

# Wireshark Lab: HTTP

Copyright (c) 2020 Minaduki Shigure.

南京大学 电子科学与工程学院 吴康正 171180571

## 实验环境

macOS “Mojave” 10.14.5

Broadcom BCM4352 Wireless Network Adapter

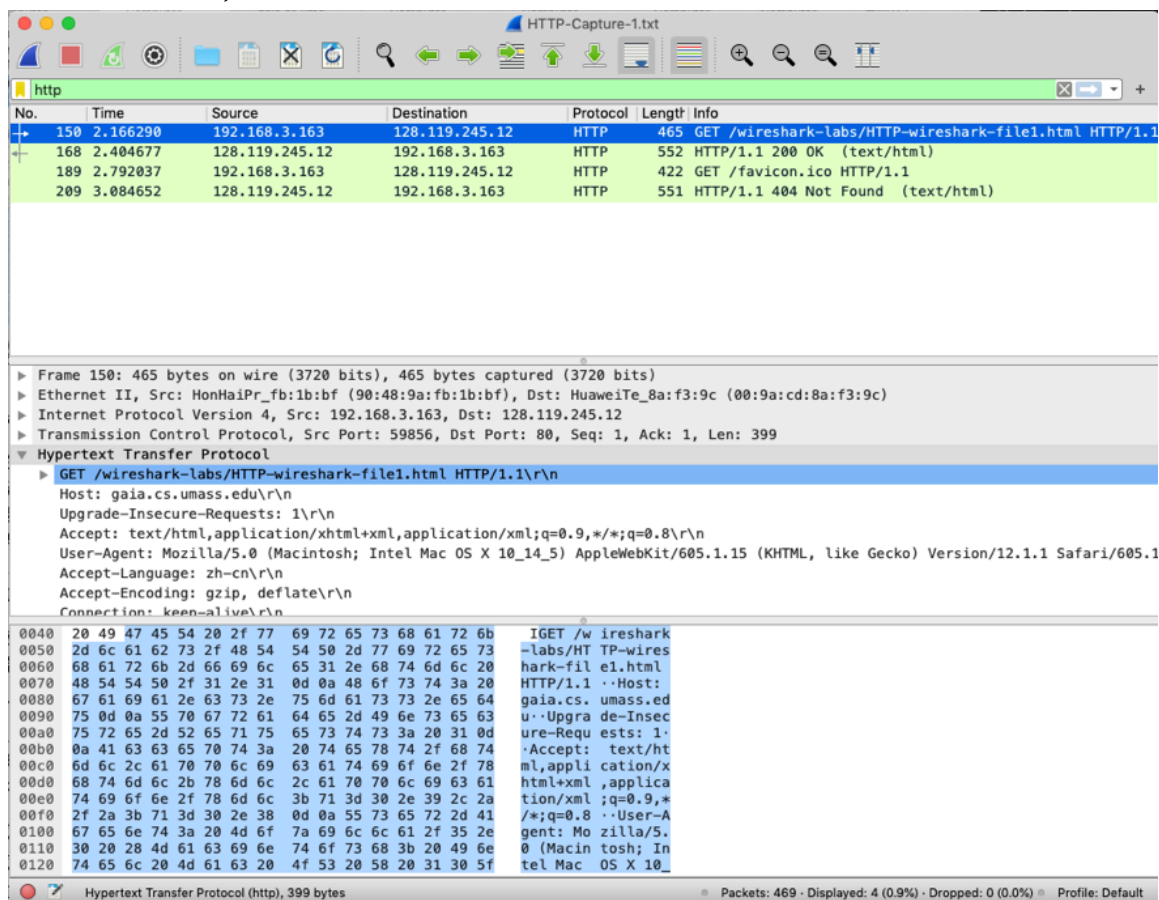
Wireshark Version 3.2.2 (v3.2.2-0-ga3efec3d640)

Safari Version 12.1.1 (14607.2.6.1.1)

## 实验内容：上网冲浪！

1. 首先按照课本要求，捕获一次访问网页 <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> 时的数据包如下所示：

其中的一个关于favicon的GET请求和对应的404回应是由于浏览器自动询问网站的默认图标而产生的，与实验内容无关



2. 按照要求打印HTTP GET和对应的响应的信息到Wireshark-HTTP-Capture1.pdf文件。文件内容在上一个报告中已经完整展现，因此此处不再浪费篇幅显示，仅附上问题有

关的部分。

您的浏览器是否运行HTTP版本1.0或1.1? 服务器运行什么版本的HTTP?

通过从GET请求的GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n和OK响应的HTTP/1.1 200 OK\r\n部分, 可以看出浏览器与服务器均运行HTTP 1.1。

您的浏览器会从服务器接受哪种语言(如果有的话)?

