天津大学

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

课　　程　计算机网络

学　　号　3018216021

年　　级　2018 级

姓　　名　王昊恩

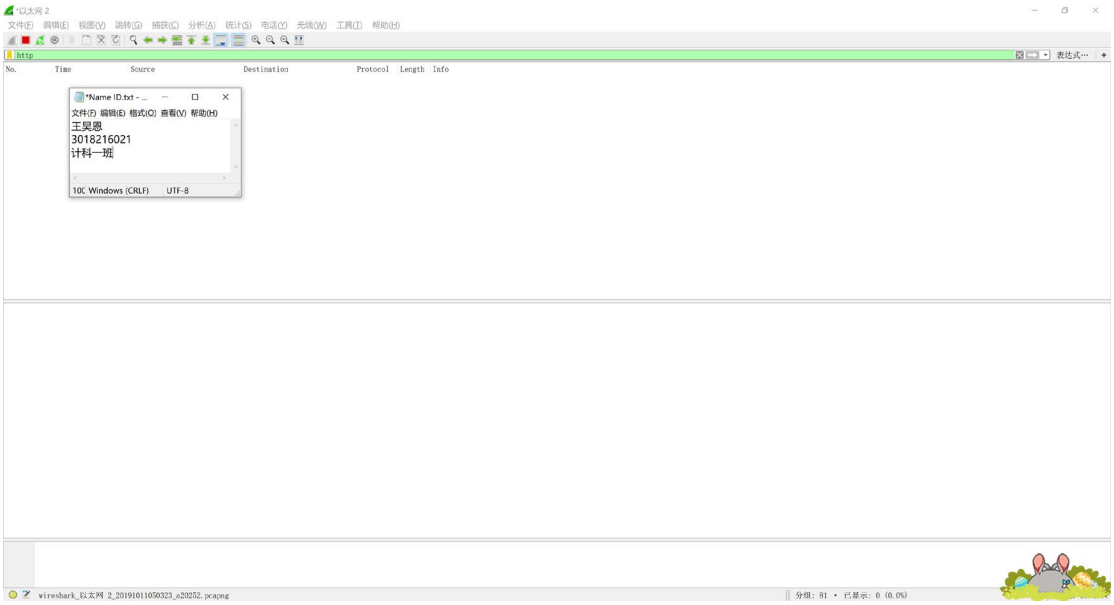
指导教师　赵增华

二零一九年十月四日

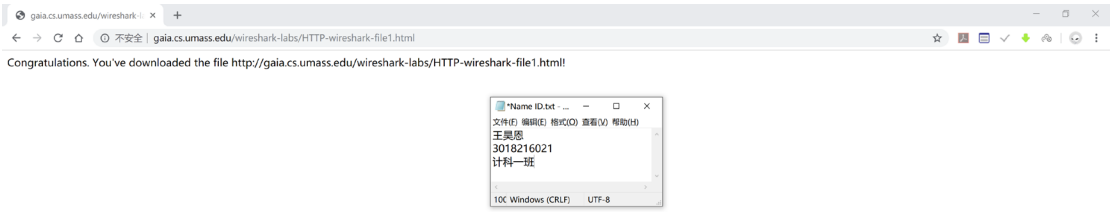
1. The Basic HTTP GET/response interaction（http 中 GET 请求的相应交互）

