

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

均为 HTTP 1.1

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

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

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

my computer: 114.214.227.222

gaia.cs.umass.edu: 128.119.245.12

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

200

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

Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT

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

128

- **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**

没有

- **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?**

没有

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

返回，可以看到返回的文件长度为 371

- **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?**

是

If-Modified-Since: Fri, 16 Sep 2022 05:59:02 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**

304 Not Modified

没有，因为内容没有修改，会直接从缓存中获取信息

- **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?**

1 HTTP GET request message

102,103,104,105 都包括

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

102

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

200 OK

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

4

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

3

128.119.245.12

128.119.245.12

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**

并行下载

第一张图片请求返回在 2.58s 而第二张图片请求在 2.54s

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

401 Unauthorized

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

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

No.	Time	Source	Destination	Protocol	Length	Info
5086	64.849906	114.214.227.222	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 5086: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61099, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 5165]
[Next request in frame: 5176]

No.	Time	Source	Destination	Protocol	Length	Info
5165	66.301946	128.119.245.12	114.214.227.222	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 5165: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 61099, Seq: 1, Ack: 513, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Fri, 16 Sep 2022 08:11:29 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT\r\n
ETag: "80-5e8c50f0c1a6a"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
[Content length: 128]
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 1.452040000 seconds]
[Request in frame: 5086]
[Next request in frame: 5176]
[Next response in frame: 5189]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n

No.	Time	Source	Destination	Protocol	Length	Info
378	4.163557	114.214.227.222	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 378: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61631, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 393]

No.	Time	Source	Destination	Protocol	Length	Info
393	4.525862	128.119.245.12	114.214.227.222	HTTP	784	HTTP/1.1 200 OK (text/html)

Frame 393: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 61631, Seq: 1, Ack: 513, Len: 730
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 16 Sep 2022 08:45:17 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT\r\n
ETag: "173-5e8c50f0c0eb2"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
[Content length: 371]
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.362305000 seconds]
[Request in frame: 378]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\n<html>\n\nCongratulations again! Now you've downloaded the file lab2-2.html.
\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy
\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\nfield in your browser's HTTP GET request to the server.\n\n</html>\n

No.	Time	Source	Destination	Protocol	Length	Info
2603	27.667653	114.214.227.222	128.119.245.12	HTTP	678	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 2603: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61632, Dst Port: 80, Seq: 1, Ack: 1, Len: 624
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
If-None-Match: "173-5e8c50f0c0eb2"\r\n
If-Modified-Since: Fri, 16 Sep 2022 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 2642]

No.	Time	Source	Destination	Protocol	Length	Info
2642	27.941084	128.119.245.12	114.214.227.222	HTTP	294	HTTP/1.1 304 Not Modified

