

Contents

1 Basic HTTP Get Interaction	2
1.1 HTTP Version	2
1.2 What Language can our browser accept from server?	2
1.3 IP Address of our computer	2
1.4 Status Code returned from Server to browser.	3
1.5 Last modified date of the html file	3
1.6 How many bytes of content are being returned to the browser?	3
1.7 Raw Data Header and Packer Listing Window - do they differ?	4
2 GET/Response Interaction	4
2.1 Any IF_MODIFIEDSINCE?	4
2.2 Did the server explicitly returned content file?	4
2.3 After refresh, any IF_MODIFIEDSINCE?	5
2.4 After refresh, status code and response.	5
3 Long Documents	5
3.1 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?	6
3.2 Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?	6
3.3 What is the status code and phrase in the response?	7
3.4 How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?	7
4 Documents with Embedded Objects	7
4.1 Number of GET requests and Where were they sent?	8
4.2 Images downloaded Serially or parallelly?	8
5 HTTP Authentication	8
5.1 Server's Response to Initial GET Request	9
5.2 When sending the GET request for the second time, what new field was included?	9
6 About Me	9

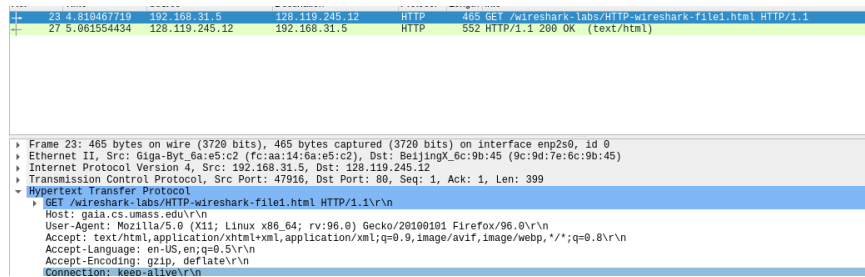
1 Basic HTTP Get Interaction

We first start the wireshark and wait for 2 minutes. Then we go to the site LINK and in the wireshark, set "http" in visual filter.

1.1 HTTP Version

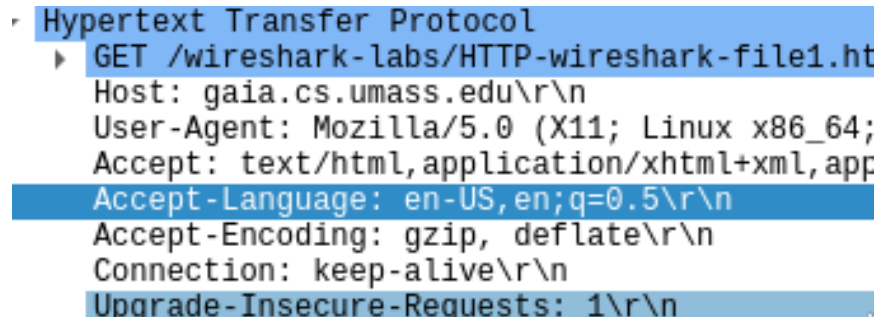
HTTP 1.1

We checked the header section of the request and response message and found the same answer.



1.2 What Language can our browser accept from server?

enUS, meaning it accepts United States English Language only.



1.3 IP Address of our computer

192.168.31.5 -> Its the ip address of my computer.

	Time	Source	Destination
23	4.810467719	192.168.31.5	128.119.245.12
27	5.061554434	128.119.245.12	192.168.31.5

1.4 Status Code returned from Server to browser.

Server responded OK.

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 07 Feb 2022 13:05:55

```

1.5 Last modified date of the html file

Current time (7 February, 2022, 7:05)

It seems it was stored in local ISP's proxy server as I requested for it multiple time as I forgot to clear my cache so no http requests were sniffed by wireshark.

```

HTTP/1.1 200 OK\r\n
Date: Mon, 07 Feb 2022 13:05:55 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.
Last-Modified: Mon, 07 Feb 2022 06:59:01 G

```

1.6 How many bytes of content are being returned to the browser?

128 Bytes.

```

ETag: "80-5d76822ad3b50"\r\n
Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
Keep-Alive: timeout=5, max=10
Connection: Keep-Alive\r\n

```

1.7 Raw Data Header and Packer Listing Window - do they differ?

Yes. The last four line in packet-listing-window were apparently extra meta data that wireshark decided to show us, We did not find this portion in raw bytes.

