计算机网络LAB1

姓名：姚丁钰

班级：智能2103班

学号：2021070301125

实验目的

通过本实验，熟练掌握Wireshark的操作和使用，学习对HTTP协议进行分析。

实验内容

HTTP 协议简介

HTTP 是超文本传输协议 （Hyper Text Transfer Protocol）的缩写，用于 WWW 服务。

1. **HTTP 的工作原理**

HTTP 是一个面向事务的客户服务器协议。尽管HTTP 使用TCP 作为底层传输协议，但 HTTP 协议是无状态的。也就是说，每个事务都是独立地进行处理。当一个事务开始时，就在web客户和服务器之间建立一个TCP 连接，而当事务结束时就释放这个连接。此外，客 户可以使用多个端口和和服务器 （80 端口）之间建立多个连接。其工作过程包括以下几个阶段。

① 服务器监听TCP 端口 80，以便发现是否有浏览器 （客户进程）向它发出连接请求；

② 一旦监听到连接请求，立即建立连接。

③ 浏览器向服务器发出浏览某个页面的请求，服务器接着返回所请求的页面作为响应。

④ 释放TCP 连接。

在浏览器和服务器之间的请求和响应的交互，必须遵循HTTP 规定的格式和规则。

当用户在浏览器的地址栏输入要访问的HTTP 服务器地址时，浏览器和被访问HTTP 服务器的工作过程如下：

① 浏览器分析待访问页面的URL 并向本地DNS 服务器请求IP 地解析；

② DNS 服务器解析出该HTTP 服务器的IP 地址并将IP 地址返回给浏览器；

③ 浏览器与HTTP 服务器建立TCP 连接，若连接成功，则进入下一步；

④ 浏览器向HTTP 服务器发出请求报文 （含GET 信息），请求访问服务器的指定页面；

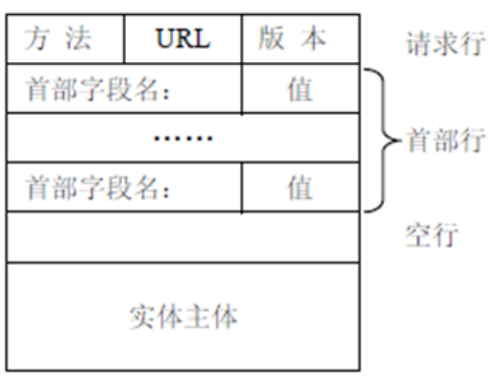
⑤ 服务器作出响应，将浏览器要访问的页面发送给浏览器，在页面传输过程中，浏览器会打开多个端口，与服务器建立多个连接；

⑥ 释放TCP 连接；

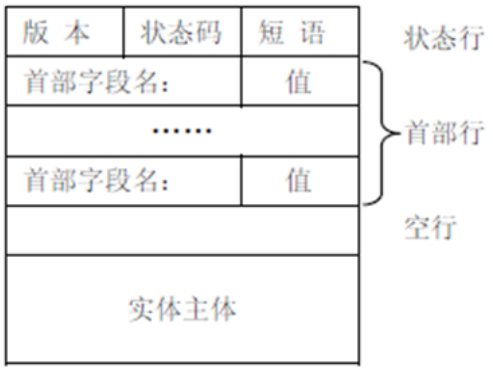
⑦ 浏览器收到页面并显示给用户。

2. **HTTP 报文格式**

HTTP 有两类报文：从客户到服务器的请求报文和从服务器到客户的响应报文。下图显示了两种报文的结构。



(a) HTTP 的请求报文结构



(b) HTTP 的响应报文结构

在图1.1 中，每个字段之间有空格分隔，每行的行尾有回车换行符。各字段的意义如下：

① 请求行由三个字段组成：

- 方法字段，最常用的方法为 “GET”，表示请求读取一个万维网的页面。常用的方法还有 “HEAD（指读取页面的首部）”和“POST（请求接受所附加的信息）；
- URL 字段为主机上的文件名，这时因为在建立TCP 连接时已经有了主机名；
- 版本字段说明所使用的HTTP 协议的版本，一般为 “HTTP/1.1”。

