****



**Wireshark Lab: WireShark HTTP实验报告**

**学院： 智能与计算学部**

**专业： 计算机科学与技术**

**姓名： 陈秋澄**

**学号： 3022244290**

**2024年3月15日**

**The Basic HTTP GET/response interaction:**

按照要求访问：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

使用WireShark Capture到的信息如下：

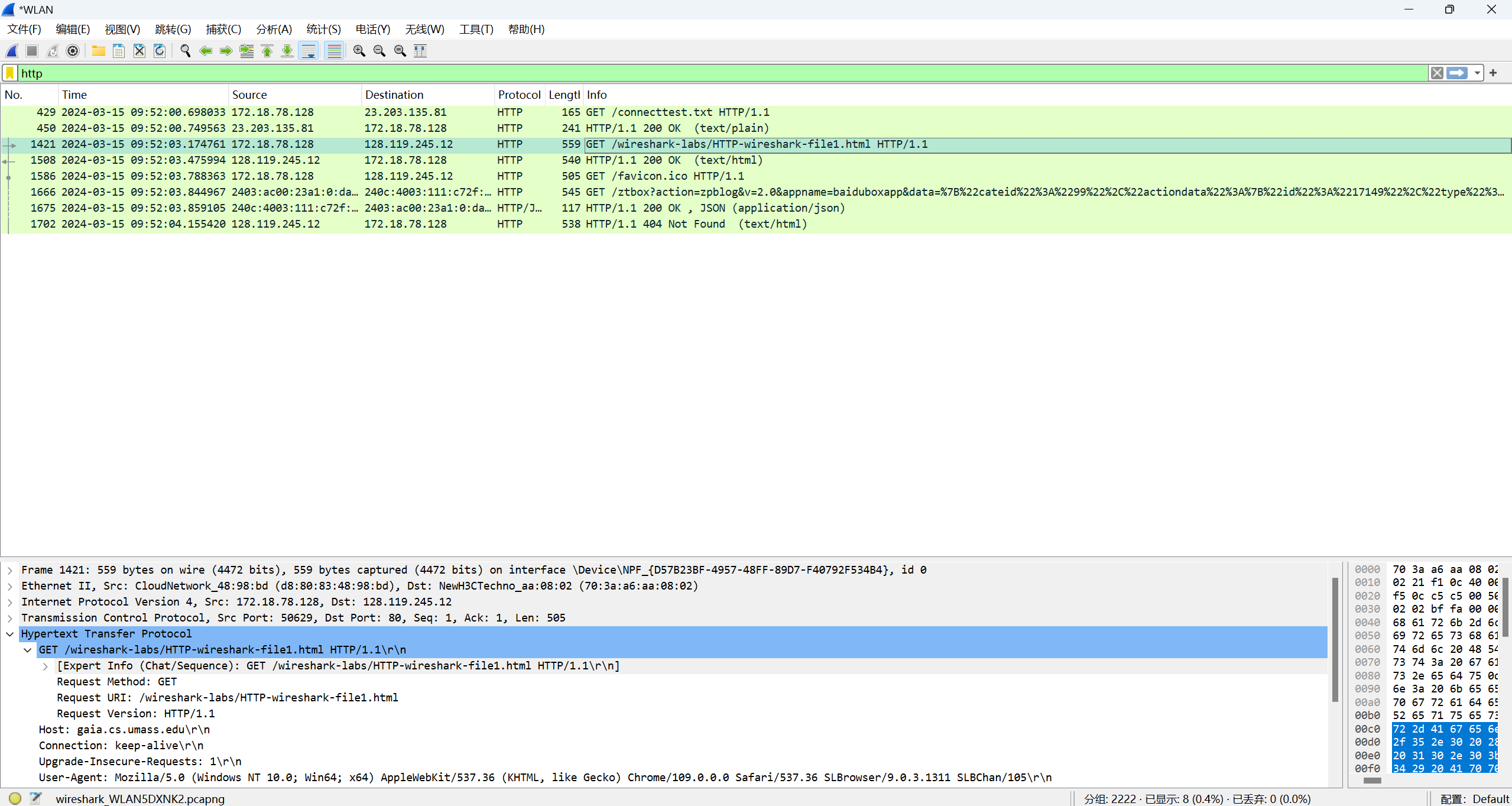


图1 采集到的信息之问题佐证

下面，我将根据自己的 Wireshark 实验回答以下四个问题：