从GET请求的Accept-Language: zh-cn\r\n这项entry可以看出, 接受简体中文。

您的计算机的IP地址是什么? gaia.cs.umass.edu服务器地址呢?

从Wireshark的条目中就可以看出, 本地计算机的地址为192.168.3.163, 服务器地址为128.119.245.12。服务器返回到浏览器的状态代码是什么?

从返回的第一行HTTP/1.1 200 OK\r\n可以看出, 返回了200 OK。

服务器上HTML文件的最近一次修改是什么时候?

从响应部分的Last-Modified: Thu, 26 Mar 2020 05:59:03 GMT\r\n条目可以得知, 最后一次修改在2020年3月26日, 格林威治标准时间05:59:03

服务器返回多少字节的内容到您的浏览器?

从响应部分的File Data: 128 bytes条目可以得知, 返回的文件内容大小128字节。如果是指的整个Frame的大小的话, 可以从Wireshark条目中看出是552字节。通过检查数据包内容窗口中的原始数据, 你是否看到有协议头在数据包列表窗口中未显示? 如果是, 请举一个例子。

目前没有发现。

3. HTTP条件交互: 按照要求打印HTTP GET和对应的响应的信息到Wireshark-HTTP-Capture2.pdf文件, 此处仅附上问题有关的部分。

似乎Safari会强制刷新内容, 得不到想要的304响应, 因此本题使用的浏览器是基于Chromium的Microsoft Edge Canary 81.0.396.0

检查第一个从您浏览器到服务器的HTTP GET请求的内容。您在HTTP GET中看到了“IF-MODIFIED-SINCE”行吗?

没有该条目。

检查服务器响应的内容。服务器是否显式返回文件的内容? 您是怎么知道的?

服务器显式返回了文件内容, 可以从输出信息的File Data: 371 bytes条目得知, 也可以直接从返回的元数据中找到网页的内容。

现在, 检查第二个HTTP GET请求的内容。您在HTTP GET中看到了“IF-MODIFIED-SINCE:”行吗? 如果是, “IF-MODIFIED-SINCE:”头后面包含哪些信息?

在GET请求中找到了If-Modified-Since: Thu, 26 Mar 2020 05:59:03 GMT\r\n条目, 这与上一次收到的响应中的Last Modified条目内容相同, 指出最后一次修改在2020年3月26日, 格林威治标准时间05:59:03。

针对第二个HTTP GET, 从服务器响应的HTTP状态码和短语是什么? 服务器是否显式返回文件的内容? 请解释。

服务器返回了304 Not Modified, 并且没有直接返回文件内容, 本地浏览器使用了缓存的网页进行显示。可以发现此次返回的Frame大小为306字节, 小于上次的796字节, 这就是由于没有回传网页文件, 同时回传的信息相较上次更少而节约下来的。

4. 取回长文件: 按照要求打印HTTP GET和对应的响应的信息到Wireshark-HTTP-

Capture3.pdf文件，此处仅附上问题有关的部分。

您的浏览器发送多少HTTP GET请求消息？哪个数据包包含了美国权利法案的消息？仅发送了一条请求，对应的Frame 1504。

在Wireshark捕捉的响应条目中，可以看见Wireshark指出，响应被分成了4个TCP段，前三个长度为1400字节，后一个长度为661字节，与本机MTU（1500）相符。查看TCP包的元数据，可以看出第一个段（Frame 1784）中包含了THE BILL OF RIGHTS内容。

