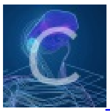
wireshark 第二章实验1http

原创

cyy想变强 于 2018-06-14 15:54:59 发布 4047 收藏 4
分类专栏： 计算机网络

本文链接：https://blog.csdn.net/qq_40178140/article/details/80692977
版权


计算机网络 专栏收录该内容
7 篇文章 0 订阅
订阅专栏

实验报告说先复习：

http报文有响应报文和请求报文两种：

请求报文第一行是请求行，接下来是首部行，每行以\r\n结尾（和编程作业类似，不加这个就都错了，原因百度上说是历史原因），请求行包含三个字段，方法字段：（get post等）；URL字段，http版本字段，如果是post等方法，那还会有实体，与首部行，空了一行\r\n

条件get要在get报文中包含if-modified-since，

缓存是web浏览器缓存在硬盘上的

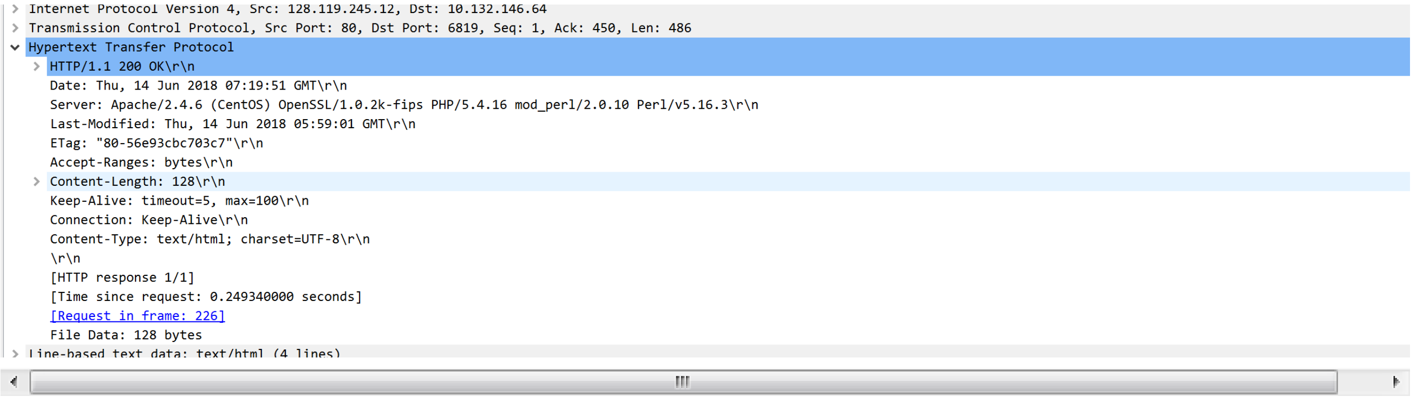
响应报文第一行是状态行，接下里6行是首部行，然后是实体体；状态行有三个字段，{协议版本，状态码，状态信息}；200：成功，301：请求的对象转移新的url在响应报文的实体中；400，通用差错，404：不在服务器上，505：http协议版本不对