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

我的浏览器运行的HTTP版本是1.1；服务器运行的HTTP版本是1.1。从GET信息中和封包列表中Info可以看到。如下图2图3：

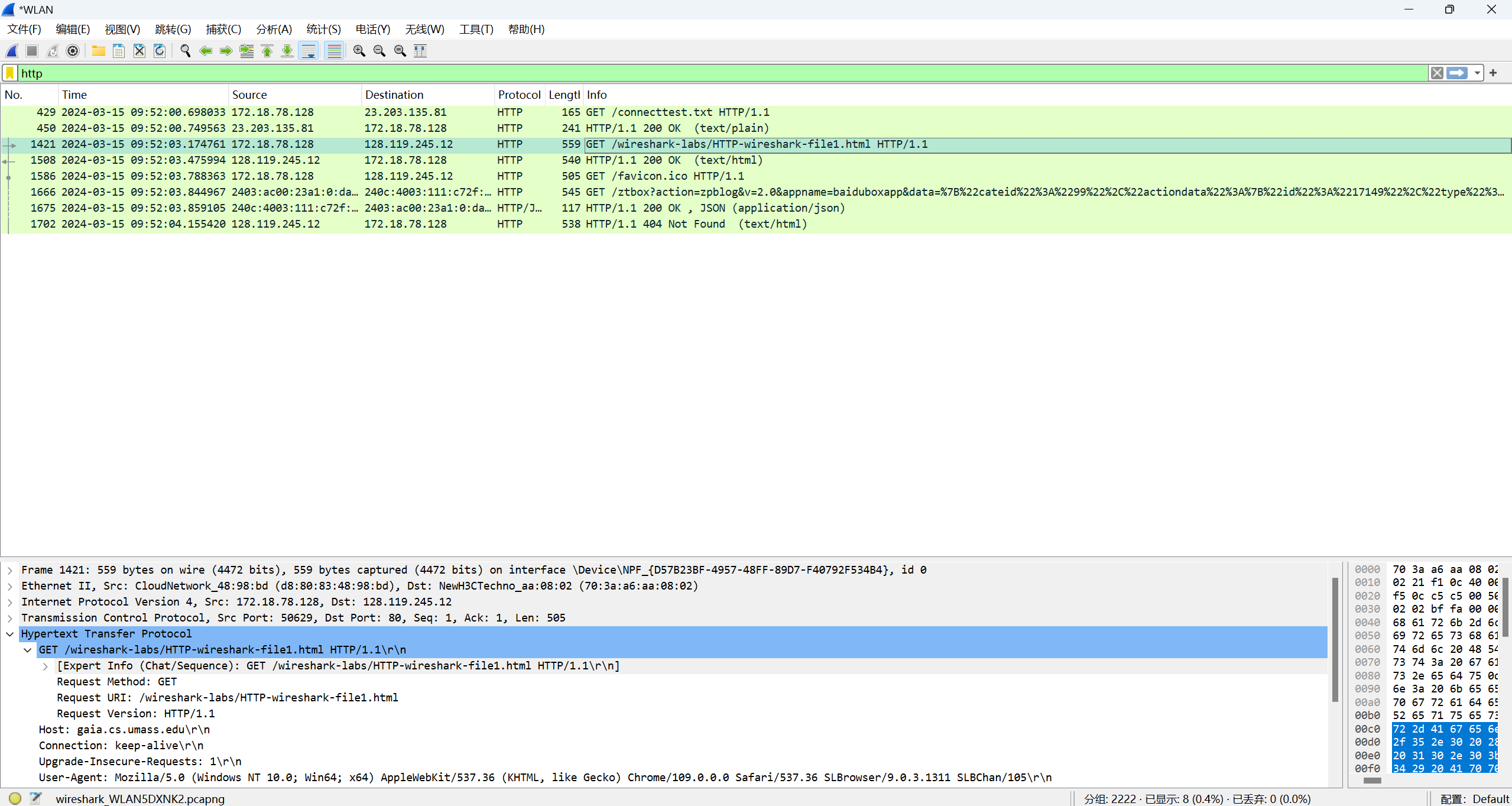


图2 问题1佐证

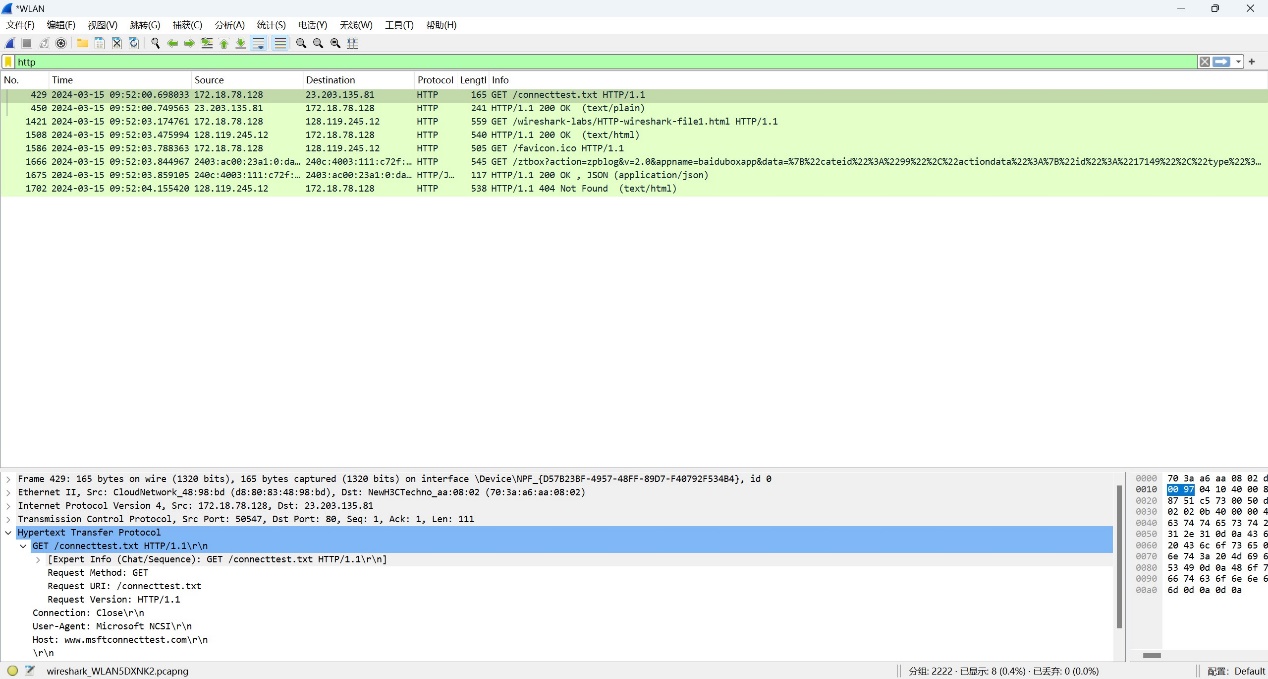


图3 问题1佐证

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

zh-CN, zh, 即：中文与简体中文，在Accept Language中可获得。

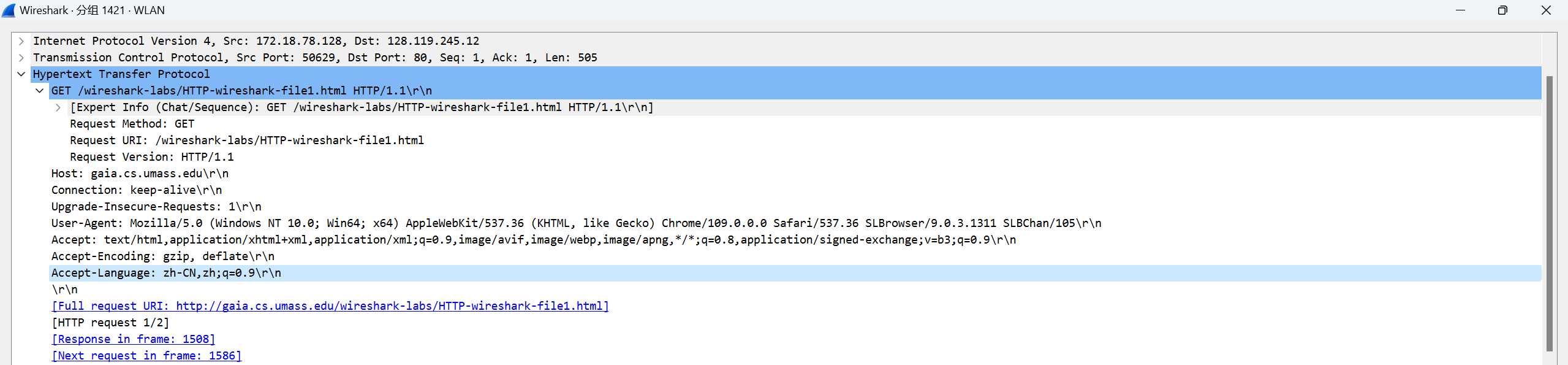