哪个数据包包含响应HTTP GET请求的状态码和短语？

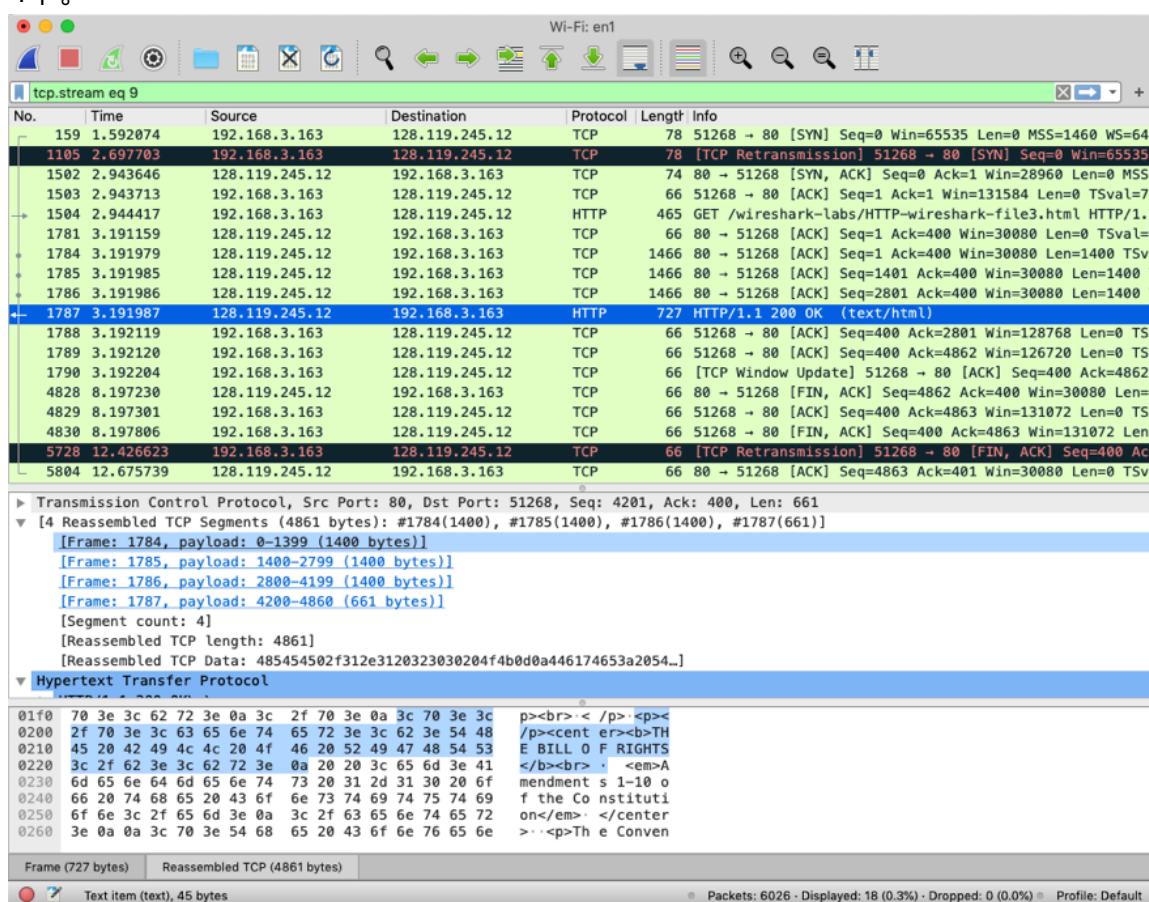
第一个TCP段（Frame 1784）中包含了状态码和短语。

响应中的状态码和短语是什么？

200 OK。

需要多少包含数据的TCP段来执行单个HTTP响应和权利法案文本？

4个。



5. 嵌入对象：按照要求打印HTTP GET和对应的响应的信息到Wireshark-HTTP-Capture4.pdf文件，此处仅附上问题有关的部分。

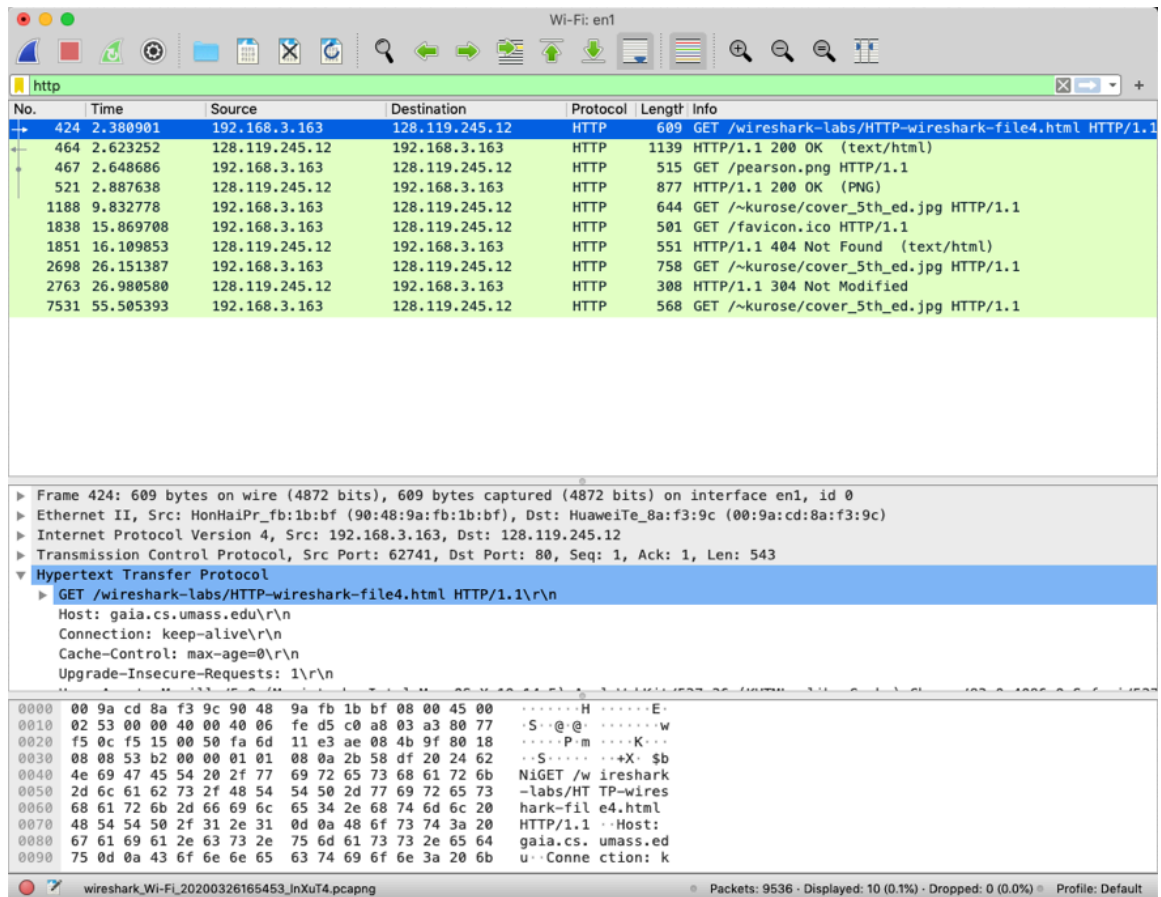
由于加载缓慢，所以对页面进行过刷新

您的浏览器发送了几个HTTP GET请求消息？这些GET请求发送到哪个地址？

根据Wireshark条目可以看出，总共发送了3个GET请求，其中网页文件与person的图片请求发送给了gaia.cs.umass.edu，而封面的请求发送给了manic.cs.umass.edu，对于两个服务器，IP地址都是129.119.245.12。

浏览器从两个网站串行还是并行下载了两张图片？请说明。

由于先收到了第一个图片的响应然后才发出第二图的请求，我认为是串行下载的。



6. HTTP认证：按照要求打印HTTP GET和对应的响应的信息到Wireshark-HTTP-Capture5.pdf文件，此处仅附上问题有关的部分。

对于您的浏览器的初始**HTTP GET**消息，服务器响应（状态码和短语）是什么响应？  
 第一个响应为401 Unauthorized。当您的浏览器第二次发送**HTTP GET**消息时，**HTTP GET**消息中包含哪些新字段？

包含了一个全新的字段Authorization: Basic

d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n，使用base64解码（或者直接观察Wireshark的分析窗口）可以看见之前输入的用户名密码组合。

Wireshark capture of an HTTP GET request and response. The packet list shows a GET request to /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html. The packet details show the request headers including Cache-Control, Authorization, Credentials, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The packet bytes show the raw HTTP request structure.

No.	Time	Source	Destination	Protocol	Length	Info
4867	8.424279	192.168.3.163	128.119.245.12	HTTP	599	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
4927	8.671386	128.119.245.12	192.168.3.163	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