1） 实验过程

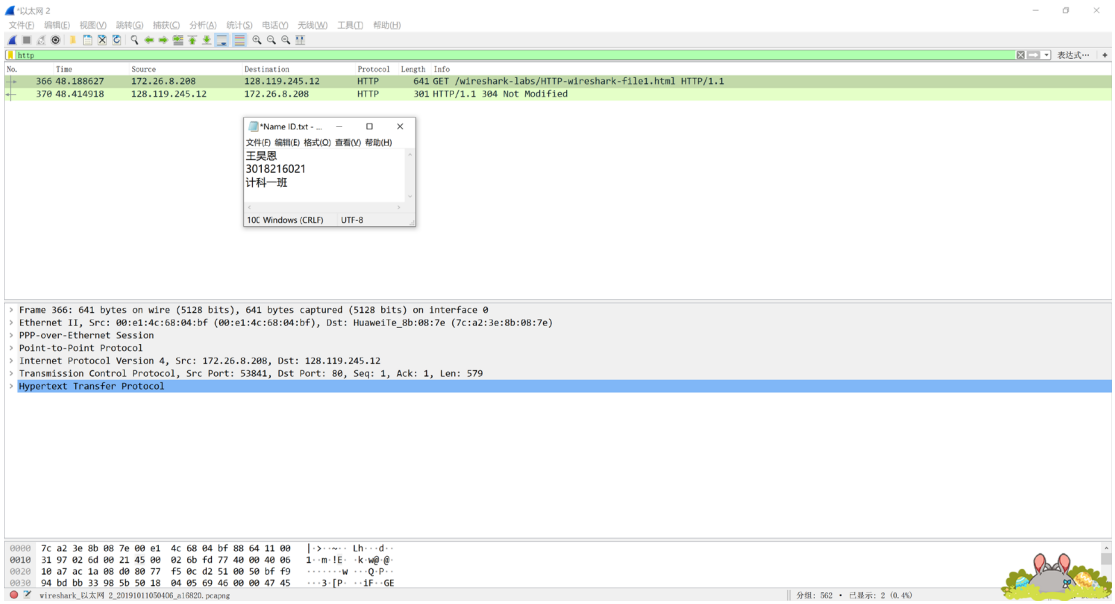
准备好 wireshark，预先填入过滤条件，准备开始抓包



在浏览器访问 pdf 中所给网址

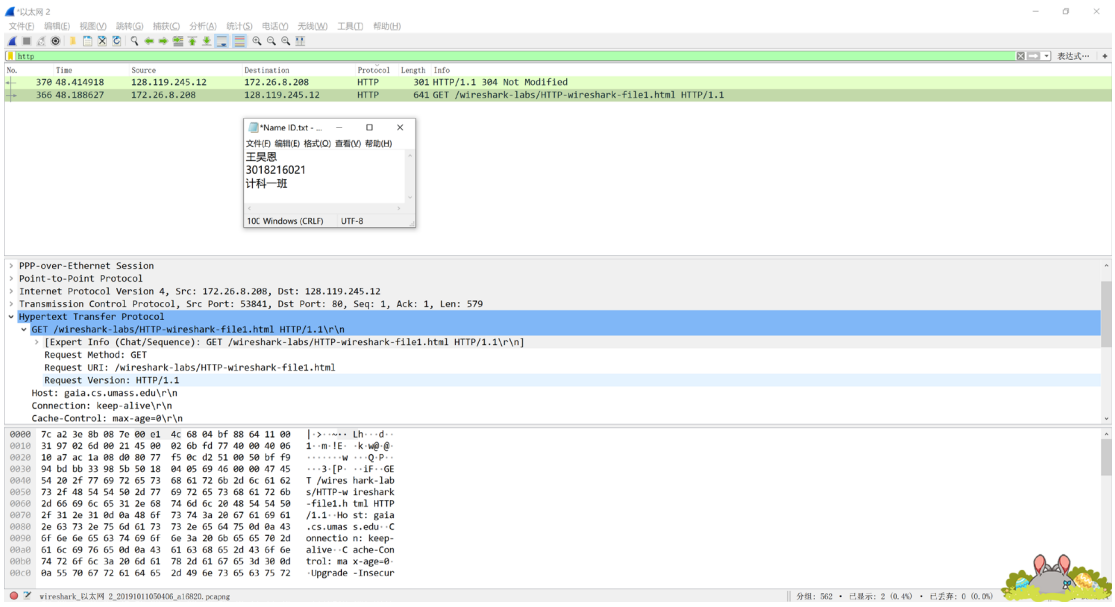


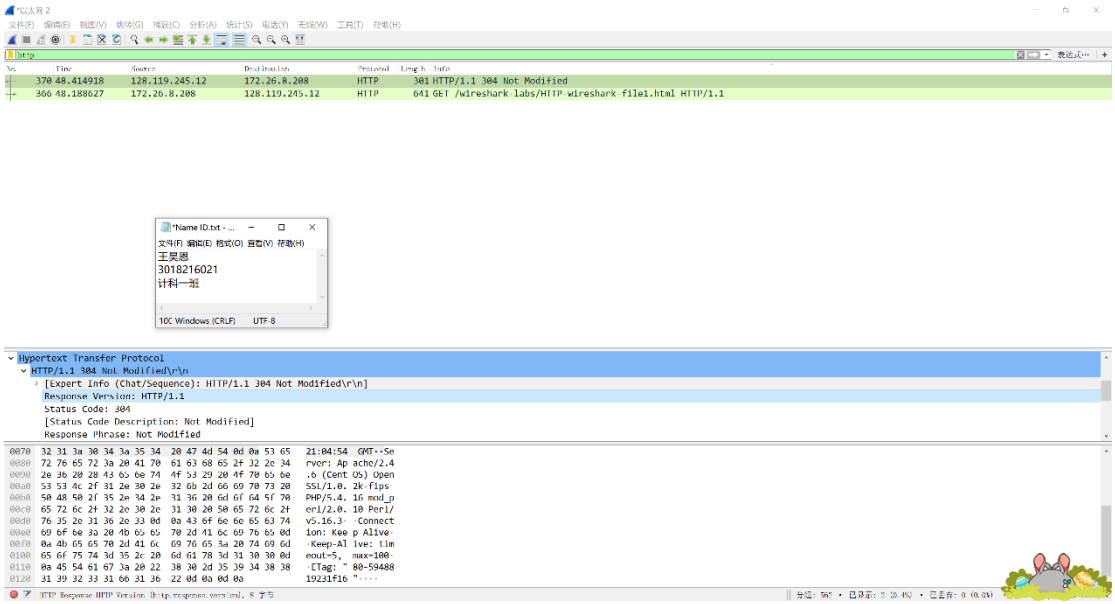
返回 wireshark 抓取数据包，由于操作比较快，顺利抓获请求和回应两个数据包



