计算机网络 课程基础实验一
应用协议与数据包分析实验(Wireshark)

计科210X 甘晴void 202108010XXX

一、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。

二、实验内容

2.1 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；

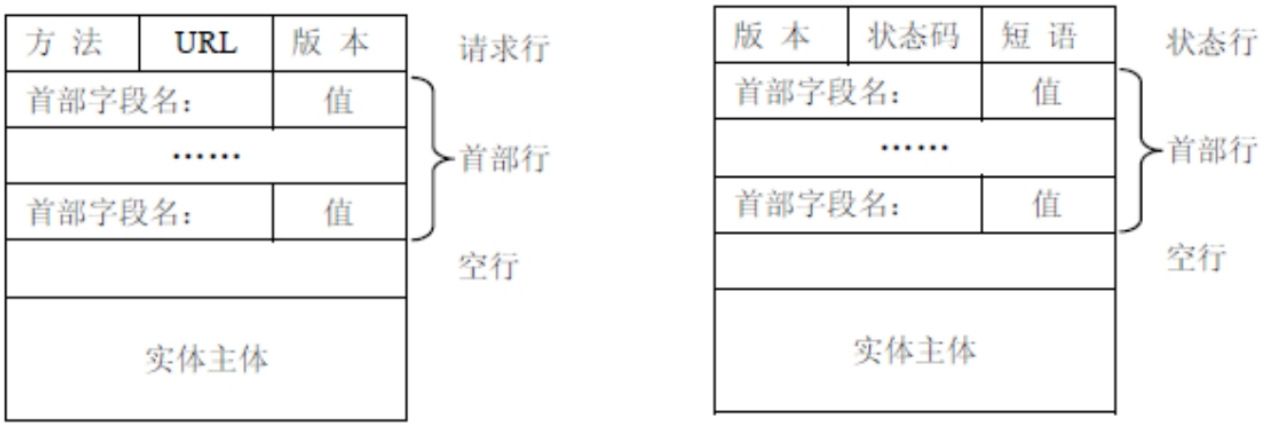
⑤ 服务器作出响应，将浏览器要访问的页面发送给浏览器，在页面传输过程中，浏览器会打开多个端口，与服务器建立多个连接；

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。图 5.46 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”

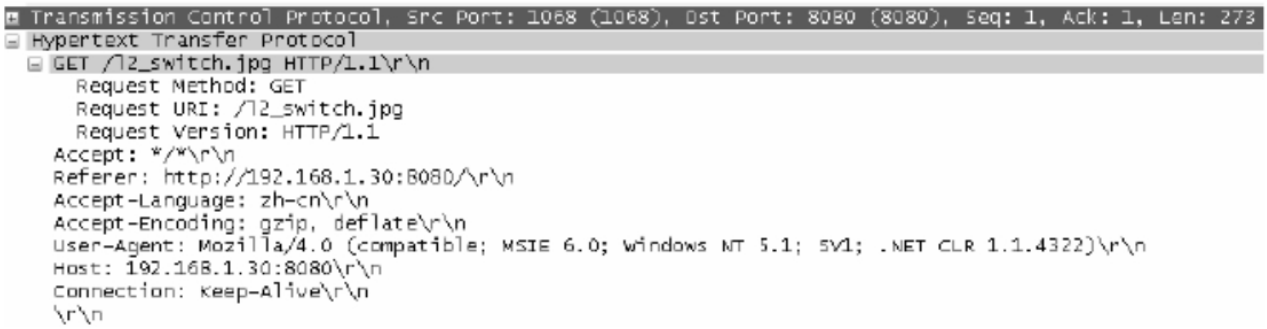
② 状态行也有三个字段：

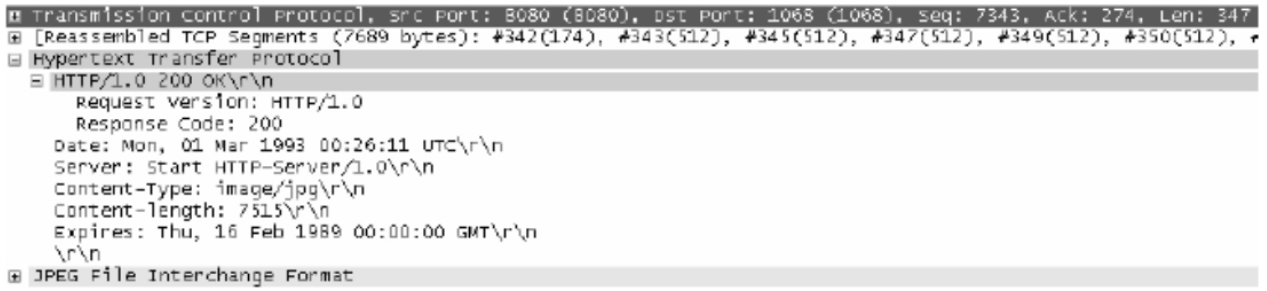
- 第一个字段等同请求行的第三字段
- 第二个字段一般为“200”，表示一切正常，状态码共有41 种，常用的有：301（网站已转移），400（服务器无法理解请求报文），404（服务器没有锁请求的对象）等
- 第三个字段时解释状态码的短语