图4 问题2佐证

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

我们选取Source和Destination交叉对应一致且为题中要求的两组。

从封包列表中的Source和Destination可以看到IP地址，如下图5所示：

我的电脑的网络地址为：172.18.78.128。

gaia.cs.umass.edu的网络地址为：128.119.245.12；

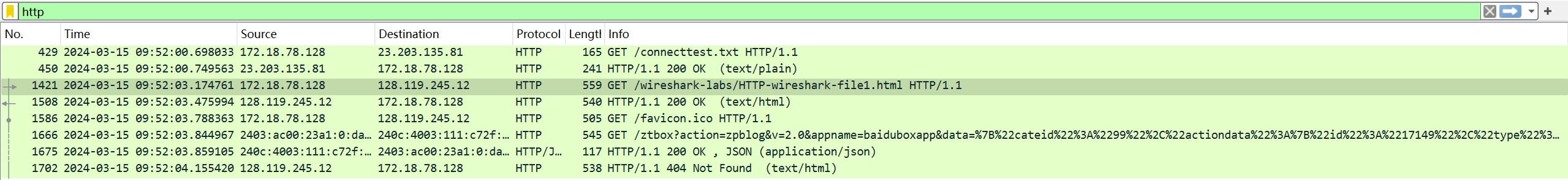


图5 问题 3佐证

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

Server 发送到我的browser的Status Code为200。