```
***
[HTTP response 1/1]
[Time since request: 0.251086715 seconds]
[Request in frame: 23]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

2 GET/Response Interaction

This is our wireshark output after we requested for the website.

The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list on the left shows four packets: a SYN, a GET request, a 200 OK response, and a FIN. The details pane for the selected packet (the 200 OK response) shows the following information:

- Frame 40: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface emp250, id 0
- Ethernet II, Src: Giga-Byt_8a:e5:c2 (fc:aa:14:8a:e5:c2), Dst: Beijing_6c:9b:45 (9c:9d:7e:6c:9b:45)
- Internet Protocol Version 4, Src: 192.168.31.5, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 47922, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 - Host: gaia.cs.umass.edu
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate
 - Connection: keep-alive
 - Upgrade-Insecure-Requests: 1
 - DNT: 1
 - Sec-DC: 1

The packet bytes pane shows the raw data of the response, starting with the HTTP status line: 200 OK (text/html).

2.1 Any IF_MODIFIEDSINCE?

No. There were no IF_MODIFIEDSINCE in the first GET message.

2.2 Did the server explicitly returned content file?

Yes. It did.

```

File Data: 371 bytes
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 IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n

```

2.3 After refresh, any IF_MODIFIED_SINCE?

Yes.

```

Upgrade-Insecure-Requests: 1\r\n
DNT: 1\r\n
Sec-GPC: 1\r\n
If-Modified-Since: Mon, 07 Feb 2022 06:59:01 GMT\r\n
If-None-Match: "173-5d76822ad3380"\r\n
Cache-Control: max-age=0\r\n

```

2.4 After refresh, status code and response.

Status code: Not modified

Text Data: None.

```

/text Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Mon, 07 Feb 2022 13:26:18 GMT\r\n

```

3 Long Documents

Entire output for 3rd capture is:

```

102 7.977004200 192.168.31.5 192.119.245.12 HTTP 465 GET /wirespark-labs/HTTP-wireshark-fil03.html HTTP/1.1
110 8.233066804 128.119.245.12 192.168.31.5 HTTP 655 HTTP/1.1 200 OK (text/html)

Frame 102: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface enp2s8, id 0
  Ethernet II, Src: Giga-Byt_6a:e5:c2 (fc:aa:14:6a:e5:c2), Dst: BeijingM_6c:9b:45 (9c:9d:7e:6c:9b:45)
  Internet Protocol Version 4, Src: 192.168.31.5, Dst: 128.119.245.12
  Transmission Control Protocol, Src Port: 47934, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
  Hypertext Transfer Protocol
    GET /wirespark-labs/HTTP-wireshark-fil03.html HTTP/1.1\r\n
    Host: gata.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    DNT: 1\r\n
    SEC-GPC: 1\r\n
    \r\n
    File Data: 4500 bytes
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#830000" vlink="#666633">\n
    <p><br>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
    <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <b>The Conventions of a number of the States having at the time of adopting\n

```

3.1 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?

Only One get message.

Packet Number 102. The response message from server contains it.

```

102 7.977004200 192.168.31.5 128.119.245.12 HTTP 465 GET /wirespark-labs/HTTP-wireshark-fil03.html HTTP/1.1
110 8.233066804 128.119.245.12 192.168.31.5 HTTP 655 HTTP/1.1 200 OK (text/html)

File Data: 4500 bytes
  Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#830000" vlink="#666633">\n
    <p><br>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
    <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <b>The Conventions of a number of the States having at the time of adopting\n

```

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

packet 110.