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”方法时，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。





2.2实验环境与说明

（1）实验目的

在PC 机上访问Web 页面，截获报文，分析HTTP 协议的报文格式和HTTP协议的工作过程。

（2）实验设备和连接

本地实验室环境，无须设备连接；

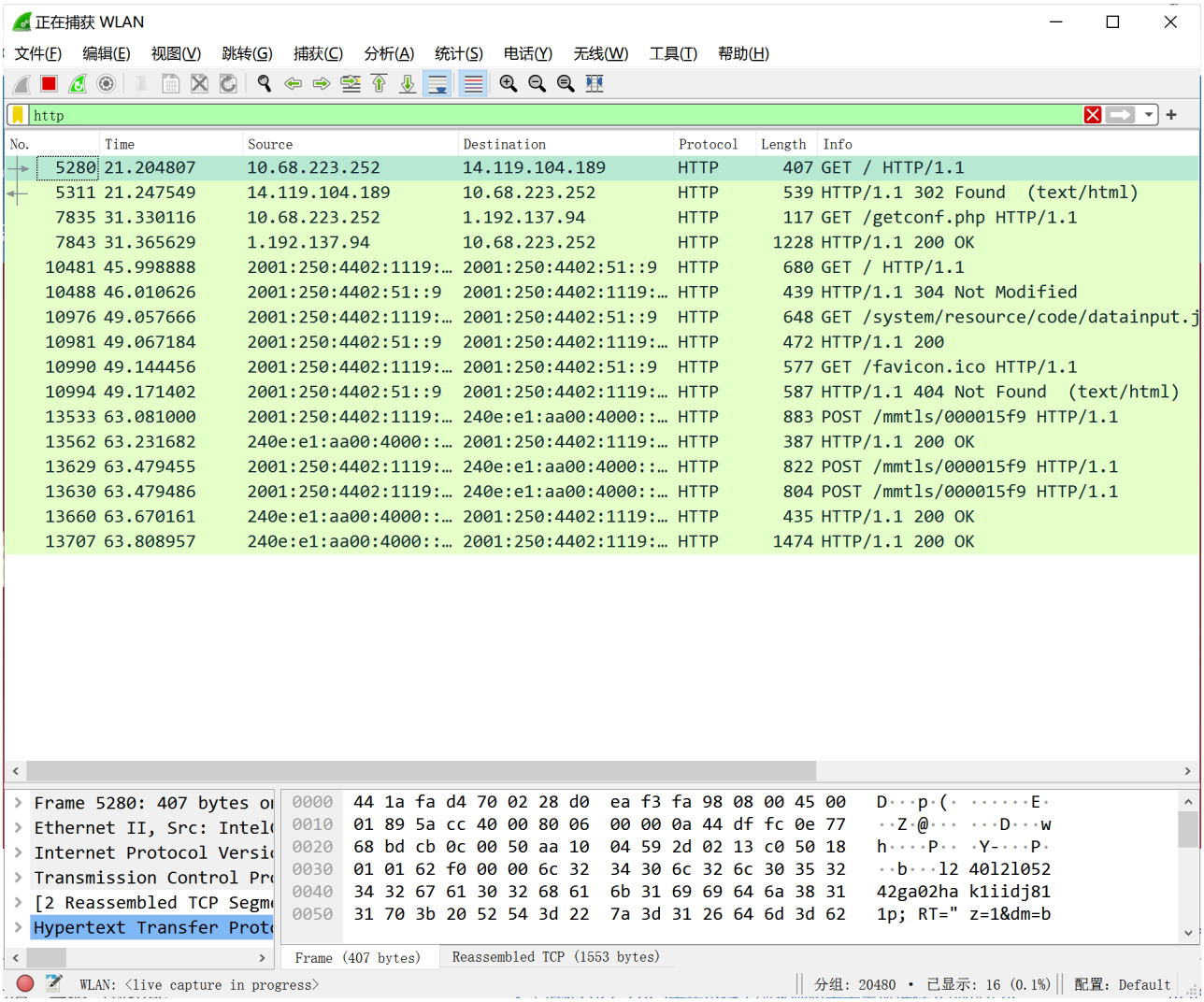
注意：请通过访问可以连接的WWW 站点或使用IIS 建立本地WWW 服务器来进行实验。