从Status Code处可以获取，如下图6所示：

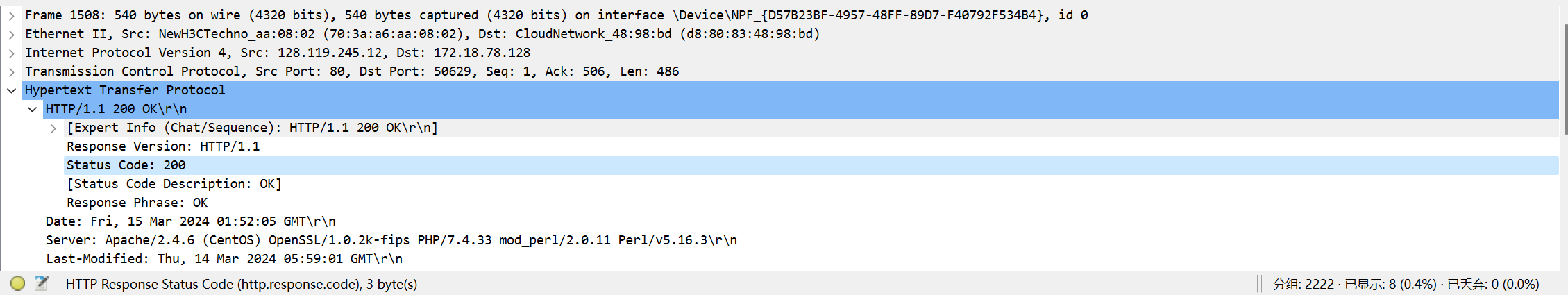


图6 问题4佐证

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

2024年3月14日星期一，05:59:01。

从Last-Modified处可以获得，如下图7所示：

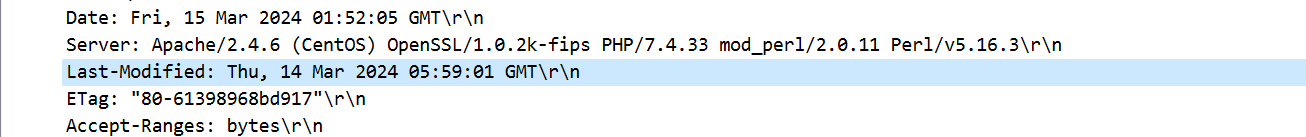


图7 问题5佐证

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

128 bytes。

我们从File Data处可以获得，如下图所示：

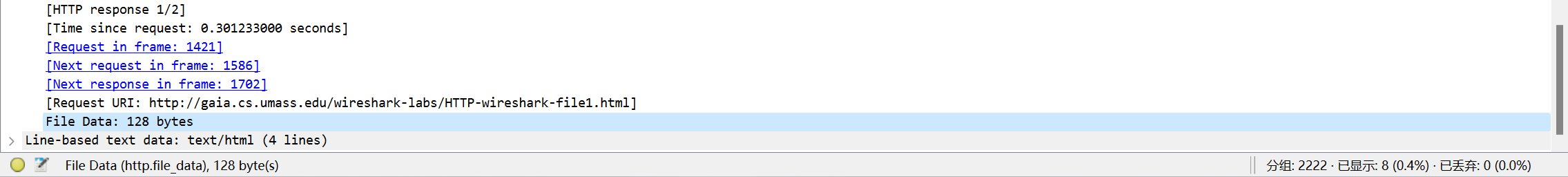