2）回答问题

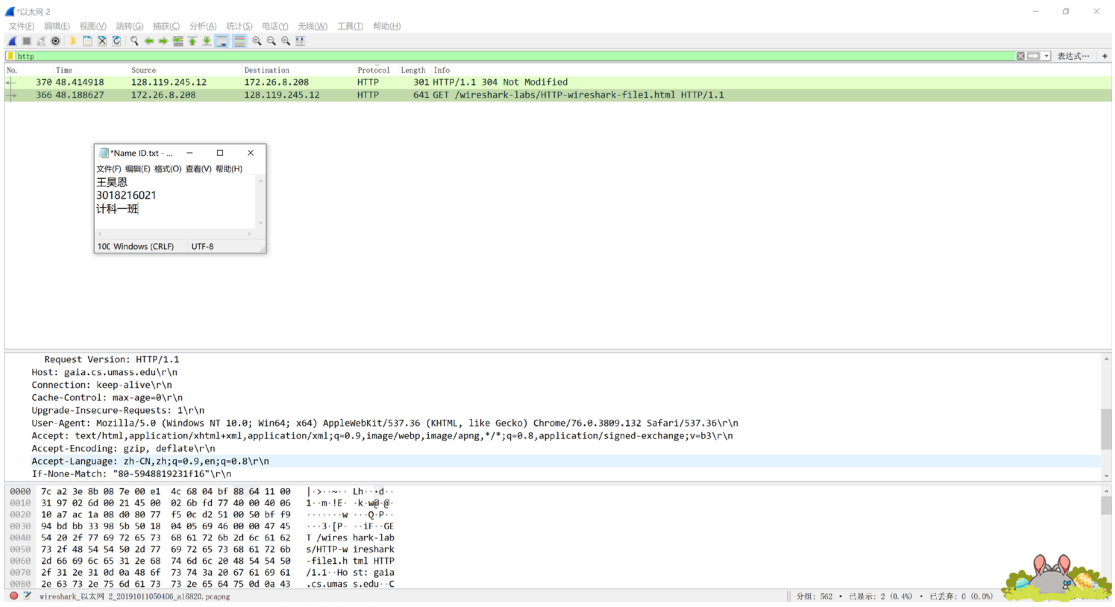
a. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?





