计网 HTTP 抓包实验

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   1.1； 1.1
2. What languages (if any) does your browser indicate that it can accept to the server?
   zh-Hans-CN;zh-Hans
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   10.132.1.247;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?
   Wed, 06 Nov 2019 06:59:02 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.
   HTTP 请求报文中还有 Host 字段、connection 字段、Accept 字段、User-agent 字段、Accept-Encoding 字段等
   HTTP 响应报文还有 server、connection、ETag、Date 等字段

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Wed, 13 Nov 2019 02:16:28 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.
  Last-Modified: Tue, 12 Nov 2019 06:59:04 GMT\r\n
  ETag: "80-59720c89fd24d"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
  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: 0.319938000 seconds]
  [Request in frame: 34]
  [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
34	4.504350	10.132.12.102	128.119.245.12	HTTP	377	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
44	4.824288	128.119.245.12	10.132.12.102	HTTP	540	HTTP/1.1 200 OK (text/html)
57	5.240106	10.132.12.102	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
63	5.864112	128.119.245.12	10.132.12.102	HTTP	539	HTTP/1.1 404 Not Found (text/html)

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?

没有这个字段，因为浏览器首次获取该页面。

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   明确返回了，从 Line-based text data 可看出
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?
    有那个字段了。信息是：Wed, 06 Nov 2019 06:59:02 GMT，是上次访问网站的最新修改时间。
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，表示未修改，没有返回页面的内容，因为没有修改，浏览器已缓存。

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
  Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: Keep-Alive\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: 43]
```

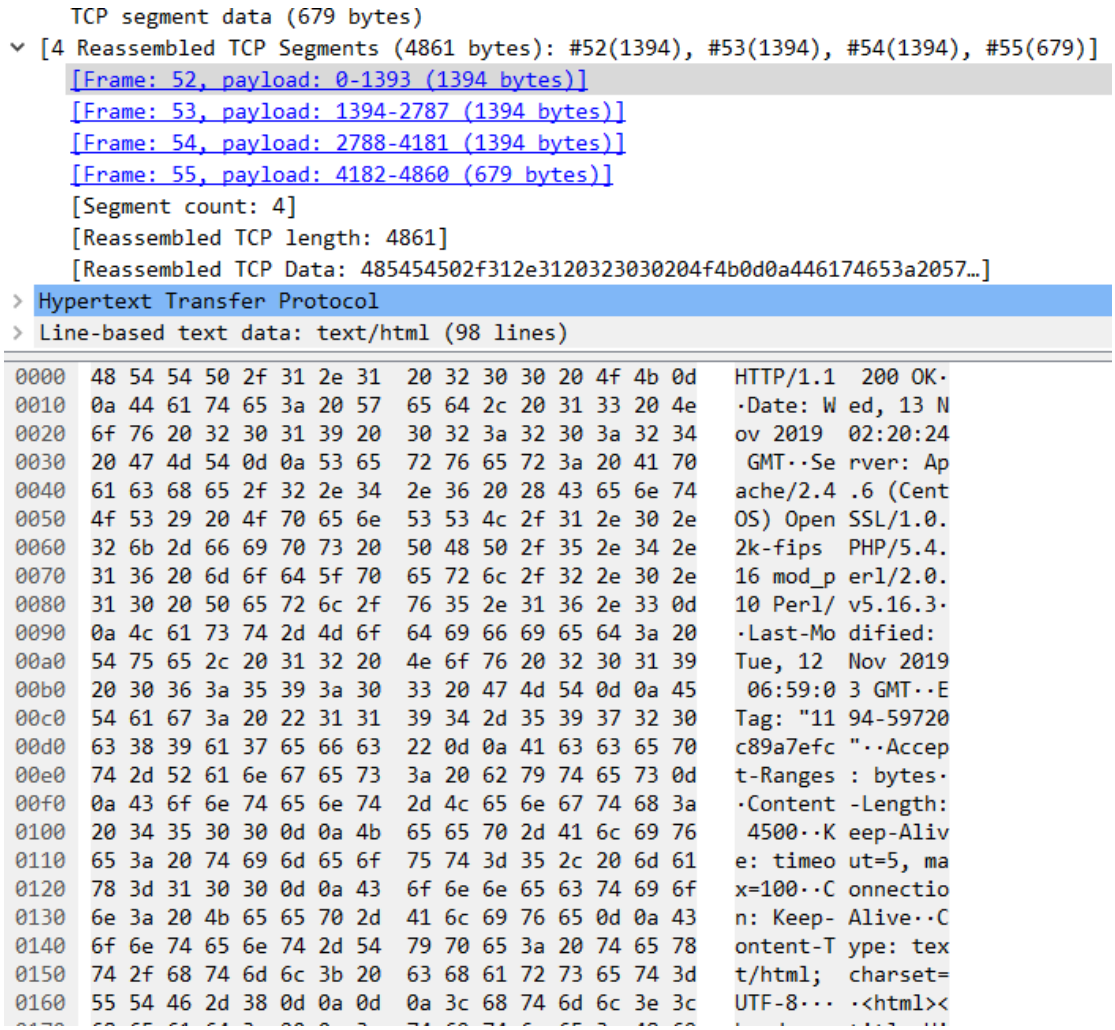
```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Wed, 13 Nov 2019 02:18:59 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Last-Modified: Tue, 12 Nov 2019 06:59:04 GMT\r\n
  ETag: "173-59720c89f266c"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
  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: 0.416043000 seconds]
  [Request in frame: 35]
  [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
  \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
```

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
  Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: gaia.cs.umass.edu\r\n
  If-Modified-Since: Tue, 12 Nov 2019 06:59:04 GMT\r\n
  If-None-Match: "173-59720c89f266c"\r\n
  Connection: Keep-Alive\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: 68]
```