② 状态行也有三个字段：

- 第一个字段等同请求行的第三字段；
- 第二个字段一般为 “200”，表示一切正常，状态码共有41 种，常用的有：301 （网站已转移），400（服务器无法理解请求报文），404（服务器没有锁请求的对象）等；
- 第三个字段时解释状态码的短语。

③ 根据具体情况，首部行的行数是可变的。请求首部有Accept 字段，其值表示浏览器 可以接受何种类型的媒体；Accept-language，其值表示浏览器使用的语言；User-agent 表明可用的浏览器类型。响应首部中有Date、Server、Content-Type、Content-Length 等字段。在请求首部和响应首部中都有 Connection 字段，其值为Keep-Alive 或 Close，表示服务器在传送完所请求的对象后是保持连接或关闭连接。

④ 若请求报文中使用 “GET”方法，首部行后面没有实体主体，当使用 “POST”方法是，附加的信息被填写在实体主体部分。在响应报文中，实体主体部分为服务器发送给客户的对象。

图1.2 和图1.3显示了捕获的HTTP 请求和响应报文，结合上面的介绍，请自己分析和体会。

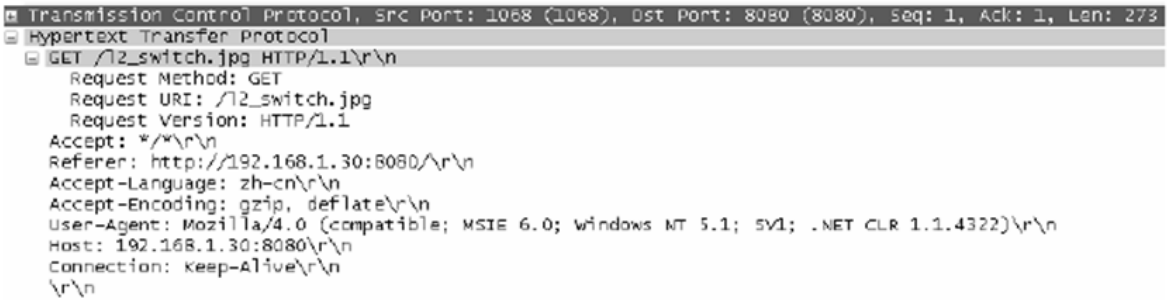


图 1.2 HTTP 请求报文示例

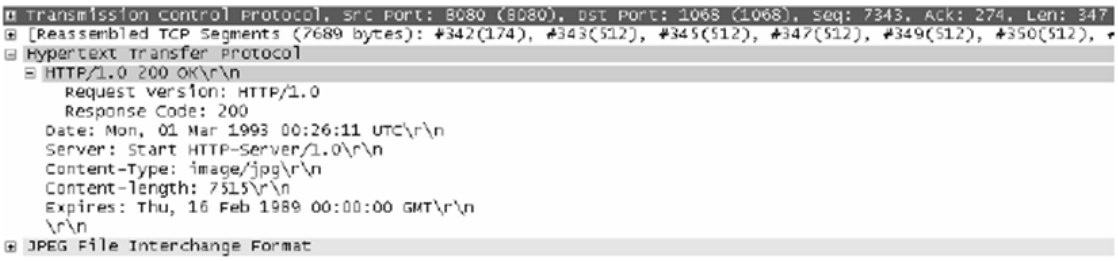
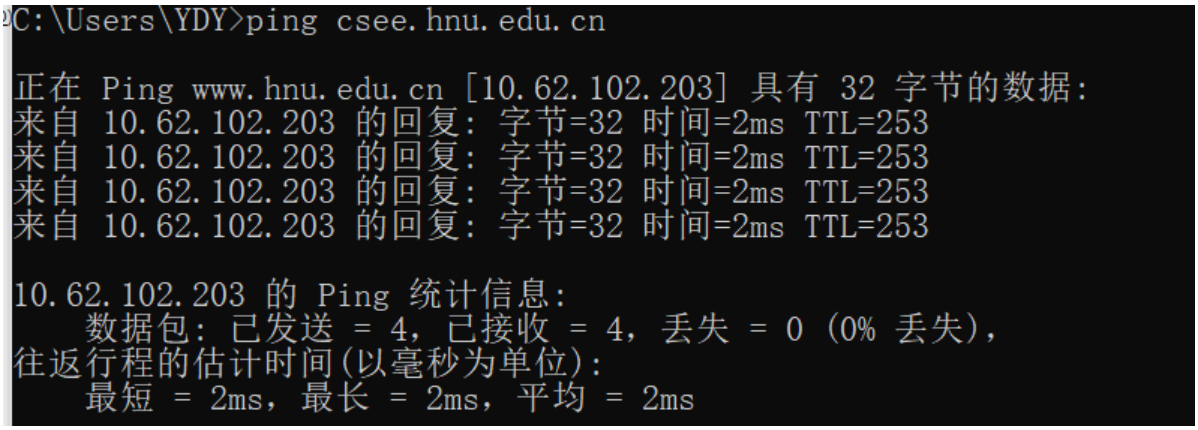