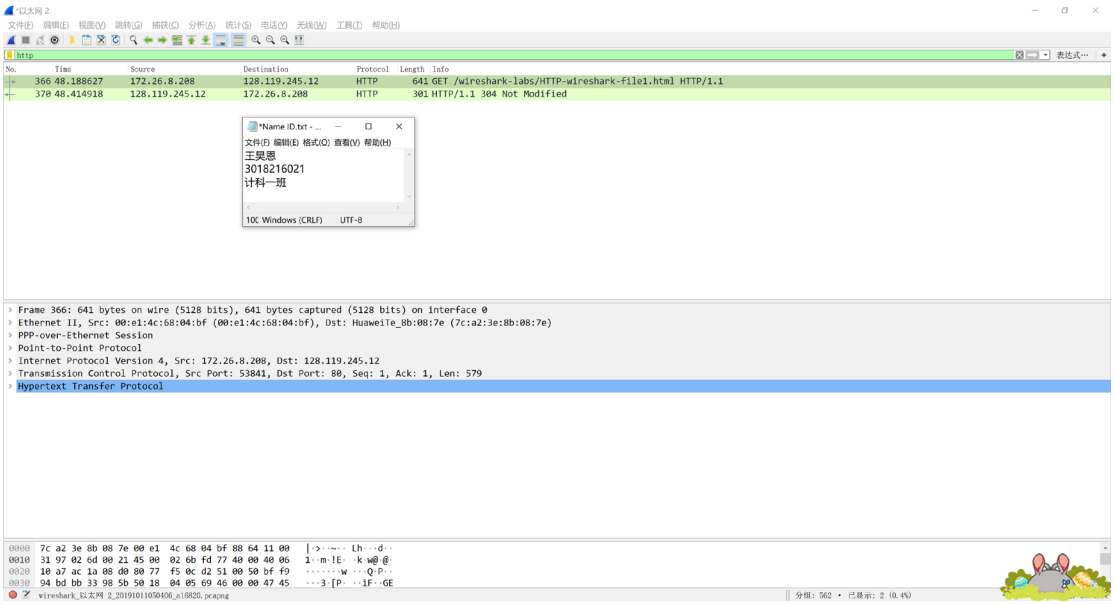
根据这两张图显示，浏览器和服务器都运行HTTP 1.1版本。

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



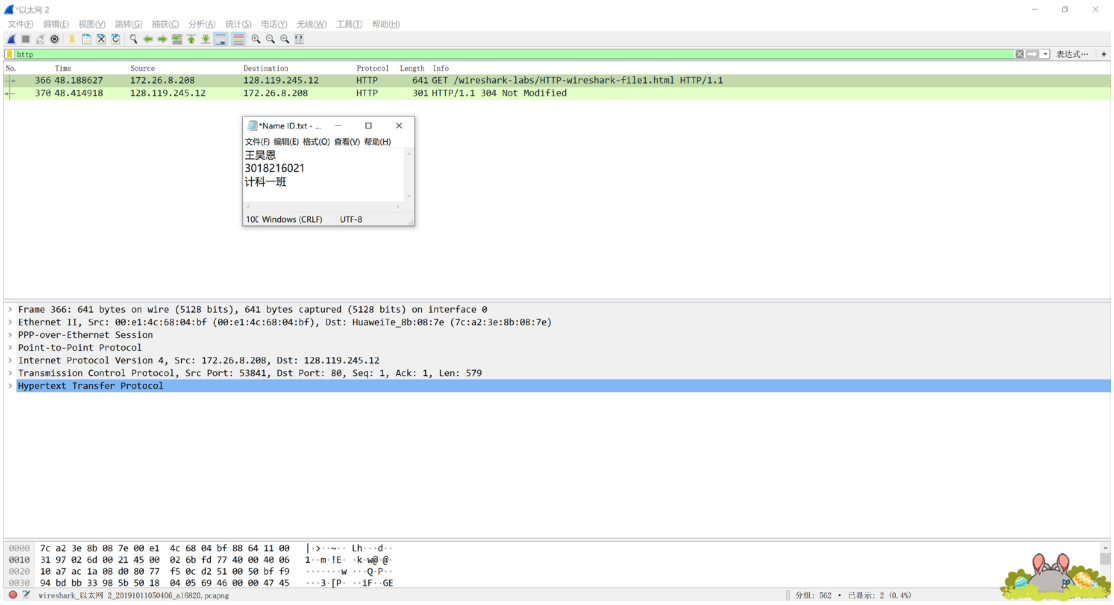
我的浏览器支持中文（zh-CN）和英文（en）。

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



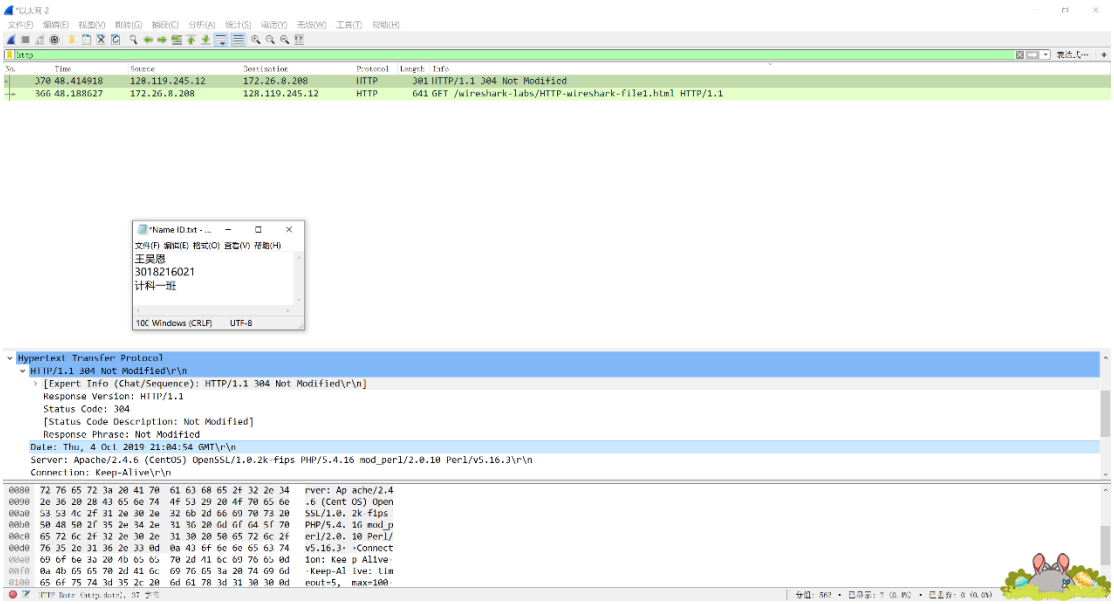
由上图第一条数据包信息可以看出，本机的IP地址是172.26.8.208，服务器的IP地址为128.119.245.12。