两种报文首行每个字段间都有一个空格，接下来的首部行，首部字段名称和内容间有空格，每一行都以\r\n结束

然后在抓包：*http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html*

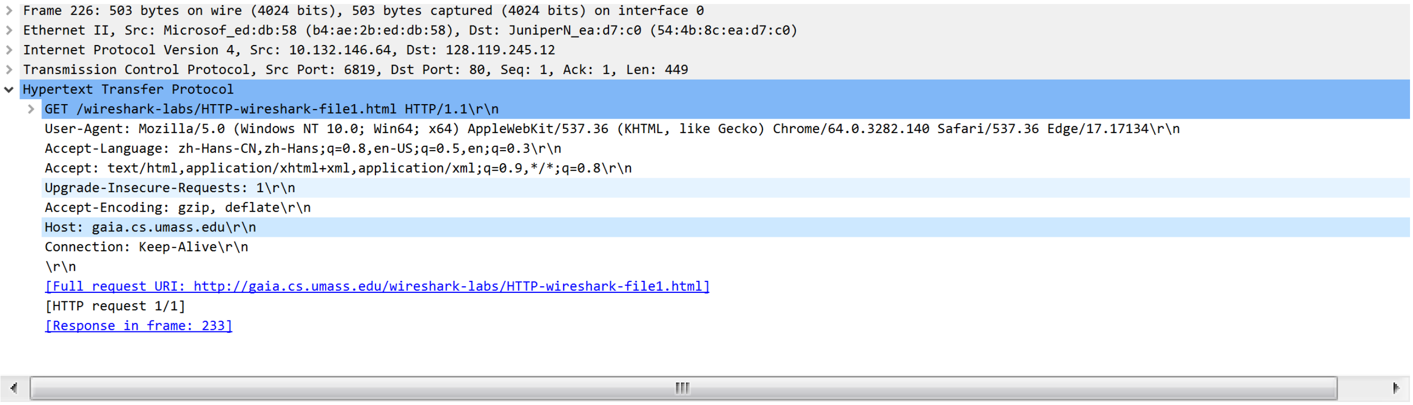
回答问题

响应报文



```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.132.146.64
> Transmission Control Protocol, Src Port: 80, Dst Port: 6819, Seq: 1, Ack: 450, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 14 Jun 2018 07:19:51 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: Thu, 14 Jun 2018 05:59:01 GMT\r\n
    ETag: "80-56e93cbc703c7"\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: 0.249340000 seconds]
    [Request in frame: 226]
    File Data: 128 bytes
> Line-based text data: text/html (4 lines)
```

请求报文



```
> Frame 226: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface 0
> Ethernet II, Src: Microsof_ed:db:58 (b4:ae:2b:ed:db:58), Dst: JuniperN_ea:d7:c0 (54:4b:8c:ea:d7:c0)
> Internet Protocol Version 4, Src: 10.132.146.64, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 6819, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Accept-Language: zh-Hans-CN,zh-Hans;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\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-file1.html]
    [HTTP request 1/1]
    [Response in frame: 233]
```

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
What languages (if any) does your browser indicate that it can accept to the server?
What is the IP address of your computer? Of the gaia.cs.umass.edu server?
What is the status code returned from the server to your browser?
When was the HTML file that you are retrieving last modified at the server?
How many bytes of content are being returned to your browser?
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.

1.both 1.1

2.zh-hans-cn,zh-hans

3.10.132.146.64；128.119.245.12

4.200

5.Thu，14 jun 2018 05：59：01 GMT

6.128bytes

7.没看到

第一部分完成

2.the http conditional get/response interaction

这个是缓存相关实验，很快的在浏览器中输入同一个网站并抓包，回答问题：

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

1.no

2.yes，from the answer code 200 I can tell，而且，也确实返回了那个文件

3.yes，第一次get得到文件的日期

4.304，not modified，没有，无实体体

3.长文件传送

知道了http过长的话会被分成几个tcp传送，最后得到的响应报文在wireshark上显示4 reassembled tcp segments

回答问题：

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?
Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
What is the status code and phrase in the response?
How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

1.1，不知道问的啥意思

2.不知道问的啥意思

3.200吧

4.4个

4.有嵌套文件的html的访问

请求html返回200时候，会把文本内容附在报文里，若过长会在tcp分段，如果有内嵌的连接，那么会把连接的地址放在报文里，然后按先后顺序找

How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

1.4条，第一条就是一开始输入的网站名，第二条是请求第一个图像的，第三条是请求第二个图像的，第四条是第二个图像被转移，302，给你一个新的地址，然后请求

2.serially（连续的），因为时间不同

5.加密网站的访问：

What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

1.401，unauthorized

2.authorization，base64encode，不是加密

实验二完成