图 1.3 HTTP 响应报文示例

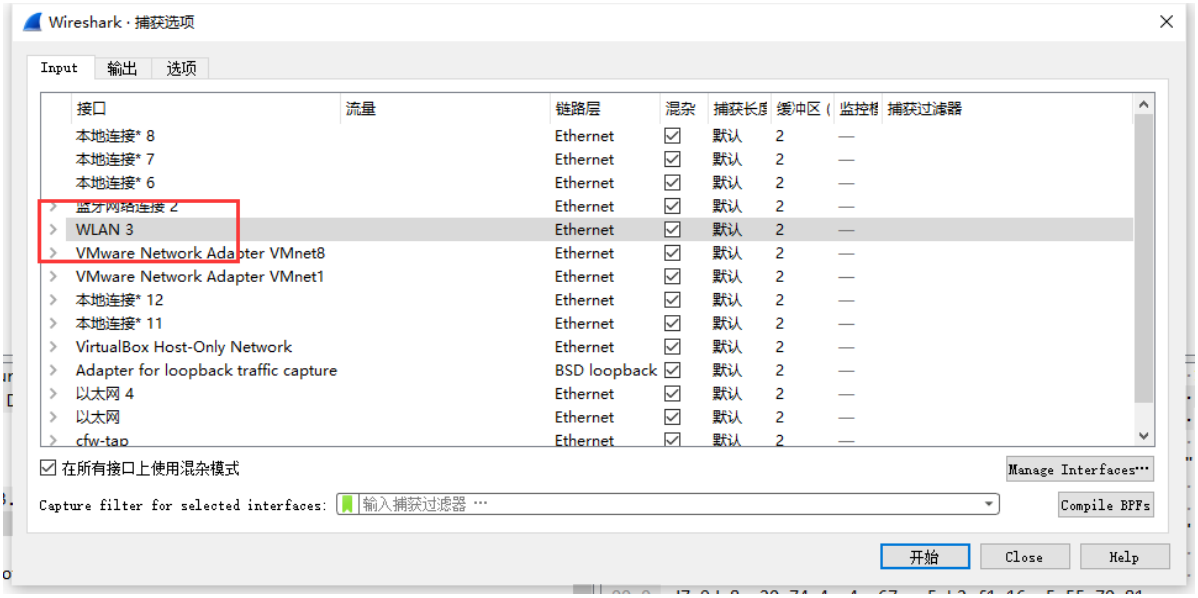
实验过程

1. 在PC 机上运行Wireshark，开始截获报文

- 在cmd中输入命令ping csee.hnu.edu.cn查看网站的ip地址



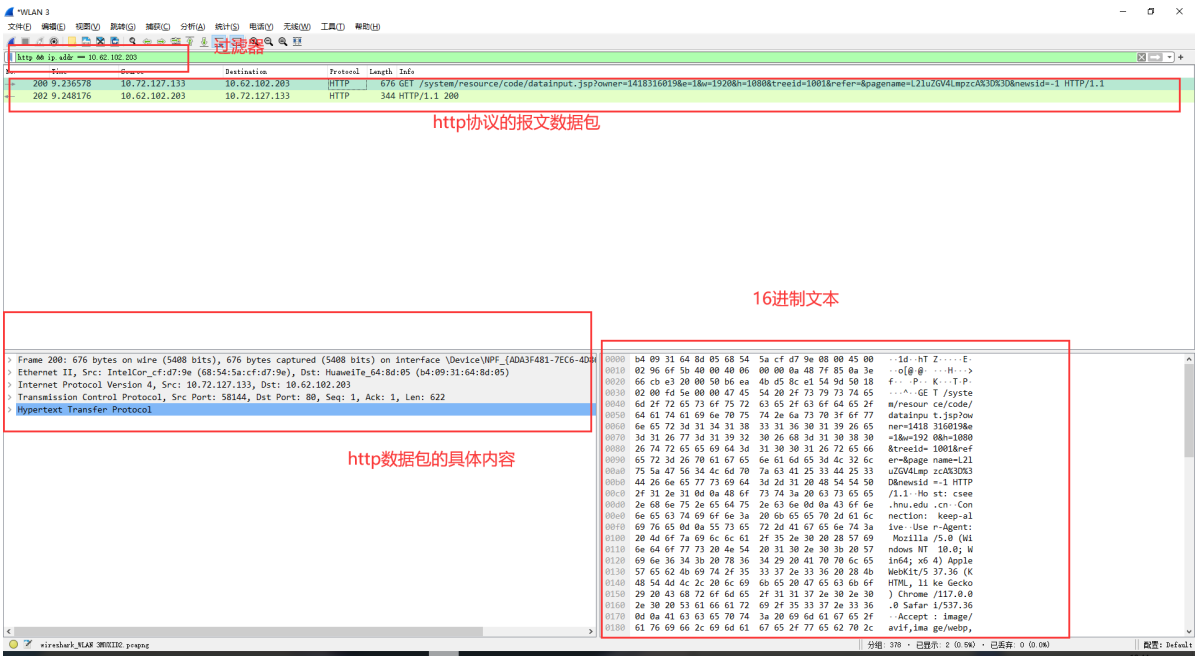
- 选择抓包方式为wlan



2. 从浏览器上访问Web 界面，如http://csee.hnu.edu.cn打开网页，待浏览器的状态栏出现 “完毕”信息后关闭网页。

wireshark有一个强大的功能就是可以选择过滤出想要的抓包信息。由于我们一打开WLAN接口软件就开始抓包，所以抓的包中可能包含不是关于想要http://csee.hnu.edu.cn的相关报文。可以在过滤器上输入http来获得相关HTTP协议的报文，这里我们可以使用过滤器。由于我们想要获得HTTP协议的报文，因此我们在过滤栏输入http过滤出http协议的报文信息：

通过输入http && ip.addr == 10.62.102.203来对截获报文进行筛选



3. 停止截获报文，将截获的报文命名为http-学号保存。

回答问题

1. 综合分析截获的报文，查看有几种HTTP 报文

有两种HTTP报文。

- 第一种是HTTP的请求报文：200 9.236578是从客户端发往服务器的请求报文，其中Source的10.72.127.133是客户端的ip，Destination的10.62.102.203是服务器的ip
- 第二种是HTTP的应答报文：202 9.248176是从服务器发往客户端的应答报文，其中Source的10.62.102.203是服务器的ip，Destination的10.72.127.133是客户端的ip

No.	Time	Source	Destination	Protocol	Length	Info
200	9.236578	10.72.127.133	10.62.102.203	HTTP	676	GET /system/resourc
202	9.248176	10.62.102.203	10.72.127.133	HTTP	344	HTTP/1.1 200

2. 在截获的HTTP 报文中，任选一个HTTP 请求报文和对应的 HTTP 应答报文，仔细分析它们的格式，填写表1.1 和表1.2。

表1.1 HTTP 请求报文格式

```
Hypertext Transfer Protocol
  GET /system/resource/code/datainput.jsp?owner=1418316019&e=1&w=1920&h=1080&treeid=1001&refer=&pagename=L2luZGV4L
  Host: csee.hnu.edu.cn\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Sa
  Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://csee.hnu.edu.cn/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9\r\n
  Cookie: UM_distinctid=18a310380af1364-09f0b44ff47cb9-26031f51-1fa400-18a310380b01941; JSESSIONID=15814B7706B4606
  \r\n
  [Full request URI: http://csee.hnu.edu.cn/system/resource/code/datainput.jsp?owner=1418316019&e=1&w=1920&h=10808
  [HTTP request 1/1]
  [Response in frame: 202]
```