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



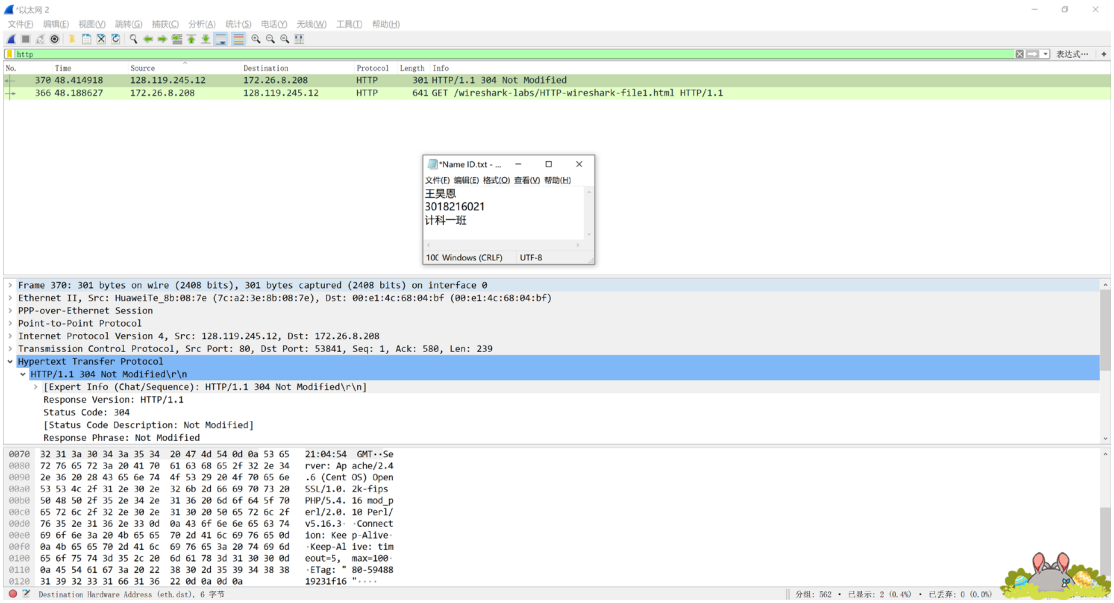
返回的状态码是304，应该是由于之前访问过该网站但没有清理浏览器缓存，所以显示“Not Modified”，说明无需再次传输请求的内容。

