

WIRESHAK LAB HTTP

KONSEP JARINGAN



Disusun oleh:

Aprilia Dwi Cristyana (3122500032)

2 D3 Teknik Informatika B

Dosen Pengampu :

Iwan Syarif S.Kom., M.Kom., M.Sc., Ph.D.

PROGRAM STUDI D3 TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI

SURABAYA 2022 / 2023

The Basic HTTP GET/response interaction

Enter the following to your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

The image shows a Wireshark packet capture of an HTTP interaction. The packet list on the left shows four packets. Packet 471 is the GET request, and packet 473 is the 200 OK response. The packet details pane for packet 471 shows the request structure, including the host, connection, user-agent, and various headers. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
401	10.000000	192.168.1.10	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
471	10.267313	128.119.245.12	192.168.1.10	HTTP	540	HTTP/1.1 200 OK (text/html)
473	10.425960	192.168.1.10	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
474	10.730339	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file1.html

Request Version: HTTP/1.1

My browser use HTTP version 1.1

HTTP version of server is 1.1

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

Accept-Language: en-US,en;q=0.9\r\n

Language : English and Indonesian

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

No.	Time	Source	Destination	Protocol	Length	Info
401	10.000000	192.168.1.10	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
471	10.267313	128.119.245.12	192.168.1.10	HTTP	540	HTTP/1.1 200 OK (text/html)
473	10.425960	192.168.1.10	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
474	10.730339	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

My IP address : 192.168.1.10

Gaia ip address : 128.119.245.12

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

No.	Time	Source	Destination	Protocol	Length	Info
471	10.267313	128.119.245.12	192.168.1.10	HTTP	540	HTTP/1.1 200 OK (text/html)

Status Code : 200 (success)

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

Last-Modified: Sat, 25 Nov 2023 06:59:02 GMT\r\n

Last Modified: Sat, 25 November 2023 06:59:02 GMT\r\n

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

Content-Length: 128\r\n

128 bytes of content are being returned

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.

I don't see any different headings between the 2 windows

The HTTP CONDITIONAL GET/response interaction

Enter the following URL into your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

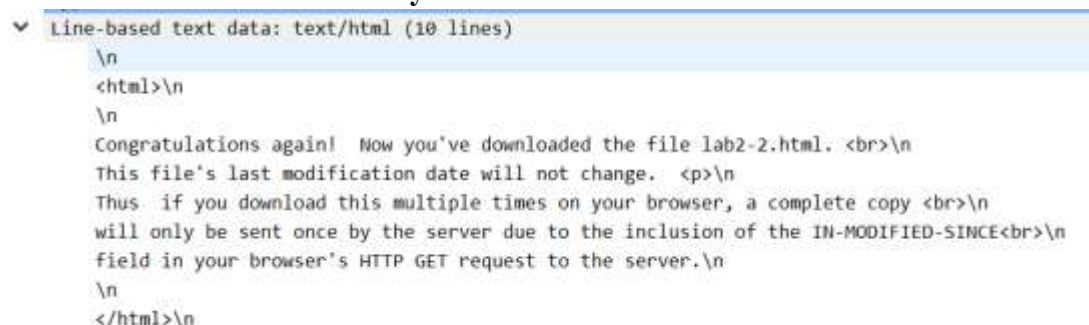


The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows Frame 227: 520 bytes on wire (4208 bits), 520 bytes captured (4208 bits) on interface 0. The packet details pane shows the following layers: Ethernet II, Src: Chonglin_52:25:40, Dst: Ziccom_08:00:06:00:00:06, Internet Protocol Version 4, Src: 192.168.1.10, Dst: 130.119.245.12, Transmission Control Protocol, Src Port: 60399, Dst Port: 80, Seq: 1, ACK: 3440, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, TCP header, and the HTTP GET request.

