTTPS):
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> → (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>)

Unanswered

Question 16

Not yet graded / 2 pts

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

Your Answer:

Unanswered

Question 17

Not yet graded / 2 pts

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

Your Answer:

Part 5 - HTTP Authentication

- Make sure to clear your cache first. Although I recommend using an icognito-type window.
- Url to request during the trace (make sure it's *NOT* HTTPS):
http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html → (http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)

Unanswered

Question 18**Not yet graded / 2 pts**

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

Your Answer:

Unanswered


Question 19**Not yet graded / 2 pts**

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

Your Answer:

Unanswered

Question 20**Not yet graded / 2 pts**

Look for the Authorization header. Find the string of characters that looks encrypted text. Copy only that string of characters and paste it into a base64 decoder such as [Base64.Guru](https://base64.guru/converter/decode)  (<https://base64.guru/converter/decode>). Copy the decoded response and paste it here for your answer to this question.

Your Answer:

Quiz Score: 0 out of 40