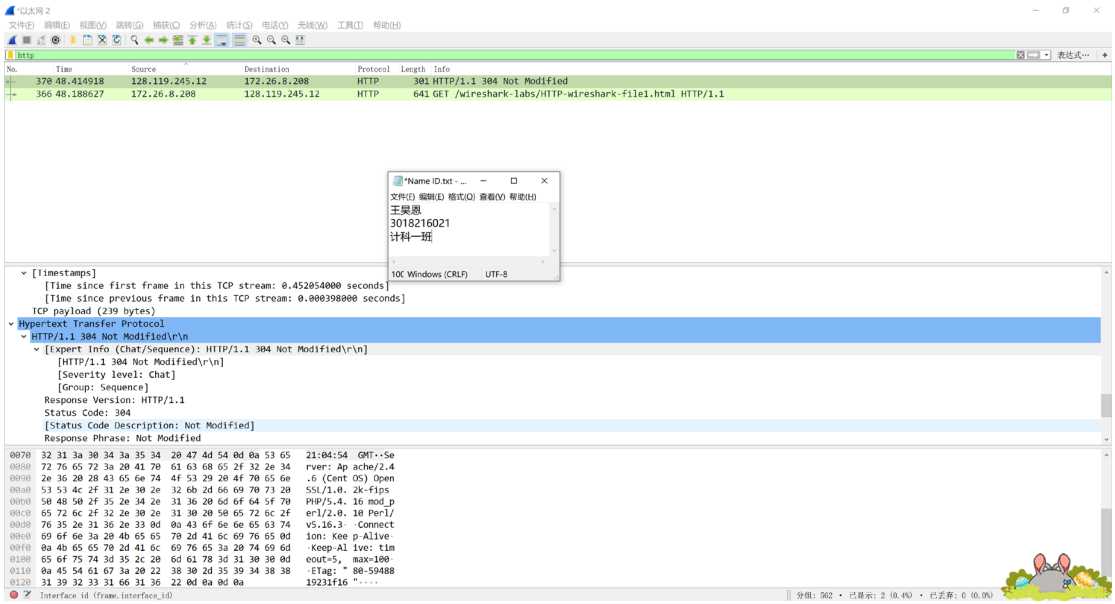
e.When was the HTML file that you are retrieving last modified at the server?



最后一次修改时间是：Thu，4 Oct 2019 21:05:54 GMT。

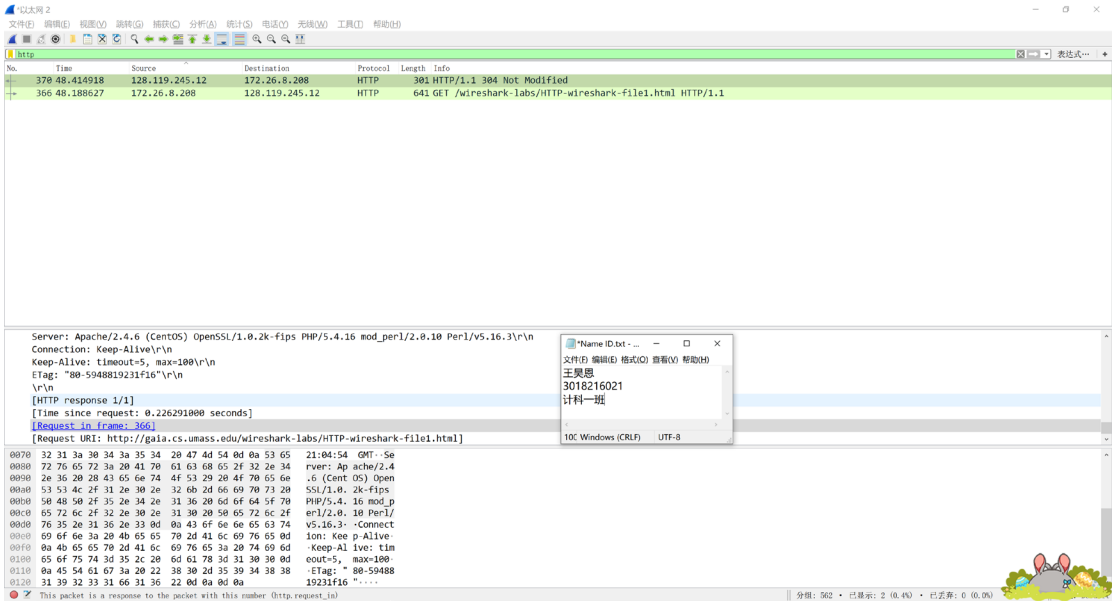
f.How many bytes of content are being returned to your browser?





返回的数据包大小为301bytes。

g.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.