图8 问题6佐证

**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.**

有， 比如TCP, DNS。如下图9所示：

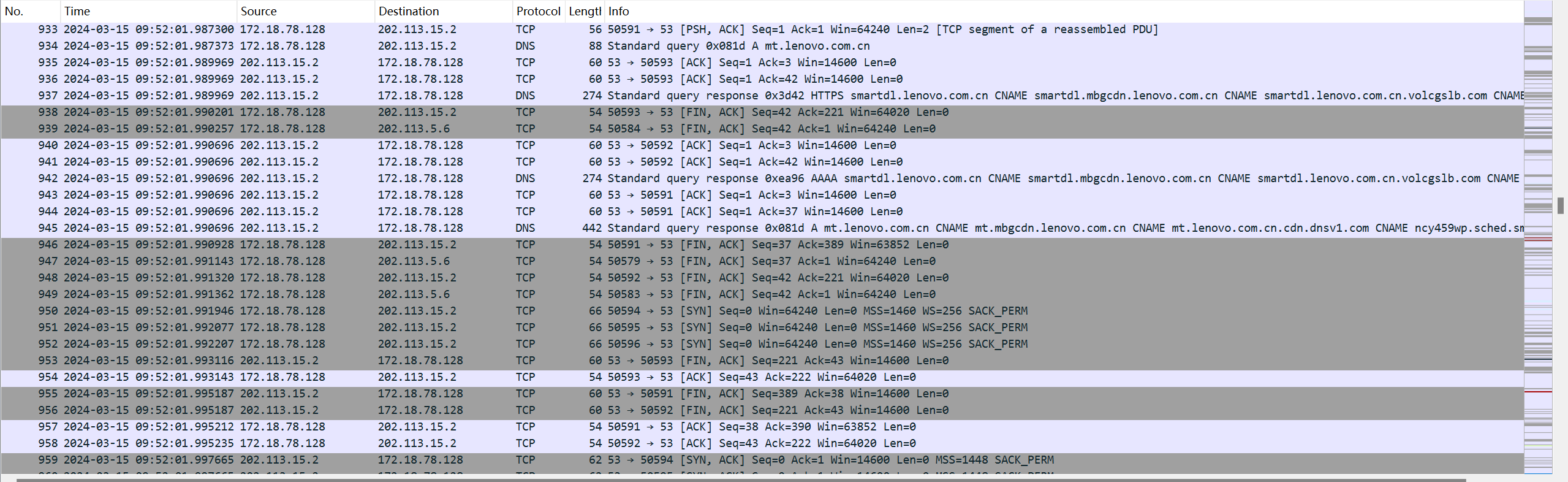


图9 问题7佐证

**The HTTP CONDITIONAL GET/response interaction：**

**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?**

在第一个GET中没有 "IF-MODIFIED-SINCE "，因为这是浏览器首次获取该页面，在缓存中并没有相应内容，"IF-MODIFIED-SINCE "行是由浏览器会向服务器传送的。如图10：