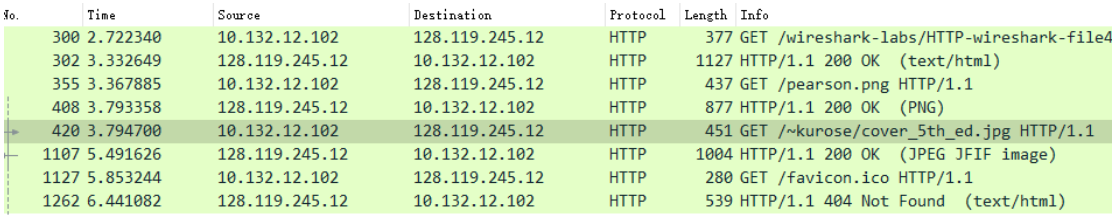
```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Wed, 13 Nov 2019 02:29:13 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-59720c89f266c"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.328523000 seconds]
  [Request in frame: 65]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

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?
    1; #52(1394)
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    #52(1394)
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 个数据段

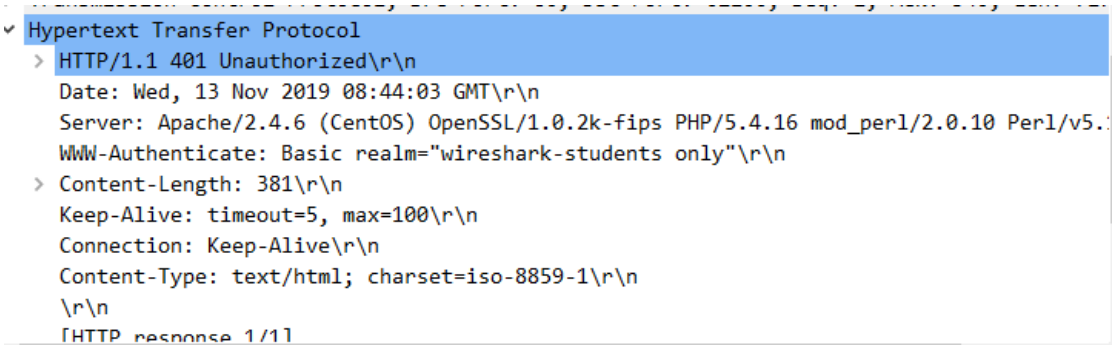
No.	Time	Source	Destination	Protocol	Length	Info
49	3.191497	10.132.12.102	128.119.245.12	HTTP	377	GET /wireshark-labs/HTTP-wireshark-file
55	3.494441	128.119.245.12	10.132.12.102	HTTP	733	HTTP/1.1 200 OK (text/html)
78	3.895505	10.132.12.102	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
95	4.209614	128.119.245.12	10.132.12.102	HTTP	539	HTTP/1.1 404 Not Found (text/html)

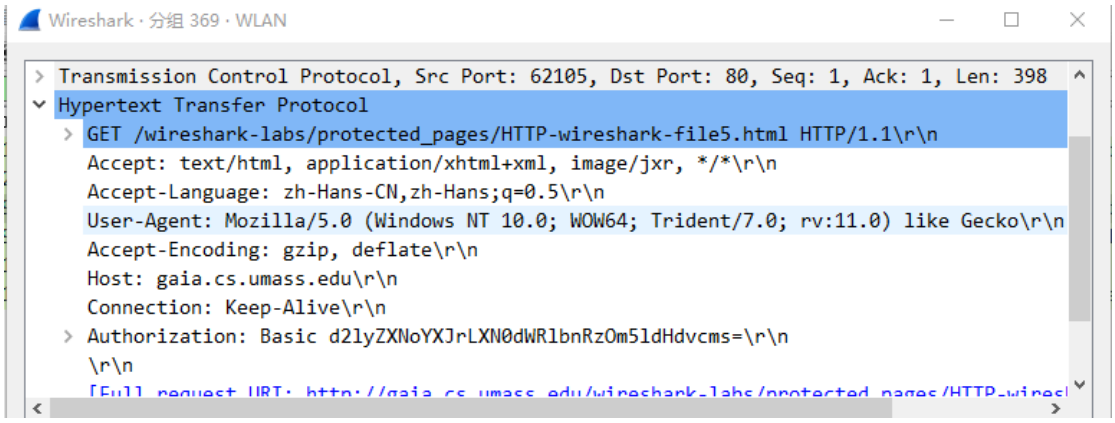


16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    3(出现 4 个有一个是获取.ico 文件)；128.119.245.12
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
    不是并发下载的，因为请求是先后到达的，所获取的对象也是先后到达的



18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
    401，未授权，授权访问
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    新出现了一个字段，Authorization


Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
Date: Wed, 13 Nov 2019 08:44:03 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.
WWW-Authenticate: Basic realm="wireshark-students only"\r\n
Content-Length: 381\r\n
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]


Wireshark · 分组 369 · WLAN
Transmission Control Protocol, Src Port: 62105, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
\r\n