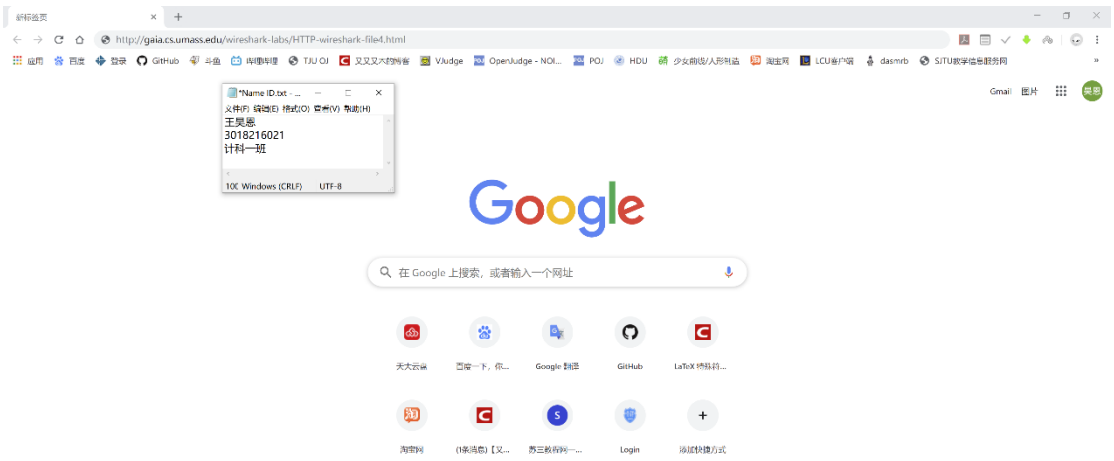


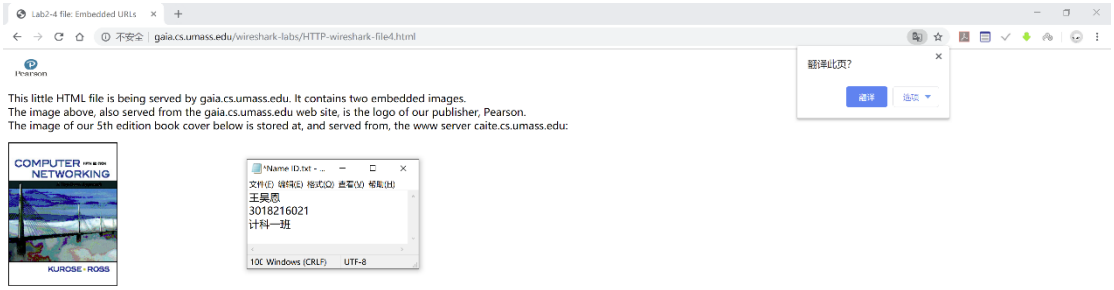
这部分信息不属于原始数据，其他部分都可以找到对应。

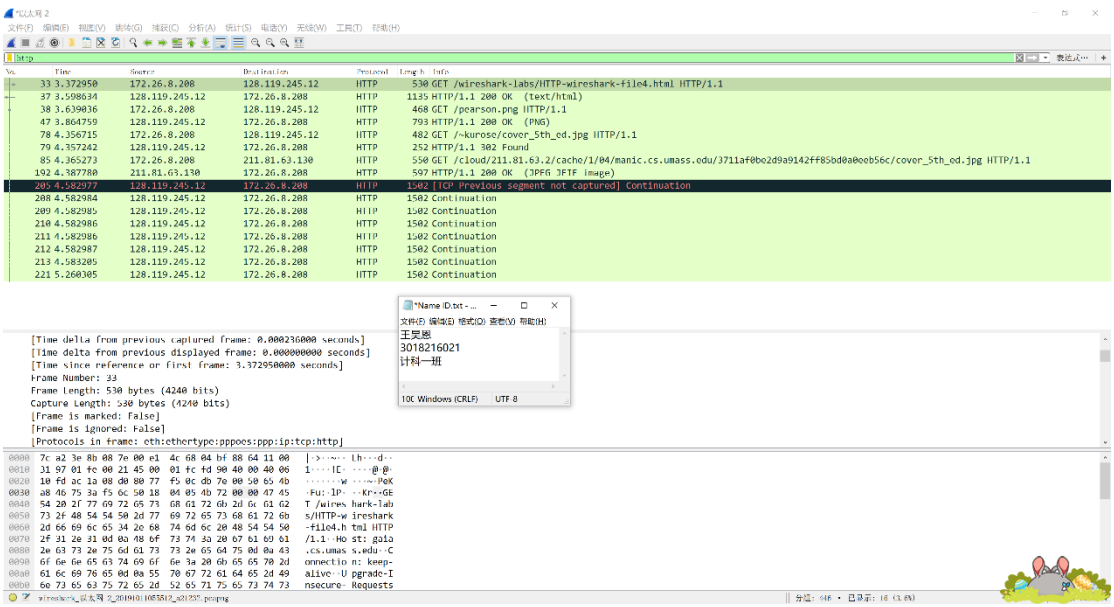
2. HTML Documents with Embedded Objects（包含嵌入式对象的 HTML 文档）