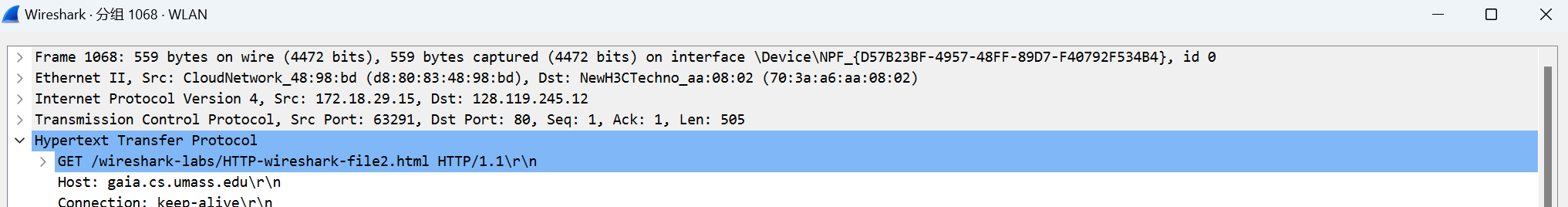
****

图10 问题8佐证

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

报文中明确地返回了文件的内容。

报文中说明了文件的大小，文件的格式，以及返回了文件的具体内容。如下图所示：

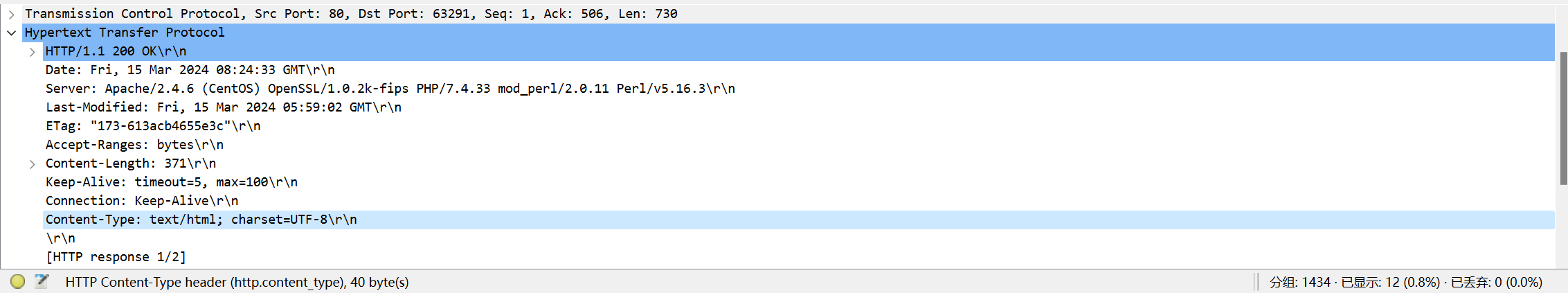
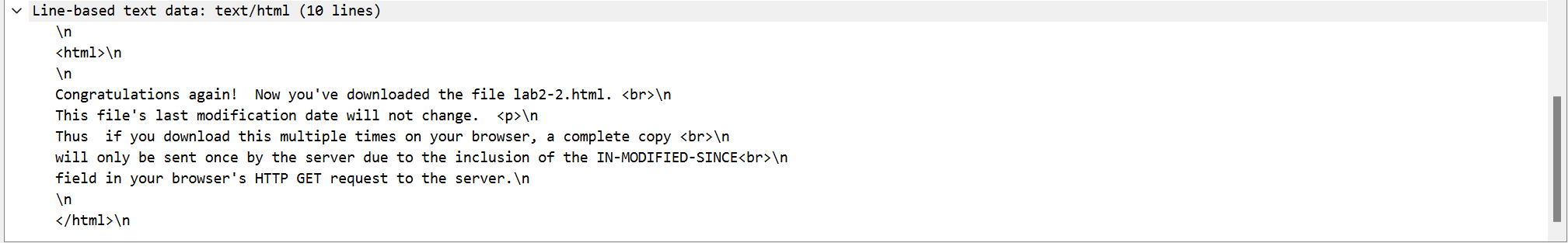
 

图11 问题9佐证

**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?**

在第二个GET中有"IF-MODIFIED-SINCE "行，"IF-MODIFIED-SINCE :"的信息是我本地浏览器存储的文件最后修改时间。如下图12所示：

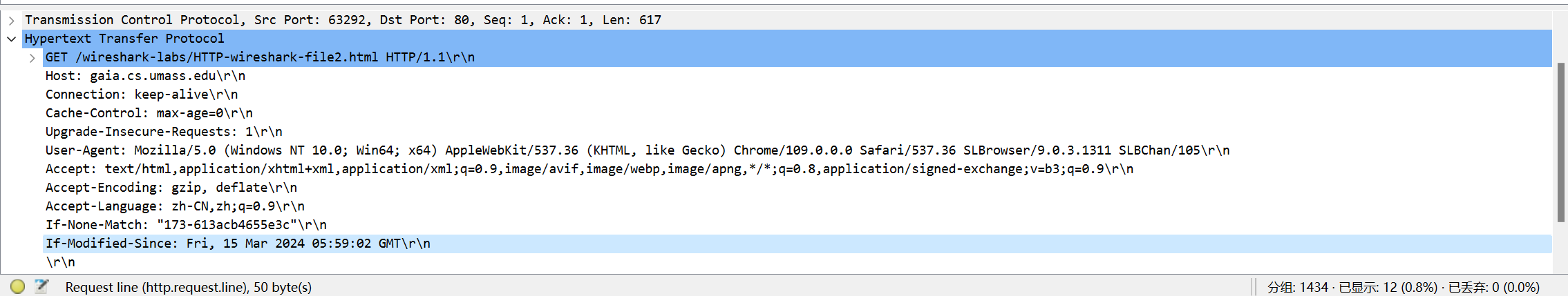


图12 问题10佐证

**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.**

响应第二个GET的status code和phrase分别为：304 “Not Modified”。Server灭有明确地返回文件内容，因为在第一次访问之后，该网站已经进入到了浏览器的缓存中，且在第二次访问之前没有被修改，第二次请求直接会从浏览器的缓存冲取出然后返回，不会再次通过server传输一份重复的文件。有利于提高响应速度。