（3）实验分组

每四名同学为一组，每人一台计算机独立完成实验。

2.3实验步骤

步骤1：在PC 机上运行Wireshark，开始截获报文；



步骤2：从浏览器上访问Web 界面(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。

步骤3：停止截获报文，将截获的报文命名为http-学号保存。

分析截获的报文，回答以下几个问题：

1）综合分析截获的报文，查看有几种HTTP 报文？

有TCP,DNS,ARP,HTTP,SSL,ICMPV6,TLSv1.3等报文

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。

▲请求报文截图：

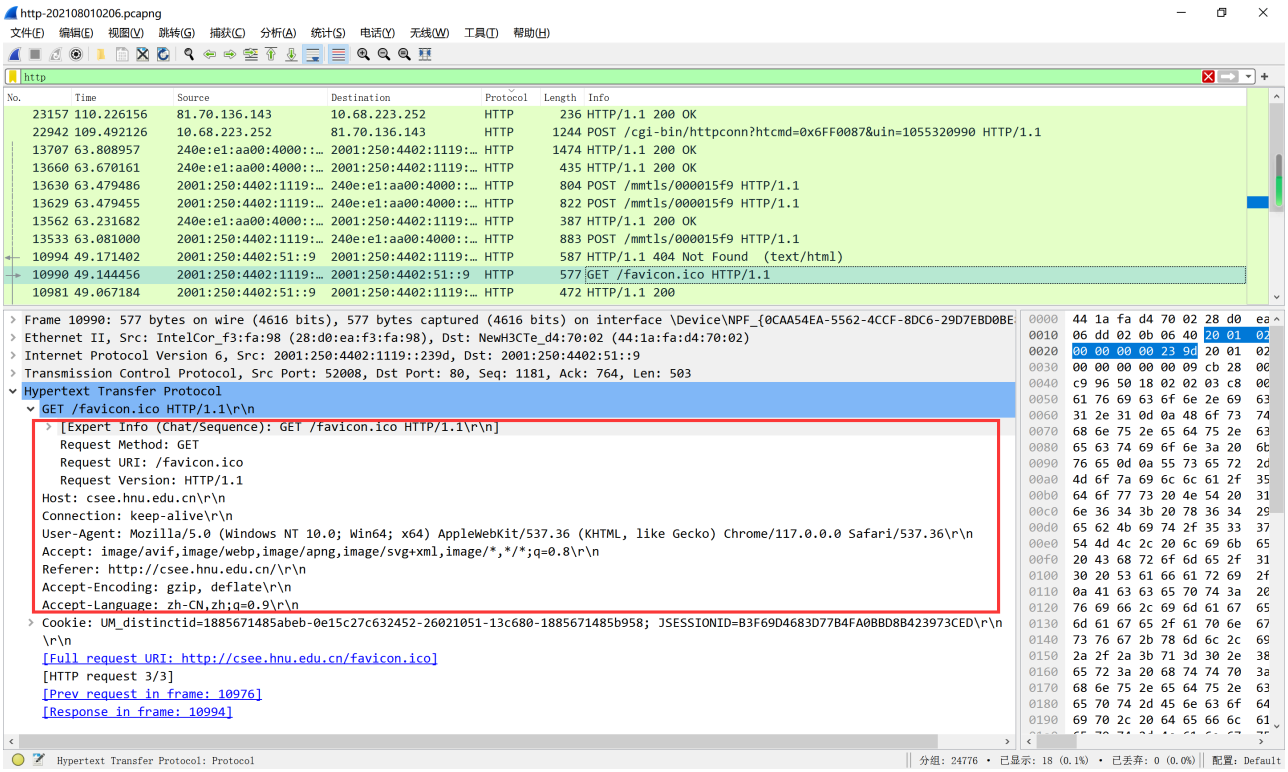


表1.1 HTTP 请求报文格式：

方法：GET

版本：HTTP/1.1

URL： /favicon.ico

首部字段名	字段值	字段所表达的信息
Host	csee.hnu.edu.cn	接收请求的主机名
Connection	keep-alive	表明可用的浏览器类型，这里使用的是
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36	表明可用的浏览器类型，这里使用的是 GoogleChrome 浏览器。

首部字段名	字段值	字段所表达的信息
Accept	image/avif,image/webp,image/apng,image/svg+xml,image/,/*;q=0.8	描述接收响应数据的数据类型，q表示相对质量因子，指示接收数据类型的优先级
Referer	http://csee.hnu.edu.cn/	提供访问来源信息，即从那里来到的这个页面
Accept-Encoding	gzip, deflate	表示客户端可处理的压缩编码
Accept-Language	zh-CN,zh;q=0.9	接收的语言类型