表 1.1 HTTP 请求报文格式

方 法	GET	版 本	HTTP/1.1
URL	/system/resource/code/datainput.jsp?owner=1418316019&e=1&w=1920&h=1080&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1		
首部字段名	字段值	字段所表达的信息	
Host	csee.hnu.edu.cn	指明了对象所在主机	
Connection	Keep-alive	该浏览器告诉服务器需要使用持续连接	
User-Agnet	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36	指明用户代理，即向服务器发送请求的浏览器类型	
Accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8	浏览器接受的文件媒体类型	
Reference	http://csee.hnu.edu.cn/	提供包含当前 URI 的文档的 URL	
Accept Encoding	gzip, deflate	告诉服务器能够发送哪些编码方式	
Accept Language	zh-CN,zh;q=0.9	表示用户想得到该对象的语言版本	
Cookie	UM_distinctid=18a310380af1364-09f0b44ff47cb9-26031f51-1fa400-18a310380b01941	用户标识	

表1.2 HTTP 应答报文格式

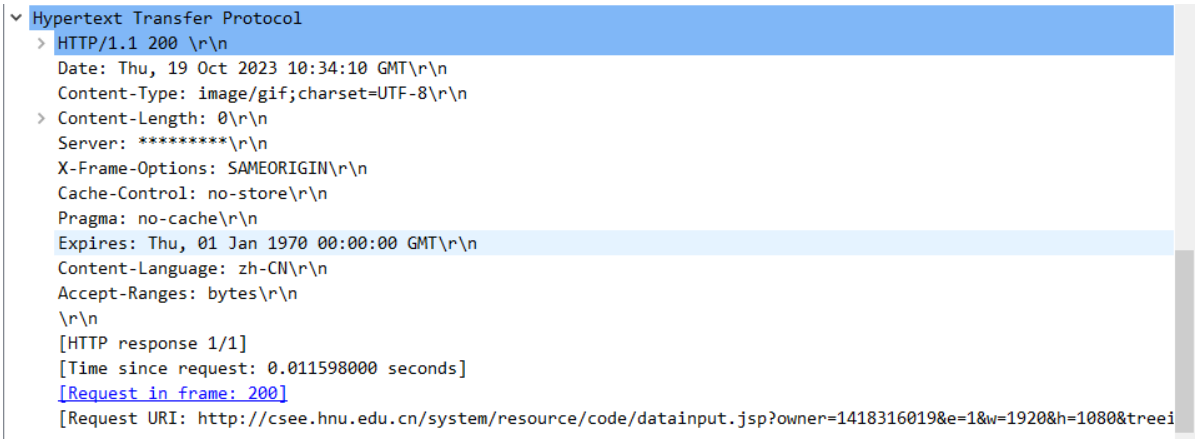


表 1.2 HTTP 应答报文格式

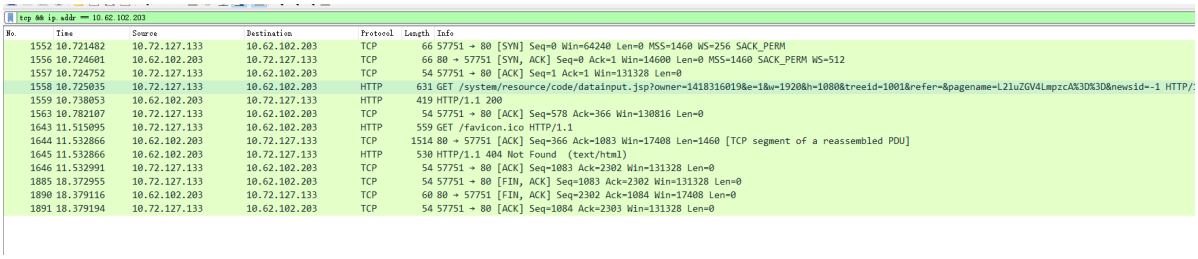
版 本	HTTP/1.1	状态码	200
短 语	空		
首部字段名	字段值	字段所表达的信息	