如下图13所示：



图13 问题11佐证

**Retrieving Long Documents：**

按照要求访问：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

使用WireShark Capture到的信息如下：

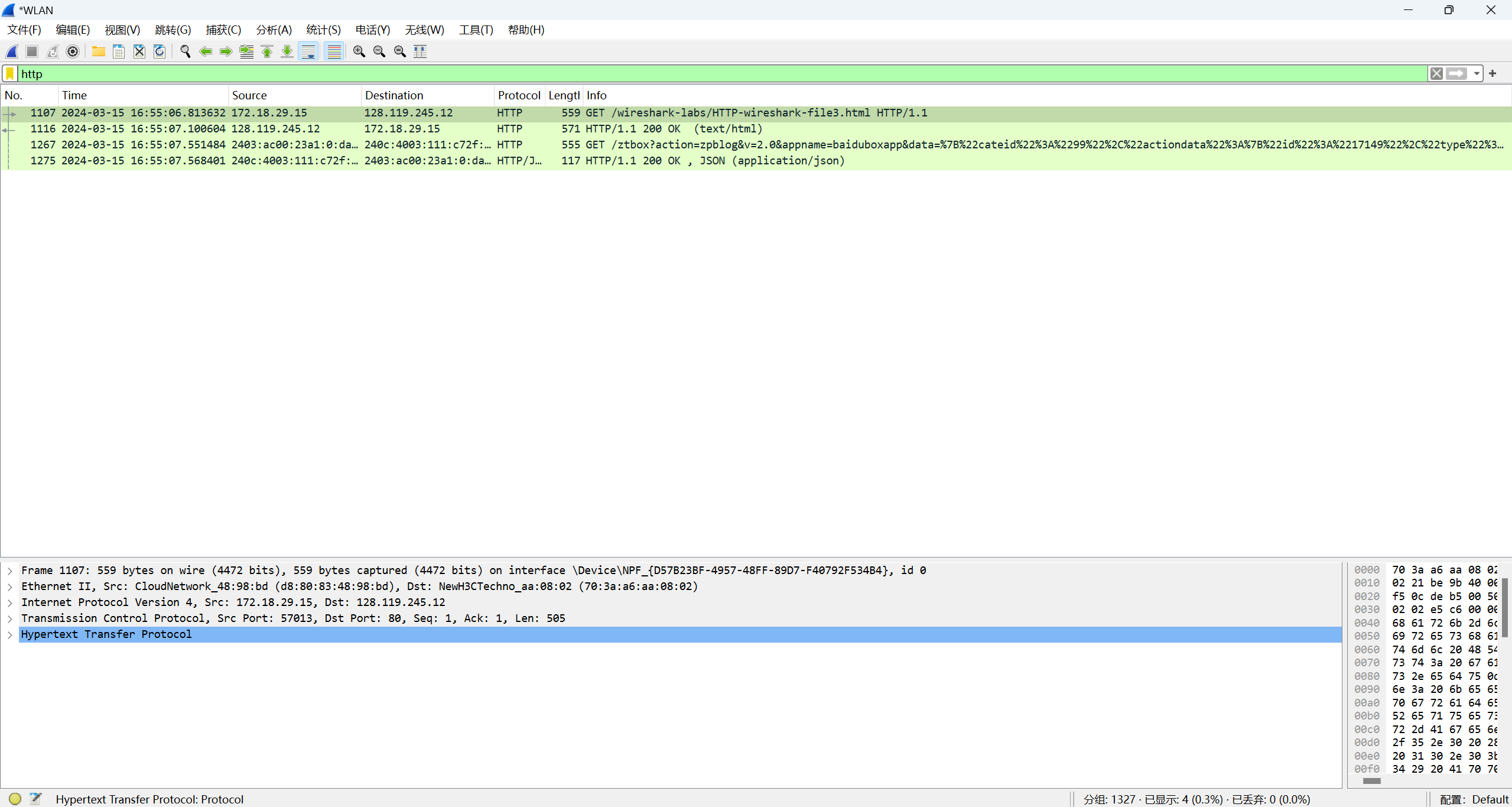


图14 Retrieving Long Documents佐证

**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?**

我的browser发送了1个HTTP GET请求。包含请求权利法案的GET信息的packet的number是1107。如下图所示：

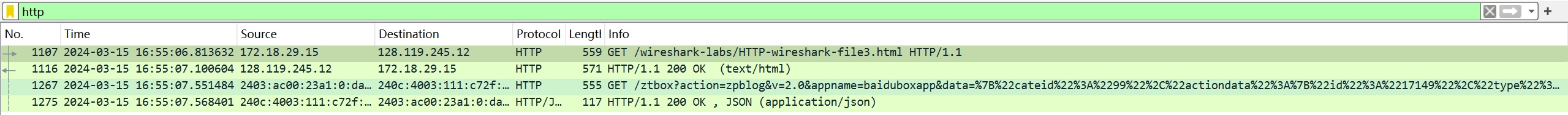


图15 问题12佐证

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

相关编号的packet包含了与HTTP GET请求相关的status code和phrase。我的browser收到的第一个包是编号1116，点击并查看其信息发现了其包含了HTTP GET相关的信息。如图16所示：