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 there's no IF-MODIFIED-SINCE line in the GET message

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



The image shows the packet details pane for the server response (Frame 228). The packet list shows Frame 228: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0. The packet details pane shows the following layers: Ethernet II, Src: Ziccom_08:00:06:00:00:06, Dst: Chonglin_52:25:40, Internet Protocol Version 4, Src: 130.119.245.12, Dst: 192.168.1.10, Transmission Control Protocol, Src Port: 80, Dst Port: 60399, Seq: 3440, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, TCP header, and the HTTP 200 OK response. The response body is displayed in the packet bytes pane as a line-based text data: text/html (10 lines).

```
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

The server did explicitly return the contents of the file. Wireshark includes a section titled “Line-Based Text Data” which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser.

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

Last-Modified: Sat, 25 Nov 2023 06:59:02 GMT\r\n

information follows the “IF-MODIFIED-SINCE:” header is Sat, 25 NOVEMBER 2023 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.

Status Code: 304

The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.

Retrieving Long Documents

Enter the following URL into your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

296	8.052734	192.168.1.10	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
302	8.399445	128.119.245.12	192.168.1.10	HTTP	539 HTTP/1.1 404 Not Found (text/html)
305	10.237136	192.168.1.10	128.119.245.12	HTTP	639 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
309	10.584367	128.119.245.12	192.168.1.10	HTTP	204 HTTP/1.1 304 Not Modified

Frame 296: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface Device(MPF_...)
Ethernet II, Src: Chongjin_57:25:85 (18:c8:06:57:25:85), Dst: Zioncom_08:02:1c (18:0d:07:a6:02:1c)
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60793, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
Hypertext Transfer Protocol

12. 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?

296	8.052734	192.168.1.10	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
302	8.399445	128.119.245.12	192.168.1.10	HTTP	539 HTTP/1.1 404 Not Found (text/html)
305	10.237136	192.168.1.10	128.119.245.12	HTTP	639 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
309	10.584367	128.119.245.12	192.168.1.10	HTTP	204 HTTP/1.1 304 Not Modified

My browser only sent 2 HTTP GET request to the server. The Packet that contained the GET message was packet number 296 and 3.

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

296	8.052734	192.168.1.10	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
302	8.399445	128.119.245.12	192.168.1.10	HTTP	539 HTTP/1.1 404 Not Found (text/html)

The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 302.

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

The status code from this packet was a 372, and the phrase was an OK.

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

[Frame: 461, payload: 0-1439 (1440 bytes)]
[Frame: 463, payload: 1440-2879 (1440 bytes)]
[Frame: 462, payload: 2880-4319 (1440 bytes)]
[Frame: 464, payload: 4320-4860 (541 bytes)]
[Segment count: 4]

The data was sent in 4 TCP segments to the browser, then reassembled

HTML Documents with Embedded Objects

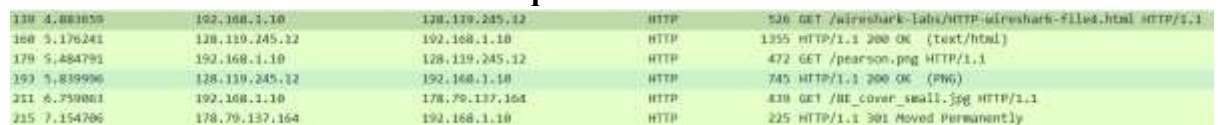
Enter the following URL into your browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>



No.	Time	Source	Destination	Protocol	Length	Info
139	4.883658	192.168.1.10	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
160	5.176241	128.119.245.12	192.168.1.10	HTTP	1355	HTTP/1.1 200 OK (text/html)
179	5.484791	192.168.1.10	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
193	5.839996	128.119.245.12	192.168.1.10	HTTP	745	HTTP/1.1 200 OK (PNG)
211	6.759081	192.168.1.10	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
215	7.154796	178.79.137.164	192.168.1.10	HTTP	225	HTTP/1.1 301 Moved Permanently

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



No.	Time	Source	Destination	Protocol	Length	Info
139	4.883658	192.168.1.10	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
160	5.176241	128.119.245.12	192.168.1.10	HTTP	1355	HTTP/1.1 200 OK (text/html)