Date	Thu, 19 Oct 2023 10:34:10 GMT	指示服务器产生并发送该响应报文的日期和时间	
Content_Type	image/gif;charset=UTF-8	指示了实体体中的对象的媒体类型	
Content_Length	0	指示了被发送对象的字节数	
Server	*********	指示该报文由什么样的服务器产生，类似 http 请求报文的 user-agent	
X-Frame-Options	X-Frame-Options: SAMEORIGIN	告诉浏览器该网页是否可以放在 iFrame 中	
Cache_Control	no-store	控制缓存的行为	
Pragma	no-cache	报文指令	
Expires	Expires: Thu, 01 Jan 1970 00:00:00 GMT	实体主题过期的日期时间	
Response-Language	zh-CN	实体主体的自然语言	
Accept-Ranges	bytes	是否接受字节范围请求	

3. 分析在截获的报文中，客户机与服务器建立了几个连接？服务器和客户机分别使用了哪几个端口号?

客户机和服务器建立1个连接。

服务器使用了**1个端口**：57751

客户机使用了**1个端口**：80端口。

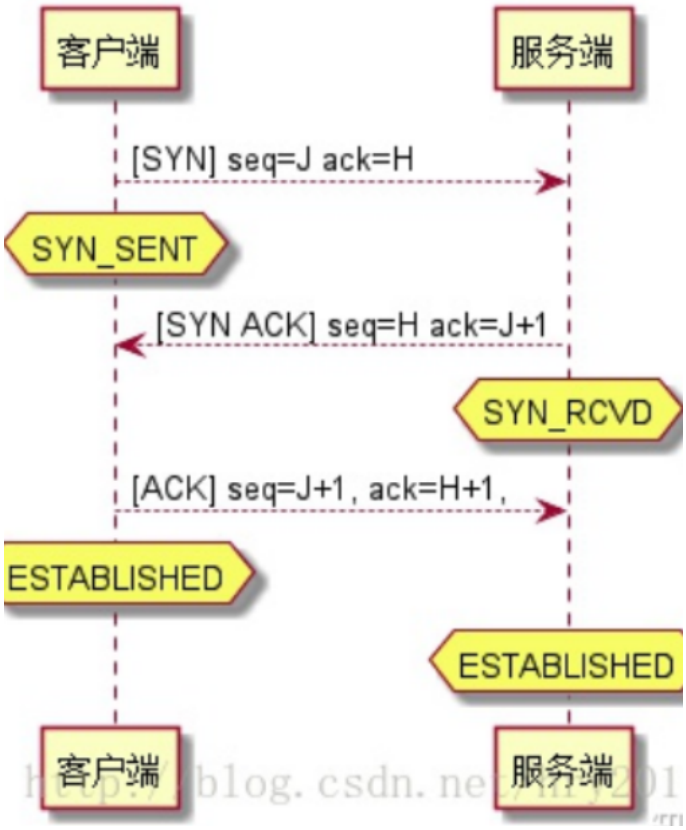


4. 综合分析截获的报文，理解HTTP 协议的工作过程，将结果填入表1.3中。

HTTP的工作流程大致为：

1. 建立连接。先解析DNS，把local host变成ip（127.0.0.1），然后根据127.0.0.1和端口号80（没有端口号则使用默认的端口）建立socket。也可以理解为通过“三次握手”建立TCP连接，确定通讯正常。
2. 发送请求命令。socket建立好之后，客户端开始向web服务器发送请求命令（GET/POST等）。