▲回复报文截图：

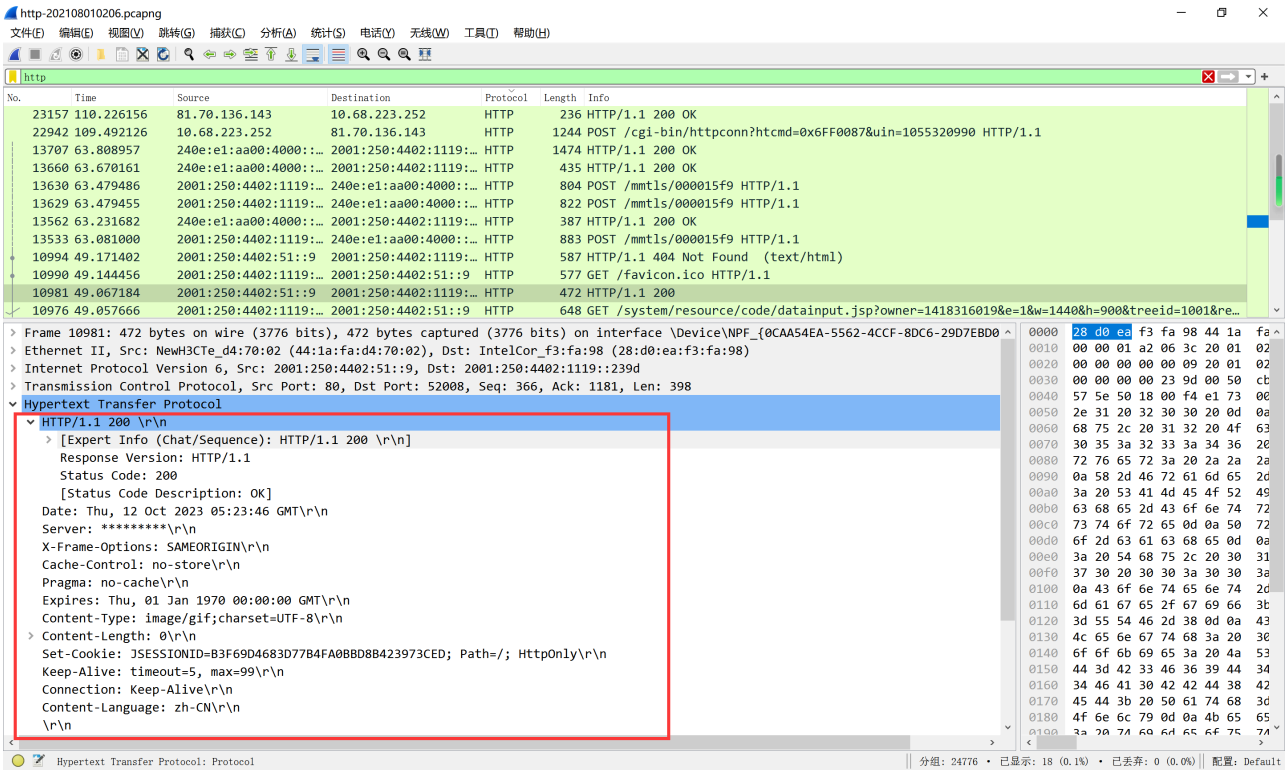


表1.2 HTTP 应答报文格式：

版本：HTTP/1.1

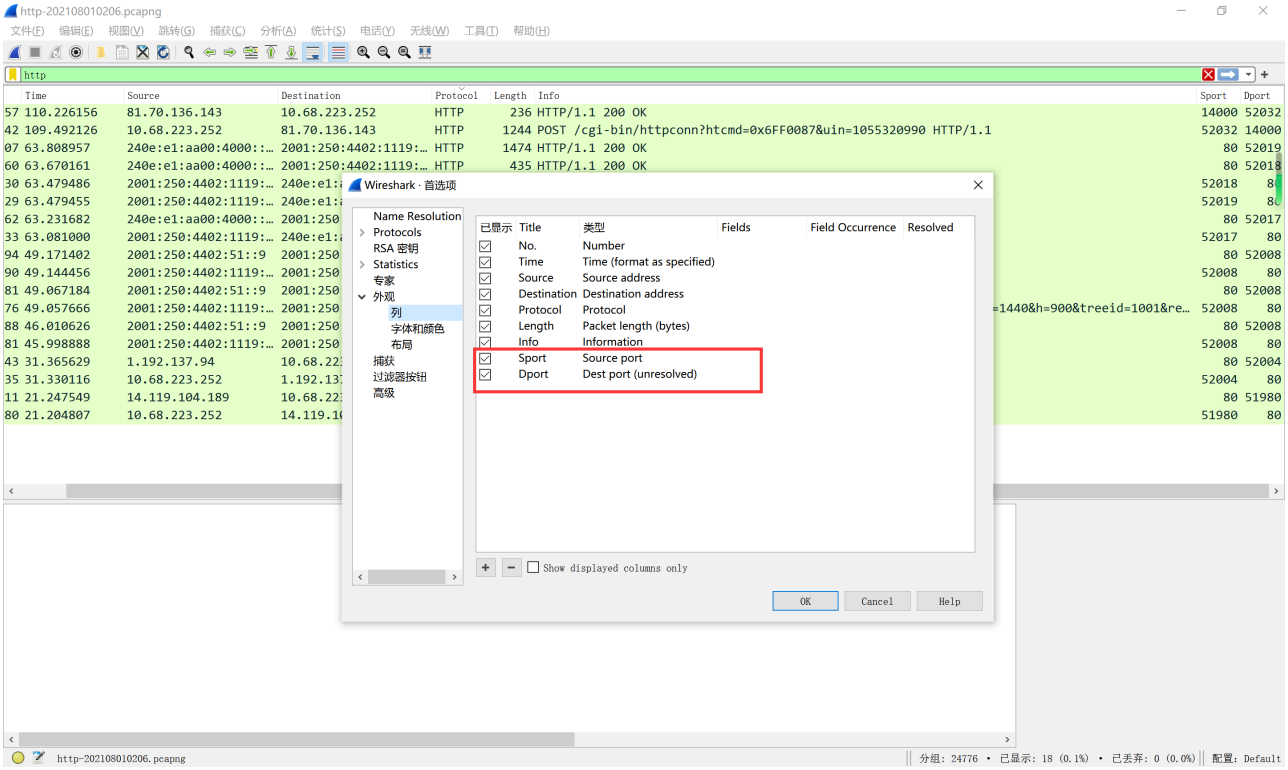
状态码：200

短语：OK

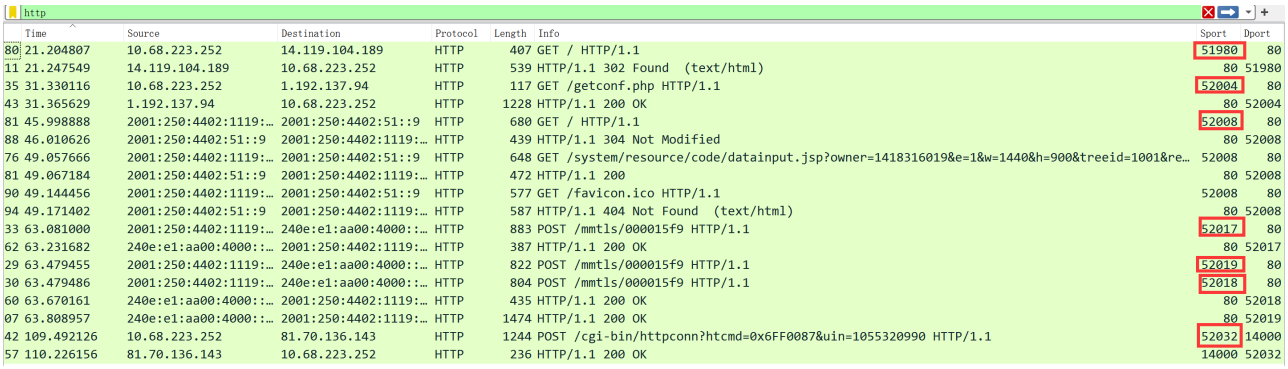
首部字段名	字段值	字段所表达的信息
Date	Thu, 12 Oct 2023 05:23:46 GMT	响应时间
Server	*****	服务器应用程序
X-Frame-Options	SAMEORIGIN	表示该页面可以在相同域名页面的frame中展示（即可以在同域名页面的frame中嵌套）
Cache-Control	no-store	指定不缓存响应，表明资源不进行缓存
Pragma	no-cache	在 HTTP/1.1 协议中，它的含义和 Cache-Control:no-cache 相同
Expires	Thu, 01 Jan 1970 00:00:00 GMT	过期时间
Content-Type	image/gif;charset=UTF-8	实体的内容类型
Content-Length	0	实体的字节大小
Set-Cookie	JSESSIONID=B3F69D4683D77B4FA0BBD8B423973CED; Path=/; HttpOnly	cookie值
Keep-Alive	timeout=5, max=99	持续连接的参数
Connection	Keep-Alive	建立持续链接
Content-Language	zh-CN	实体的语言

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？

★菜单栏“编辑”，“首选项”，“外观”，“列”中添加两项，就可以查看端口和端口号了。这一步灵感来源于https://blog.csdn.net/h1580824951/article/details/120333571