Frame 2642: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 61632, Seq: 1, Ack: 625, Len: 240
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
[HTTP/1.1 304 Not Modified\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Fri, 16 Sep 2022 08:45:41 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-5e8c50f0c0eb2"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.273431000 seconds]
[Request in frame: 2603]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```
No.      Time      Source      Destination      Protocol Length Info
 74 2.542365 114.214.227.222 128.119.245.12 HTTP 566 GET /wireshark-labs/HTTP-wireshark-
file3.html HTTP/1.1
Frame 74: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61844, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file3.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/
537.36 Edg/105.0.1343.33\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
  [HTTP request 1/1]
  [Response in frame: 105]
No.      Time      Source      Destination      Protocol Length Info
 105 2.803738 128.119.245.12 114.214.227.222 HTTP 535 HTTP/1.1 200 OK (text/html)
Frame 105: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 61844, Seq: 4381, Ack: 513, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #102(1460), #103(1460), #104(1460), #105(481)]
  [Frame: 102, payload: 0-1459 (1460 bytes)]
  [Frame: 103, payload: 1460-2919 (1460 bytes)]
  [Frame: 104, payload: 2920-4379 (1460 bytes)]
  [Frame: 105, payload: 4380-4860 (481 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203136205365702032...]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Fri, 16 Sep 2022 09:00:12 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT\r\n
  ETag: "1194-5e8c50f0bc091"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 4500\r\n
    [Content length: 4500]
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.261373000 seconds]
  [Request in frame: 74]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.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="#330000" vlink="#666633">\n
```

<p>
\n</p>\n<p></p><center>THE BILL OF RIGHTS
\nAmendments 1-10 of the Constitution\n</center>\n\n<p>The Conventions of a number of the States having, at the time of adopting\nthe Constitution, expressed a desire, in order to prevent misconstruction\nor abuse of its powers, that further declaratory and restrictive clauses\nshould be added, and as extending the ground of public confidence in the\nGovernment will best insure the beneficent ends of its institution; </p><p> Resolved, by the Senate and House of Representatives of the United\nStates of America, in Congress assembled, two-thirds of both Houses concurring,\nthat the following articles be proposed to the Legislatures of the several\nStates, as amendments to the Constitution of the United States; all or any\nof which articles, when ratified by three-fourths of the said Legislatures,\nto be valid to all intents and purposes as part of the said Constitution,\nnamely: </p><p><h3>Amendment I</h3>\n\n<p></p><p>Congress shall make no law respecting an establishment of\nreligion, or prohibiting the free exercise thereof; or\nabridging the freedom of speech, or of the press; or the\nright of the people peaceably to assemble, and to petition\nthe government for a redress of grievances.\n\n<p><p><h3>Amendment II</h3>\n\n<p></p><p>A well regulated militia, being necessary to the security\nof a free state, the right of the people to keep and bear\narms, shall not be infringed.\n\n<p><p><h3>Amendment III</h3>\n\n<p></p><p>No soldier shall, in time of peace be quartered in any house,\nwithout the consent of the owner, nor in time of war, but\nin a manner to be prescribed by law.\n\n<p><p><h3>Amendment IV</h3>\n\n<p></p><p>The right of the people to be secure in their persons, houses,\npapers, and effects, against unreasonable searches and seizures,\nshall not be violated, and no warrants shall issue, but upon\nprobable cause, supported by oath or affirmation, and\nparticularly describing the place to be searched, and the\npersons or things to be seized.\n\n<p><p><h3>Amendment V</h3>\n\n<p></p><p>No person shall be held to answer for a capital, or otherwise\ninfamous crime, unless on a presentment or indictment of a grand\njury, except in cases arising in the land or naval forces,\nor in the militia, when in actual service in time of war\nor public danger; nor shall any person be subject for the\nsame offense to be twice put in jeopardy of life or limb;\nnor shall be compelled in any criminal case to be a witness\nagainst himself, nor be deprived of life, liberty, or property,\nwithout due process of law; nor shall private property be\ntaken for public use, without just compensation.\n\n<p><p><h3>Amendment VI</h3>\n\n<p></p><p>In all criminal prosecutions, the accused shall enjoy the right\n to a speedy and public trial, by an impartial jury of the state\nand district wherein the crime shall have been committed, which\ndistrict shall have been previously ascertained by law, and\nto be informed of the nature and cause of the accusation;\nto be confronted with the witnesses against him; to have\ncompulsory process for obtaining witnesses in his favor,\nand to have the assistance of counsel for his defense.\n\n<p><p><h3>Amendment VII</h3>\n\n<p></p><p>In suits at common law, where the value in controversy shall\nexceed twenty dollars, the right of trial by jury shall be\npreserved, and no fact tried by a jury, shall be otherwise\nreexamined in any court of the United States, than according\nto the rules of the common law.\n

\n
</p><p><h3>Amendment VIII</h3>\n
\n
<p></p><p>Excessive bail shall not be required, nor excessive fines\nimposed, nor cruel and unusual punishments inflicted.\n
\n
</p><p><h3>Amendment IX</h3>\n
\n
<p></p><p>The enumeration in the Constitution, of certain rights, shall\nnot be construed to deny or disparage others retained by the people.\n
\n
</p><p><h3>Amendment X</h3>\n
\n
<p></p>\n
<p>The powers not delegated to the United States by the Constitution, nor prohibited \nby it to the states, are reserved to the states respectively, or to the people.</p>\n</body></html>

```

No.      Time      Source      Destination      Protocol Length Info
 54 1.903245 114.214.208.164 128.119.245.12 HTTP 533 GET /wireshark-labs/HTTP-wireshark-
file4.html HTTP/1.1
Frame 54: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.208.164, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62565, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol

No.      Time      Source      Destination      Protocol Length Info
 61 2.254444 128.119.245.12 114.214.208.164 HTTP 1355 HTTP/1.1 200 OK (text/html)
Frame 61: 1355 bytes on wire (10840 bits), 1355 bytes captured (10840 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.208.164
Transmission Control Protocol, Src Port: 80, Dst Port: 62565, Seq: 1, Ack: 480, Len: 1301
Hypertext Transfer Protocol
Line-based text data: text/html (23 lines)

No.      Time      Source      Destination      Protocol Length Info
 63 2.284653 114.214.208.164 128.119.245.12 HTTP 479 GET /pearson.png HTTP/1.1
Frame 63: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.208.164, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62565, Dst Port: 80, Seq: 480, Ack: 1302, Len: 425
Hypertext Transfer Protocol