3. 发送请求头（和请求正文如果有）。客户端先发送与自身相关的信息，再发送空行表示请求头发送完毕，如果是post则继续发送请求正文。
4. 回传状态行。应答第一步，发送协议版本和状态码（200、503、404等）
5. 回传应答头。应答第二步，先发送自身相关信息、Content-Type(必须)及被请求的文档，在发送空行宝石应答头发送完毕。
6. 回传应答正文。应答第三步，根据应答头的Content-Type指定的格式发送应答正文。
7. 关闭连接。一次‘会话’完成，如果设置了Connection：keep-alive则TCP连接不关闭，否则关闭连接。



- **第一次握手**：客户端发送SYN到服务器，并进入SYN_SENT状态。SYN ： 标志位，表示请求建立连接。Seq = 0 ： 初始建立连接值为0，数据包的相对序列号从0开始，表示当前还没有发送数据。Ack =0：初始建立连接值为0，已经收到包的数量，表示当前没有接收到数据。
- **第二次握手**：服务器收到请求后，回送SYN+ACK信令到客户端，此时服务器进入SYN_RECV状态，Seq = 0 ： 初始建立值为0，表示当前还没有发送数据，Ack = 1 : 表示当前端成功接收的数据位数，虽然客户端没有发送任何有效数据，确认号还是被加1，因为包含SYN或FIN标志位。
- **第三次握手**：主客户端收到SYN+ACK包，向服务器发送确认ACK包，客户端进入ESTABLISHED状态，服务器收到请求后也进入

ESTABLISHED状态，完成三次握手，此时TCP连接成功，客户端与服务器开始传送数据。ACK：标志位，表示已经收到记录。Seq = 1：表示当前已经发送1个数据。

下图为对应报文段：

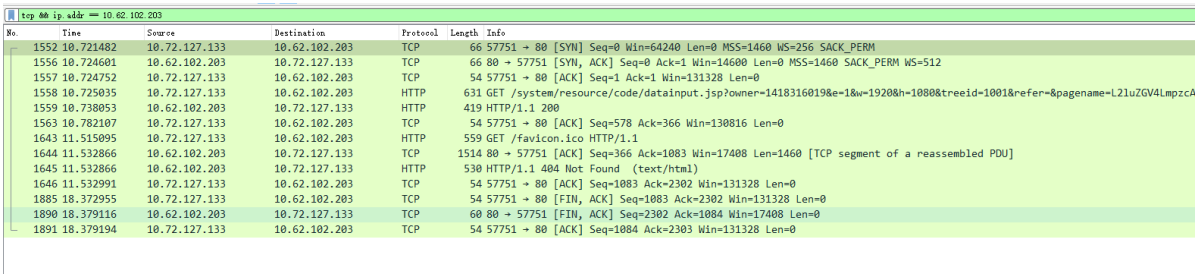


表1.3 HTTP 协议工作过程

HTTP 客户机端口号	HTTP 服务器端口号	所包括的报文号	步骤说明
57751	80	1552	TCP三次握手的第一次握手：客户端发送一个SYN=1的数据包给服务器
57751	80	1556	TCP三次握手的二次握手：客户端发送一个SYN=1，ACK=1的数据包给服务器，表示服务端可以收到客户端的数据然后询问客户端是否能收到服务端的数据
57751	80	1557	TCP三次握手的三次握手：客户端发送一个ACK=1的数据包给服务器，表示服务端可以收到客户端的数据，至此TCP建立
57751	80	1559	浏览器发出一个页面HTTP请求
57751	80	1563	客户端浏览器确认
57751	80	1644	服务器发送数据
57751	80	1646	客户端浏览器确认

实验总结

实验过程遇到的问题

- Wireshark截获了很多无用报文

【解决方案】

1. 将其他接入网络的应用程序关闭，避免捕捉到不需要的报文。
2. 将使用的浏览器设置成关闭时消除浏览记录，可以避免每次手工操作删除。
3. 学会利用过滤器，如使用http、TCP等过滤器，寻找到自己想要分析查看的报文内容

总结

通过这次实验，让我熟悉了常用网络命令，并学习了这些命令的使用环境以及使用方法；掌握了Wireshark的操作和使用。通过截获的报文，能够对HTTP协议进行分析，更清晰地认识了http协议的工作过程。

在用wireshark时掌握一些技巧能够帮助我们更好地分析理解报文，还需在使用过程中多加积累。