按照以上方式可得到所有HTTP报文对应的端口号



	Time	Source	Destination	Protocol	Length	Info	Sport	Dport
80	21.204807	10.68.223.252	14.119.104.189	HTTP	407	GET / HTTP/1.1	51980	80
11	21.247549	14.119.104.189	10.68.223.252	HTTP	539	HTTP/1.1 302 Found (text/html)	80	51980
35	31.330116	10.68.223.252	1.192.137.94	HTTP	117	GET /getconf.php HTTP/1.1	52004	80
43	31.365629	1.192.137.94	10.68.223.252	HTTP	1228	HTTP/1.1 200 OK	80	52004
81	45.998888	2001:250:4402:1119:...	2001:250:4402:51::9	HTTP	680	GET / HTTP/1.1	52008	80
88	46.010626	2001:250:4402:51::9	2001:250:4402:1119:...	HTTP	439	HTTP/1.1 304 Not Modified	80	52008
76	49.057666	2001:250:4402:1119:...	2001:250:4402:51::9	HTTP	648	GET /system/resource/code/datainput.jsp?owner=1418316019&e=1&w=1440&h=900&treeid=1001&re...	52008	80
81	49.067184	2001:250:4402:51::9	2001:250:4402:1119:...	HTTP	472	HTTP/1.1 200	80	52008
90	49.144456	2001:250:4402:1119:...	2001:250:4402:51::9	HTTP	577	GET /favicon.ico HTTP/1.1	52008	80
94	49.171402	2001:250:4402:51::9	2001:250:4402:1119:...	HTTP	587	HTTP/1.1 404 Not Found (text/html)	80	52008
33	63.081000	2001:250:4402:1119:...	240e:e1:aa00:4000::...	HTTP	883	POST /mmtls/000015f9 HTTP/1.1	52017	80
62	63.231682	240e:e1:aa00:4000::...	2001:250:4402:1119:...	HTTP	387	HTTP/1.1 200 OK	80	52017
29	63.479455	2001:250:4402:1119:...	240e:e1:aa00:4000::...	HTTP	822	POST /mmtls/000015f9 HTTP/1.1	52019	80
30	63.479486	2001:250:4402:1119:...	240e:e1:aa00:4000::...	HTTP	804	POST /mmtls/000015f9 HTTP/1.1	52018	80
60	63.670161	240e:e1:aa00:4000::...	2001:250:4402:1119:...	HTTP	435	HTTP/1.1 200 OK	80	52018
07	63.808957	240e:e1:aa00:4000::...	2001:250:4402:1119:...	HTTP	1474	HTTP/1.1 200 OK	80	52019
42	109.492126	10.68.223.252	81.70.136.143	HTTP	1244	POST /cgi-bin/httpconn?htcmd=0x6FF0087&uin=1055320990 HTTP/1.1	52032	14000
57	110.226156	81.70.136.143	10.68.223.252	HTTP	236	HTTP/1.1 200 OK	14000	52032

答案如下：

> 客户机与服务器建立了7个连接，
> 服务器使用的都是端口号80，
> 用户机使用了端口号51900，52004，52008，52017，52019，52018，52032
> 其中三次使用52008是TCP的三次握手

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。

实际上，由于我的页面打开初始是www.baidu.com，所以上面的初始一部分实际上在跟www.baidu.com进行通讯。我略去这一过程，只关注与http://csee.hnu.edu.cn进行通讯的过程。

注意到这里报文类型实际上也是一个需要关注的点，故加入这一列。另由于端口过多，只关注部分端口（尤其是端口52019，另外的52108、52107与这个类似）的连接与断开。

HTTP客户机端口号	**HTTP**服务机端口号	所包括的报文号	报文类型	步骤说明
58508	53	10337	DNS	请求报文
53	58508	10352	DNS	DNS响应报文，返回域名对应的IP地址
52008	80	10477	TCP	SYN报文，请求建立与服务器的连接
80	52008	10479	TCP	SYN ACK报文，允许客户与服务器建立连接
52008	80	10480	TCP	对SYN ACK的确认，连接已建立
52008	80	10481	HTTP	对网页的请求报文
80	52008	10488	HTTP	响应报文
52019	80	13629	HTTP	请求报文
80	52019	13707	HTTP	响应报文
52019	80	13708	TCP	ACK报文
80	52019	13709	TCP	FIN ACK报文（服务端发的第一个释放连接的请求）
52019	80	13710	TCP	ACK报文（客户端给服务端回应确认消息）
52019	80	13711	TCP	FIN ACK报文（客户端发给服务端释放连接的请求）
80	52019	13727	TCP	RST报文（本来应该是ACK表示服务端发确认消息，这里是连接突然终止了）

上面只重点列出了一个TCP连接的建立和释放的过程，其他两个连接是类似的，以上报文体现了HTTP的工作过程。

特别需要指出的是：典型的关闭请求，有时由客户端发起中断连接。但在这里的关闭请求由服务端发起，即http://csee.hnu.edu.cn主动发起并请求中断TCP连接。