No.      Time      Source      Destination      Protocol Length Info
 71 2.547314 114.214.208.164 178.79.137.164 HTTP 446 GET /8E_cover_small.jpg HTTP/1.1
Frame 71: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.208.164, Dst: 178.79.137.164
Transmission Control Protocol, Src Port: 62567, Dst Port: 80, Seq: 1, Ack: 1, Len: 392
Hypertext Transfer Protocol

No.      Time      Source      Destination      Protocol Length Info
 78 2.585452 128.119.245.12 114.214.208.164 HTTP 745 HTTP/1.1 200 OK (PNG)
Frame 78: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.208.164
Transmission Control Protocol, Src Port: 80, Dst Port: 62565, Seq: 4222, Ack: 905, Len: 691
[3 Reassembled TCP Segments (3611 bytes): #76(1460), #77(1460), #78(691)]
Hypertext Transfer Protocol
Portable Network Graphics

No.      Time      Source      Destination      Protocol Length Info
 110 2.798209 178.79.137.164 114.214.208.164 HTTP 225 HTTP/1.1 301 Moved Permanently
Frame 110: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 178.79.137.164, Dst: 114.214.208.164
Transmission Control Protocol, Src Port: 80, Dst Port: 62567, Seq: 1, Ack: 393, Len: 171
Hypertext Transfer Protocol

```

No. Time Source Destination Protocol Length Info
177 1.821132 114.214.227.222 128.119.245.12 HTTP 545 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1

Frame 177: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0

Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)

Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 531
Identification: 0x9f85 (40837)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 114.214.227.222
Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 50363, Dst Port: 80, Seq: 1, Ack: 1, Len: 491

Hypertext Transfer Protocol

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 201]

No. Time Source Destination Protocol Length Info
201 2.080870 128.119.245.12 114.214.227.222 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)

Frame 201: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-B4CB-6B8F87A64AB6}, id 0

Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 757
Identification: 0x701d (28701)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 32
Protocol: TCP (6)
Header Checksum: 0x1bad [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 114.214.227.222

Transmission Control Protocol, Src Port: 80, Dst Port: 50363, Seq: 1, Ack: 492, Len: 717

Hypertext Transfer Protocol

HTTP/1.1 401 Unauthorized\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
Response Version: HTTP/1.1
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
Date: Fri, 16 Sep 2022 14:14:28 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
WWW-Authenticate: Basic realm="wireshark-students only"\r\n
Content-Length: 381\r\n
[Content length: 381]
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 1/1]

```
[Time since request: 0.259738000 seconds]
[Request in frame: 177]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
File Data: 381 bytes
Line-based text data: text/html (12 lines)
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
<html><head>\n
<title>401 Unauthorized</title>\n
</head><body>\n
<h1>Unauthorized</h1>\n
<p>This server could not verify that you\n
are authorized to access the document\n
requested. Either you supplied the wrong\n
credentials (e.g., bad password), or your\n
browser doesn't understand how to supply\n
the credentials required.</p>\n
</body></html>\n
No.      Time            Source            Destination      Protocol Length Info
 901 10.591197      114.214.227.222   128.119.245.12   HTTP      630      GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 901: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.227.222, Dst: 128.119.245.12
 0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 616
Identification: 0x9f8b (40843)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 114.214.227.222
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 51964, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcms=\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/
537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/2]
[Response in frame: 945]
[Next request in frame: 947]
No.      Time            Source            Destination      Protocol Length Info
 945 10.866822      128.119.245.12    114.214.227.222   HTTP      544      HTTP/1.1 200 OK (text/html)
Frame 945: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{493C4AC5-6E7E-4816-
B4CB-6B8F87A64AB6}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_3e:5e:86 (a4:b1:c1:3e:5e:86)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.227.222
 0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 530
Identification: 0x89c2 (35266)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 33
Protocol: TCP (6)
Header Checksum: 0x01eb [validation disabled]
[Header checksum status: Unverified]
```

```
Source Address: 128.119.245.12
Destination Address: 114.214.227.222
Transmission Control Protocol, Src Port: 80, Dst Port: 51964, Seq: 1, Ack: 577, Len: 490
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Fri, 16 Sep 2022 14:14:36 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Fri, 16 Sep 2022 05:59:02 GMT\r\n
  ETag: "84-5e8c50f0c2df2"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 132\r\n
    [Content length: 132]
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.275625000 seconds]
[Request in frame: 901]
[Next request in frame: 947]
[Next response in frame: 964]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
File Data: 132 bytes
Line-based text data: text/html (6 lines)
\r\n
<html>\r\n
\r\n
This page is password protected!  If you're seeing this, you've downloaded the page correctly <br>\r\n
Congratulations!\r\n
</html>
```