思考题解答

1. HTTP1.1

```
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/201
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
```

2. 中文-大陆 中文-台湾 中文-香港，英文

```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
```

3. 本地IP:114.214.252.245 目的主机IP:128.119.245.12

Source	Destination
114.214.252.245	128.119.245.12

4. 200

```
17.423207    128.119.245.12    114.214.252.245    HTTP    540 HTTP/1.1 200 OK  (text/html)
```

5. `Last-Modified: Fri, 13 Nov 2020 06:58:01 GMT\r\n`

6.
```
Frame Length: 540 bytes (4320 bits)
Capture Length: 540 bytes (4320 bits)
```

7. context_length

8. 没有

```
[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/86.0.4240.193 Safari/537.36 Edg/86.0.622.68\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
```

9. yes

```
tml>··Co ngratula
tions ag ain!  No
w you've  downloa
ded the  file lab
2-2.html . <br>·T
his file 's last
modifica tion dat
e will n ot chang
```

10.有

```
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/86.0.4240.193 Safari/537.36 Edg/86.0.622.68\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: "173-5b3f78ca1489f"\r\n
If-Modified-Since: Fri, 13 Nov 2020 06:58:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
```

是一个空行，下面是传输的数据，完整的URL

11.

```
    [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 304
  [Status Code Description: Not Modified]
  Response Phrase: Not Modified
Date: Fri, 13 Nov 2020 12:50:15 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 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: "173-5b3f78ca1489f"\r\n
```

304 没有修改，表示对象在给定时间之后没有修改

12. 两次

```
500 GET /favicon.ico HTTP/1.1
 54 58328 → 80 [ACK] Seq=447 Ack=486 Win=130816 Len=0
 54 58328 → 80 [ACK] Seq=447 Ack=487 Win=130816 Len=0
 54 58328 → 80 [FIN, ACK] Seq=447 Ack=487 Win=130816 Len=0
681 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
```

13. 三个

```
2054 39.906121   128.119.245.12   114.214.252.245   TCP    1514 80 → 54161 [AC
2055 39.906121   128.119.245.12   114.214.252.245   TCP    1514 80 → 54161 [AC
2056 39.906121   128.119.245.12   114.214.252.245   TCP    1514 80 → 54161 [AC
```

14. 200

```
128.119.245.12   114.214.252.245   HTTP   535 HTTP/1.1 200 OK  (text/html)
```

15. 没有，观察报文内容可以发现，所有报文内容一次性全部返回，context_length较长

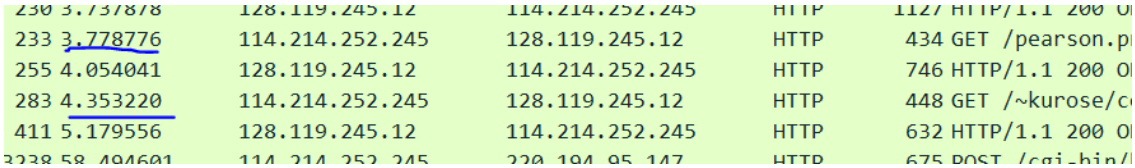
```
File Data: 4500 bytes
ine-based text data: text/html (98 lines)
```

```
0  74 65 73 20 62 79 20 74  68 65 20 43 6f 6e 73 74   tes by t he Const
0  69 74 75 74 69 6f 6e 2c  20 6e 6f 72 20 70 72 6f   itution,  nor pro
0  68 69 62 69 74 65 64 20  0a 20 20 62 79 20 69 74   hibited ·  by it
0  20 74 6f 20 74 68 65 20  73 74 61 74 65 73 2c 20    to the  states,
0  61 72 65 20 72 65 73 65  72 76 65 64 20 74 6f 20   are rese rved to
0  74 68 65 20 73 74 61 74  65 73 20 72 65 73 70 65   the stat es respe
0  63 74 69 76 65 6c 79 2c  20 6f 72 20 74 6f 20 74   ctively,  or to t
0  68 65 20 70 65 6f 70 6c  65 2e 3c 2f 70 3e 0a 3c   he peopl e.</p>·<
0  2f 62 6f 64 79 3e 3c 2f  68 74 6d 6c 3e             /body></ html>
```

16. 三个get，第一个Get对html获取，剩下两个get对两个图片对象进行获取

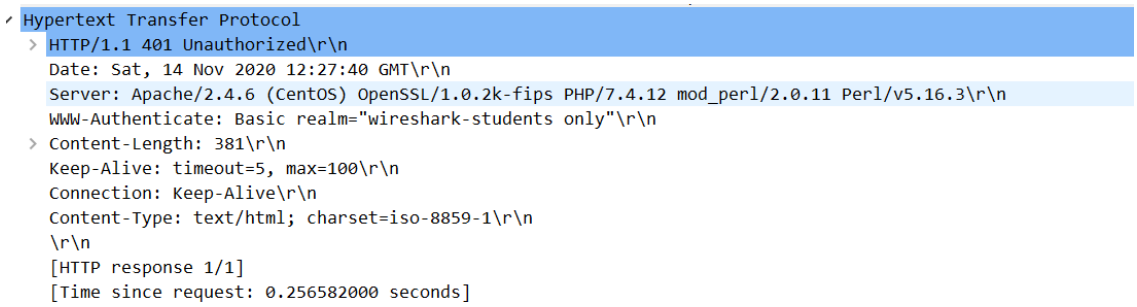
```
14 3.475285   114.214.252.245   128.119.245.12   HTTP   477 GET /wireshark-
30 3.737878   128.119.245.12   114.214.252.245   HTTP  1127 HTTP/1.1 200 OK
33 3.778776   114.214.252.245   128.119.245.12   HTTP   434 GET /pearson.pn
55 4.054041   128.119.245.12   114.214.252.245   HTTP   746 HTTP/1.1 200 OK
83 4.353220   114.214.252.245   128.119.245.12   HTTP   448 GET /~kurose/co
11 5.179556   128.119.245.12   114.214.252.245   HTTP   632 HTTP/1.1 200 OK
```

17. 可以根据时间判断



可以根据时间判断，因为两个对象请求的时间不相同，存在明显的先后顺序，不可能是并行的

18. initial responce



这个响应的含义是告诉用户，GET已经正常收到，返回的报文告诉我们没有权限访问这个服务器

19. 观察wireshark报文，可以发现请求报文中多了一项