5842	19.105563	192.168.3.163	128.119.245.12	HTTP	684	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
5877	19.353577	128.119.245.12	192.168.3.163	HTTP	556	HTTP/1.1 200 OK (text/html)

Cache-Control: max-age=0\r\n  
 Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=\r\n  
 Credentials: wireshark-students:network\r\n  
 Upgrade-Insecure-Requests: 1\r\n  
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4086.0 Safari/537.36\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/protected\_pages/HTTP-wireshark-file5.html]

0040 dc 14 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b ... GET /w ireshark  
 0050 2d 6c 61 62 73 2f 70 72 6f 74 65 63 74 65 64 5f ... labs/pr oteded\_  
 0060 70 61 67 65 73 2f 48 54 54 50 2d 77 69 72 65 73 ... pages/HT TP-wires  
 0070 68 61 72 6b 2d 66 69 6c 65 35 2e 68 74 6d 6c 20 ... hark-fil e5.html  
 0080 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 ... HTTP/1.1 Host:  
 0090 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 ... gaia.cs. umass.ed  
 00a0 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b ... u Connection: k  
 00b0 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 ... eep-aliv e Cache  
 00c0 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 ... -Control : max-ag  
 00d0 65 3d 30 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 ... e=0 Aut horizat

Credentials (http.authbasic) Packets: 6371 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) Profile: Default

## 小结

了解了HTTP请求，并对TCP封包和MTU等有了初步的认识。