The Basic HTTP GET/response interaction

> Reference files for this part:
>
> - HTTP_Wireshark_Lab/wireshark_files/basic-http-get-response.pcapng
> - HTTP_Wireshark_Lab/wireshark_pdfs/wireshark-basic-http-get.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/wireshark-basic-http-response.pdf

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

-Both my browswe and the server are running `HTTP version 1.1`

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

- Accept-language is en-US (US English)

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

- IP address of my computer is `10.0.2.15`
- IP address for gaia.cs.umass.edu server is `128.119.245.12`

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

- The status code is 200.

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

- Last modified Thursday, 2 Jan, 2025, 06:59:02 GMT

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

- The content is 128 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.

- There are no headers.

The HTTP CONDITIONAL GET/response interaction

> Reference files for this part:
>
> - HTTP_Wireshark_Lab/wireshark_files/http-conditional-get-response.pcapng
> - HTTP_Wireshark_Lab/wireshark_pdfs/conditional-get_no.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/conditional-get_yes.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/conditional-not_modified.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/conditional-response1.pdf

8. 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

9. 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 content of the file explicitly.
- I can tell because the repoonse status is 200 OK. Also, when the header `Line-based text data` in the **packet detail pane** is expanded, the same content displayed in the browser is displayed.

10. 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 GET1? If so, what information follows the "IF-MODIFIED-SINCE:" header?

- Yes. The information is `Thu, 02 Jan 2025 06:59:02 GMT \r\n`

11. 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 response status code is `304`.
- The server did not explicity return the content, since the text after the status code reads `Not Modified`

Retrieving Long Documents

> Reference files for this part
>
> - HTTP_Wireshark_Lab/wireshark_files/long-doc-retrieval.pcapng
> - HTTP_Wireshark_Lab/wireshark_pdfs/wireshark-retrieval-get_16.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/wireshark-retrieval-response_21.pdf

12. 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 one `GET request`
- The packet number in the trace containing the GET for the Bill or Rights is 16.

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

- The packet number in the trace containing the status code and phrase associated with the response to the HTTP GET is `21`.

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

- The status code is `200 OK` and the phrase is `(text/html))`

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

- Four data-containing TCP segments were needed.

HTML Documents with Embedded Objects

> Reference file for this part
>
> - HTTP_Wireshark_Lab/wireshark_files/embedded_objects.pcapng
> - HTTP_Wireshark_Lab/wireshark_pdfs/wireshark-embedded-object_1.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/wireshark--embedded-object_2.pdf

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

- Four HTTP GET request were sent, including `GET /favicon.ico`. So, without `GET /favicon.ico`, three requests were sent.
- The addresses are:
  - /wireshark-labs/HTTP-wireshark-file4.html
  - /pearson.png
  - /8E_cover_small.jpg

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

- Yes, they were downloaded serially. This is because the time difference between the first and second HTTP GET request for the images is $05:13:40.601781039−05:13:40.343538981=0.258242058$ That is `0.258242058 seconds`, which is quite significant in terms of computer time.

HTTP Authentication

> Reference files for this part
>
> - HTTP_Wireshark_Lab/wireshark_files/http-authenticate.pcapng
> - HTTP_Wireshark_Lab/wireshark_pdfs/http-authenticate-401-unauth.pdf
> - HTTP_Wireshark_Lab/wireshark_pdfs/http-authenticate-auth.pdf

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

- The status code is `401` and the phrase is `Unauthorized`; there is the header `WW-Authenticate`

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

- The field is `Authorization: Basic d2lyZXNo...cms=\r\n` header