★中间解题过程与截图如下：

DNS部分略

TCP三次握手建立连接

10361	45.167428	220.181.38.156	10.68.223.252	TLSv1.2	88	Application Data	443 → 52007
10362	45.167520	10.68.223.252	220.181.38.156	TCP	54	52007 → 443 [ACK] Seq=2112 Ack=6016 Win=131…	52007 → 443
10366	45.186768	220.181.38.156	10.68.223.252	TCP	88	[TCP Spurious Retransmission] 443 → 52007 […	443 → 52007
10367	45.186814	10.68.223.252	220.181.38.156	TCP	66	[TCP Dup ACK 10362#1] 52007 → 443 [ACK] Seq…	52007 → 443
10477	45.989218	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	86	52008 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=…	52008 → 80
10478	45.990338	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	86	52009 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=…	52009 → 80
10479	45.998604	2001:250:4402:51::9	2001:250:4402:1119:…	TCP	86	80 → 52008 [SYN, ACK] Seq=0 Ack=1 Win=28800…	80 → 52008
10480	45.998663	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	52008 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len…	52008 → 80
10481	45.998888	2001:250:4402:1119:…	2001:250:4402:51::9	HTTP	680	GET / HTTP/1.1	52008 → 80
10485	46.008057	2001:250:4402:51::9	2001:250:4402:1119:…	TCP	86	80 → 52009 [SYN, ACK] Seq=0 Ack=1 Win=28800…	80 → 52009
10486	46.008134	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	52009 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len…	52009 → 80
10487	46.009505	2001:250:4402:51::9	2001:250:4402:1119:…	TCP	74	80 → 52008 [ACK] Seq=1 Ack=607 Win=30080 Le…	80 → 52008
10488	46.010626	2001:250:4402:51::9	2001:250:4402:1119:…	HTTP	439	HTTP/1.1 304 Not Modified	80 → 52008
10490	46.024492	42.194.252.230	10.68.223.252	TCP	406	14000 → 50058 [PSH, ACK] Seq=3521 Ack=118 W…	14000 → 50058
10495	46.033560	10.68.223.252	142.251.42.238	TCP	66	52010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS…	52010 → 443
10497	46.054202	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	52008 → 80 [ACK] Seq=607 Ack=366 Win=132096…	52008 → 80
10501	46.066585	10.68.223.252	42.194.252.230	TCP	54	50058 → 14000 [ACK] Seq=118 Ack=3873 Win=51…	50058 → 14000

52017，52018，52019端口的结束报文

tcp.connection.fin

No.	Time	Source	Destination	Protocol	Length	Info	Sport	Dport
12915	59.886799	240e:97c:2f:2::5c	2001:250:4402:1119:…	TCP	74	443 → 52016 [FIN, ACK] Seq=362 Ack=1848 Win…	443	52016
12920	59.887381	2001:250:4402:1119:…	240e:97c:2f:2::5c	TCP	74	52016 → 443 [FIN, ACK] Seq=1879 Ack=363 Win…	52016	443
13563	63.231682	240e:e1:aa00:4000::…	2001:250:4402:1119:…	TCP	74	80 → 52017 [FIN, ACK] Seq=314 Ack=810 Win=6…	80	52017
13565	63.232158	2001:250:4402:1119:…	240e:e1:aa00:4000::…	TCP	74	52017 → 80 [FIN, ACK] Seq=810 Ack=315 Win=6…	52017	80
13661	63.670317	240e:e1:aa00:4000::…	2001:250:4402:1119:…	TCP	74	80 → 52018 [FIN, ACK] Seq=362 Ack=731 Win=6…	80	52018
13663	63.670783	2001:250:4402:1119:…	240e:e1:aa00:4000::…	TCP	74	52018 → 80 [FIN, ACK] Seq=731 Ack=363 Win=6…	52018	80
13709	63.809114	240e:e1:aa00:4000::…	2001:250:4402:1119:…	TCP	74	80 → 52019 [FIN, ACK] Seq=5661 Ack=749 Win=…	80	52019
13711	63.809412	2001:250:4402:1119:…	240e:e1:aa00:4000::…	TCP	74	52019 → 80 [FIN, ACK] Seq=749 Ack=5662 Win=…	52019	80
14924	70.081210	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	52008 → 80 [FIN, ACK] Seq=1684 Ack=2718 Win…	52008	80
14983	70.380413	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	[TCP Retransmission] 52008 → 80 [FIN, ACK] …	52008	80
15100	70.990233	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	[TCP Retransmission] 52008 → 80 [FIN, ACK] …	52008	80
15336	72.190360	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	[TCP Retransmission] 52008 → 80 [FIN, ACK] …	52008	80
15802	74.592126	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	[TCP Retransmission] 52008 → 80 [FIN, ACK] …	52008	80
15924	75.167865	220.181.38.156	10.68.223.252	TCP	60	443 → 52007 [FIN, ACK] Seq=6047 Ack=2112 Wi…	443	52007
15928	75.189773	220.181.38.156	10.68.223.252	TCP	60	[TCP Retransmission] 443 → 52007 [FIN, ACK]…	443	52007
16882	79.392945	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	[TCP Retransmission] 52008 → 80 [FIN, ACK] …	52008	80
21800	105.018255	2001:250:4402:1119:…	240e:97c:2f:2::5c	TCP	74	52031 → 443 [FIN, ACK] Seq=17150 Ack=362 Wi…	52031	443
21801	105.019726	240e:97c:2f:2::5c	2001:250:4402:1119:…	TCP	74	443 → 52031 [FIN, ACK] Seq=362 Ack=17119 Wi…	443	52031
23091	109.898488	240e:97c:2f:2::5c	2001:250:4402:1119:…	TCP	74	443 → 52033 [FIN, ACK] Seq=362 Ack=14235 Wi…	443	52033
23094	109.899239	2001:250:4402:1119:…	240e:97c:2f:2::5c	TCP	74	52033 → 443 [FIN, ACK] Seq=14266 Ack=363 Wi…	52033	443
23763	113.580041	2001:250:4402:1119:…	240e:97c:2f:2::5c	TCP	74	52035 → 443 [FIN, ACK] Seq=2676 Ack=362 Win…	52035	443
23765	113.588704	240e:97c:2f:2::5c	2001:250:4402:1119:…	TCP	74	443 → 52035 [FIN, ACK] Seq=362 Ack=2645 Win…	443	52035