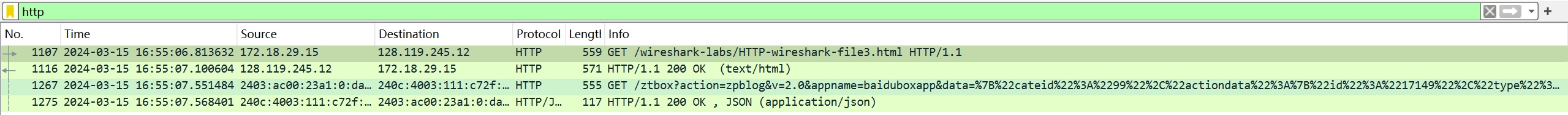


图16 问题13佐证a

详细内容如图17：

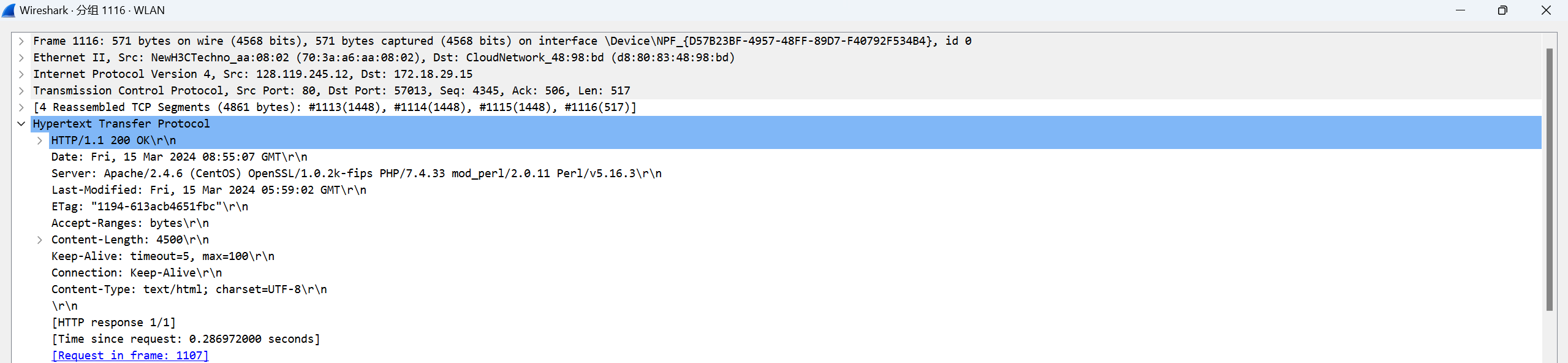


图17 问题13佐证b

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

响应的status code 和phrase分别为：200 “OK”。 如图18所示：

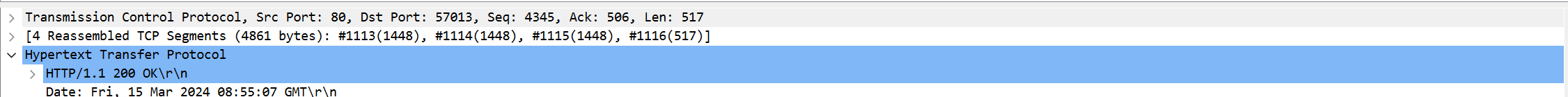


图18 问题14佐证

**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，由下图可以看出有四个TCP段号，所以需要四个TCP段来传输单个HTTP响应的数据。

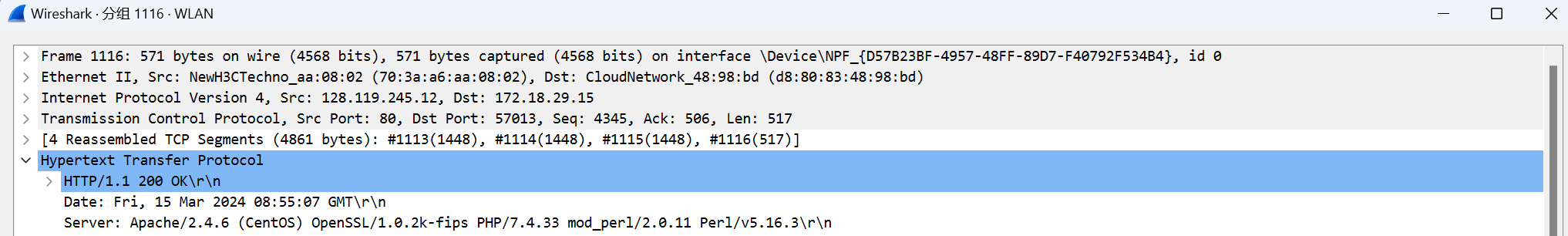


图19 问题15佐证