1） 实验过程

实验过程与 1 中类似，故只贴出实验截图。

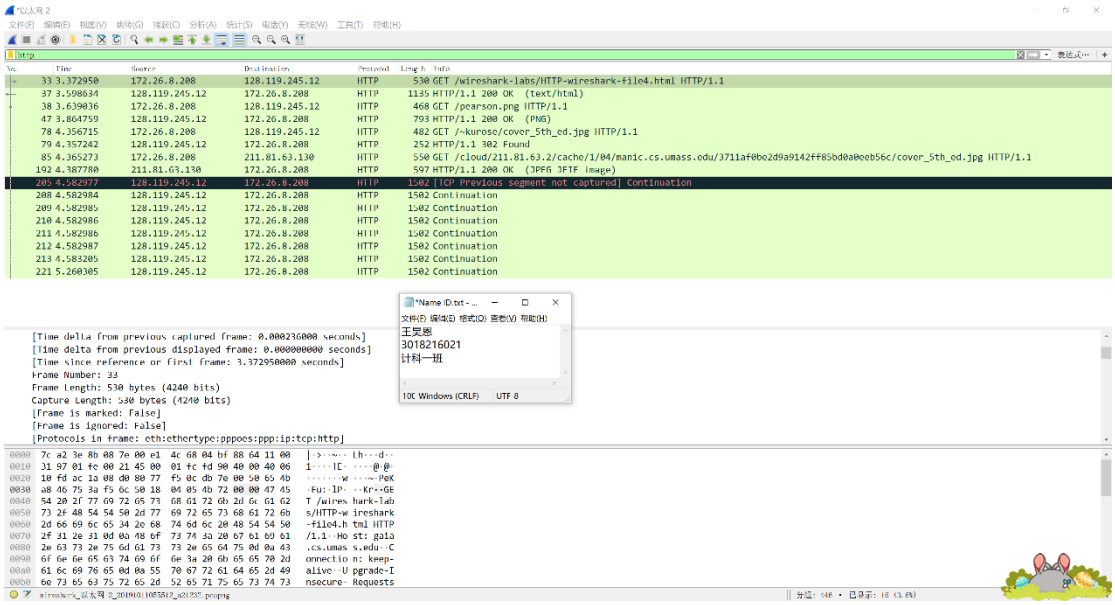

*Name ID.txt - ...
王昊恩
3018216021
计科一班
Google
在 Google 上搜索，或者输入一个网址


Lab2-4 file: Embedded URLs
gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
翻译此页?
This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images.
The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson.
The image of our 5th edition book cover below is stored at, and served from, the www server caite.cs.umass.edu:
COMPUTER NETWORKING
KUROSE · ROSS
*Name ID.txt - ...
王昊恩
3018216021
计科一班


No. Time Source Destination Protocol Length Info
33 3.372950 172.26.8.208 128.119.245.12 HTTP 530 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
37 3.598634 128.119.245.12 172.26.8.208 HTTP 1135 HTTP/1.1 200 OK (text/html)
38 3.639036 172.26.8.208 128.119.245.12 HTTP 468 GET /pearson.png HTTP/1.1
47 3.864759 128.119.245.12 172.26.8.208 HTTP 793 HTTP/1.1 200 OK (PNG)
78 4.356715 172.26.8.208 128.119.245.12 HTTP 482 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
79 4.357242 128.119.245.12 172.26.8.208 HTTP 252 HTTP/1.1 302 Found
85 4.365273 172.26.8.208 211.81.63.130 HTTP 550 GET /cloud/211.81.63.2/cache/1/04/manic.cs.umass.edu/3711af0bc2d9a9142ff85bd0a0eeb56c/cover_5th_ed.jpg HTTP/1.1
192 4.387780 211.81.63.130 172.26.8.208 HTTP 597 HTTP/1.1 200 OK (JPEG JFIF image)
205 4.582977 128.119.245.12 172.26.8.208 HTTP 1502 [TCP Previous segment not captured] Continuation
208 4.582984 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
209 4.582985 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
210 4.582986 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
211 4.582986 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
212 4.582987 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
213 4.583205 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
221 5.260305 128.119.245.12 172.26.8.208 HTTP 1502 Continuation
[Time delta from previous captured frame: 0.000236000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 3.372950000 seconds]
Frame Number: 33
Frame Length: 530 bytes (4240 bits)
Capture Length: 530 bytes (4240 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:tcp:http]
*Name ID.txt - ...
王昊恩
3018216021
计科一班

2） 回答问题

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



共发送了四个GET请求，分别是上图33、38、78、85四行，其中前三个发送给128.119.245.12，第四个发送给211.81.63.130。

b. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

串行下载。

观察四个请求和四次回应的顺序发现，第二张 jpg 文件的请求是在收到第一张 jpg 后才发出的，这符合串行下载的运行模式。