179	5.484791	192.168.1.10	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
193	5.839996	128.119.245.12	192.168.1.10	HTTP	745	HTTP/1.1 200 OK (PNG)
211	6.759081	192.168.1.10	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
215	7.154796	178.79.137.164	192.168.1.10	HTTP	225	HTTP/1.1 301 Moved Permanently

My browser sent 3 http GET message requests. One each to each for each of the following: The initial page, the Pearson logo, and the cover of the Pearson book, 5th Edition.

Initial page : 128.119.245.12

Pearson logo : 128.119.245.12

Cover : 178.79.137.164

Rincian :

The first request was for /wireshark-labs/HTTP-wiresharkfile4.html from IP 192.168.1.10 to 128.119.245.12. The second request was for /pearson.png, also from 192.168.1.10 to 128.119.245.12. The third request was for /8E_cover_small.jpg from 192.168.1.10 to IP address 178.79.137.164.

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.

The browser's downloading behavior seems to have occurred in a sequential manner rather than in parallel. This is evident because the request for the second image (/pearson.png) was made only after the response for the first image (/wireshark-labs/HTTP-wireshark-file4.html) was received. In contrast, the browser initiated a separate GET request for a different image (/8E_cover_small.jpg) to a different server (178.79.137.164) while waiting for the response for the second image. This suggests a sequential downloading pattern rather than a parallel one, as the requests for the images were not made concurrently, but one after the other.

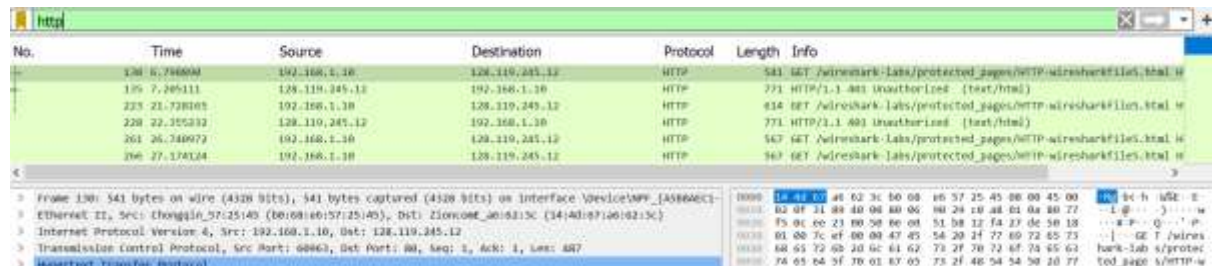
HTTP Authentication

Enter the following URL into your browser

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html

Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.



The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows several packets, with packet 277 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP 401 Unauthorized response. The status bar at the bottom indicates the packet is from 192.168.1.10 to 128.119.245.12.

No.	Time	Source	Destination	Protocol	Length	Info
130	6.786000	192.168.1.10	128.119.245.12	HTTP	541	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
135	7.245111	128.119.245.12	192.168.1.10	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
225	21.738105	192.168.1.10	128.119.245.12	HTTP	414	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
228	22.255232	128.119.245.12	192.168.1.10	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
261	26.748972	192.168.1.10	128.119.245.12	HTTP	547	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
266	27.374124	192.168.1.10	128.119.245.12	HTTP	547	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1

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

The server issues a 401 Unauthorized status code, along with the message "HTTP/1.1 401 Unauthorized (text/html)." This signals that access to the requested resource located at /wireshark-labs/protected_pages/HTTP-wireshark-file5.html is restricted, necessitating authentication or proper permissions. The reason for denial is attributed to the absence of essential credentials in the initial request made by the client (browser). In essence, the server communicates that access is not granted due to the insufficient authentication information provided in the initial request.

19. 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 instance of the browser sending an HTTP GET message, it is probable that the Authorization header is now part of the message. This header serves the purpose of incorporating credentials, like a username and password, into the request. By doing so, the client establishes its identity to the server, facilitating access to the safeguarded resource. The addition of this header is a response to the initial 401 Unauthorized reply encountered when trying to access the protected page initially.

Conclusion :

The analysis reveals successful communication between the browser and server using HTTP 1.1. It includes details on language preferences, IP addresses, status codes, modification dates, content size, and headers. Additionally, the examination of conditional GET/response interactions, long document retrieval, and authentication processes provides insights into the communication dynamics between the client and server.