Response: Ok.

```

102 7.977004200 192.168.31.5 128.119.245.12 HTTP 465 GET /wirespark-labs/HTTP-wireshark-fil03.html HTTP/1.1
110 8.233066804 128.119.245.12 192.168.31.5 HTTP 655 HTTP/1.1 200 OK (text/html)

```

200 Ok.

```
[4 Reassembled TCP Segments (486
Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
  Date: Mon, 07 Feb 2022 13:34:
```

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

4 TCP segments.

- ▶ Transmission Control Protocol, Src
- ▶ [4 Reassembled TCP Segments (4861 b
- Hypertext Transfer Protocol

4 Documents with Embedded Objects

The capture for this part is:

Time	Source	Destination	Protocol	Length	Info
59.2.769567767	192.168.31.5	128.119.245.12	HTTP	665	GET /wireshark-labs/HTTP-wireshark-file64.html HTTP/1.1
89.2.97489431	128.119.245.12	192.168.31.5	HTTP	1367	HTTP/1.1 200 OK (text/html)
102.3.689086160	192.168.31.5	128.119.245.12	HTTP	422	GET /pearson.png HTTP/1.1
112.3.874898164	192.168.31.5	178.79.137.164	HTTP	829	GET /BE_cover_small.jpg HTTP/1.1
118.3.947885875	128.119.245.12	192.168.31.5	HTTP	389	HTTP/1.1 200 OK (png)
167.4.958255232	178.79.137.164	192.168.31.5	HTTP	237	HTTP/1.1 301 Moved Permanently
794.4.786196552	192.168.31.5	23.58.120.18	OCSP	479	Request
842.5.216755169	23.58.120.18	192.168.31.5	OCSP	955	Response

[illegible]

4.1 Number of GET requests and Where were they sent?

3 GET messages. They were sent to:

- 128.119.245.12
- 128.119.245.12
- 178.79.137.164

4.2 Images downloaded Serially or parallelly?

Parallelly. Because the GET requests for both of them were sent first and then we eventually got the response messages for the image GET requests.

```
422 GET /pearson.png HTTP/1.1
389 GET /8E_cover_small.jpg HTTP/1.1
829 HTTP/1.1 200 OK (PNG)
```

5 HTTP Authentication

The total capture for this section is:

No.	Time	Source	Destination	Protocol	Length	Info
73	0.155091150	192.168.31.5	128.119.245.12	HTTP	481	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
75	0.365584089	128.119.245.12	192.168.31.5	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
87	0.901428286	192.168.31.5	128.119.245.12	HTTP	548	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
89	0.15233214	128.119.245.12	192.168.31.5	HTTP	556	HTTP/1.1 200 OK (text/html)


```
Frame 73: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface enp2s0, id 0
Ethernet II, Src: Giga-Byt_6a:e5:c2 (fc:aa:14:6a:e5:c2), Dst: BeijingX_6c:9b:45 (0c:9d:7e:6c:9b:45)
Internet Protocol Version 4, Src: 192.168.31.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 47948, Dst Port: 80, Seq: 1, Ack: 1, Len: 415
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  \r\n
  <pre>
0000  9c 9d 7e 6c 9b 45 fc aa 14 6a e5 c2 98 00 45 00  --lE...j...E
0010  01 d3 76 0c 40 00 40 06 0d e7 c9 a8 1f 05 80 77  --v.0.0.n...w
0020  f5 9c bb 44 00 50 09 38 26 c4 cf 1e 0c 55 80 18  --D.P.8.&...U.
0030  01 f6 56 77 00 00 01 01 08 0a c2 e2 15 90 ea 8f  --V.....
0040  4d 3d 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b  =GET /w ireshark
0050  2d 6c 61 62 73 2f 79 72 6f 74 65 63 74 65 64 5f  -labs/pr otedect_
0060  70 61 67 65 73 2f 48 54 54 50 2d 77 69 72 65 73  pages/HT TP-wires
0070  68 61 72 6b 2d 66 69 6c 65 35 2e 68 74 6d 6c 20  hark-fil e5.html
0080  48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20  HTTP/1.1 - Host:
0090  67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64  gaia.cs.umass.ed
00a0  75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d  u-User- Agent: M
00b0  6f 7a 69 6c 6c 61 2f 35 2e 30 28 28 58 31 31 3b ozilla/5 .0 (X11;
```


5.1 Server's Response to Initial GET Request

Status Code: 401

Phrase: Unauthorized

```
783 HTTP/1.1 401 Unauthorized (text/html)
540 GET /wireshark-labs/protected pages/H
```

5.2 When sending the GET request for the second time, what new field was included?

Authorization was the new field.

It carries the very basic encrypted form of our username and password.

```
UNI: 1\r\n
Sec-GPC: 1\r\n
▶ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcms=\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected
```

6 About Me

Abhijit Paul

BSSE 1201

Institute of Information & Technology
University of Dhaka