52019端口：RST报文

tcp.connection.rst

No.	Time	Source	Destination	Protocol	Length	Info	Sport	Dport
2262	5.888515	10.68.223.252	14.119.104.254	TCP	54	51957 → 443 [RST, ACK] Seq=7317 Ack=186327 …	51957	443
4444	17.025497	64.233.188.188	10.68.223.252	TCP	60	5228 → 51971 [RST] Seq=7422 Win=0 Len=0	5228	51971
5805	21.889448	10.68.223.252	14.215.178.125	TCP	54	51990 → 443 [RST, ACK] Seq=2808 Ack=5562 Wi…	51990	443
6506	23.525878	10.68.223.252	14.215.178.125	TCP	54	51995 → 443 [RST, ACK] Seq=11555 Ack=384 Wi…	51995	443
6616	24.570441	10.68.223.252	14.119.104.189	TCP	54	51989 → 443 [RST, ACK] Seq=3067 Ack=74958 W…	51989	443
6634	24.573370	10.68.223.252	14.119.104.189	TCP	54	51984 → 443 [RST, ACK] Seq=7339 Ack=189540 …	51984	443
6635	24.573425	10.68.223.252	14.119.104.254	TCP	54	51994 → 443 [RST, ACK] Seq=3897 Ack=6352 Wi…	51994	443
6636	24.573482	10.68.223.252	14.119.104.189	TCP	54	51991 → 443 [RST, ACK] Seq=1456 Ack=849 Win…	51991	443
6637	24.573521	10.68.223.252	180.101.49.186	TCP	54	51992 → 443 [RST, ACK] Seq=3517 Ack=12766 W…	51992	443
6638	24.573540	10.68.223.252	14.119.104.189	TCP	54	51983 → 443 [RST, ACK] Seq=661 Ack=5457 Win…	51983	443
6643	24.573704	10.68.223.252	14.119.104.254	TCP	54	51987 → 443 [RST, ACK] Seq=5138 Ack=6781 Wi…	51987	443
6651	24.588947	10.68.223.252	14.119.104.254	TCP	54	51988 → 443 [RST, ACK] Seq=8288 Ack=7676 Wi…	51988	443
6660	24.598859	10.68.223.252	14.119.104.189	TCP	54	51982 → 443 [RST, ACK] Seq=645 Ack=5457 Win…	51982	443
6704	24.754716	240e:c3:2c00:303::7…	2001:250:4402:1119:…	TCP	74	443 → 51993 [RST] Seq=68058 Win=0 Len=0	443	51993
7147	27.640236	14.119.104.189	10.68.223.252	TCP	60	80 → 51980 [RST] Seq=487 Win=0 Len=0	80	51980
7851	31.386461	1.192.137.94	10.68.223.252	TCP	60	80 → 52004 [RST] Seq=1176 Win=0 Len=0	80	52004
13683	63.733170	240e:e1:aa00:4000::…	2001:250:4402:1119:…	TCP	74	80 → 52018 [RST] Seq=363 Win=0 Len=0	80	52018
13727	63.868981	240e:e1:aa00:4000::…	2001:250:4402:1119:…	TCP	74	80 → 52019 [RST] Seq=5662 Win=0 Len=0	80	52019
16336	77.007068	172.217.160.74	10.68.223.252	TCP	60	443 → 52023 [RST] Seq=1 Win=0 Len=0	443	52023
16611	78.232348	220.181.38.156	10.68.223.252	TCP	60	443 → 52007 [RST] Seq=6048 Win=0 Len=0	443	52007
18877	89.001502	2001:250:4402:1119:…	2001:250:4402:51::9	TCP	74	52008 → 80 [RST, ACK] Seq=1685 Ack=2718 Win…	52008	80
19388	91.794271	172.217.160.74	10.68.223.252	TCP	60	443 → 52022 [RST] Seq=1 Win=0 Len=0	443	52022

52019端口：正常传输

http

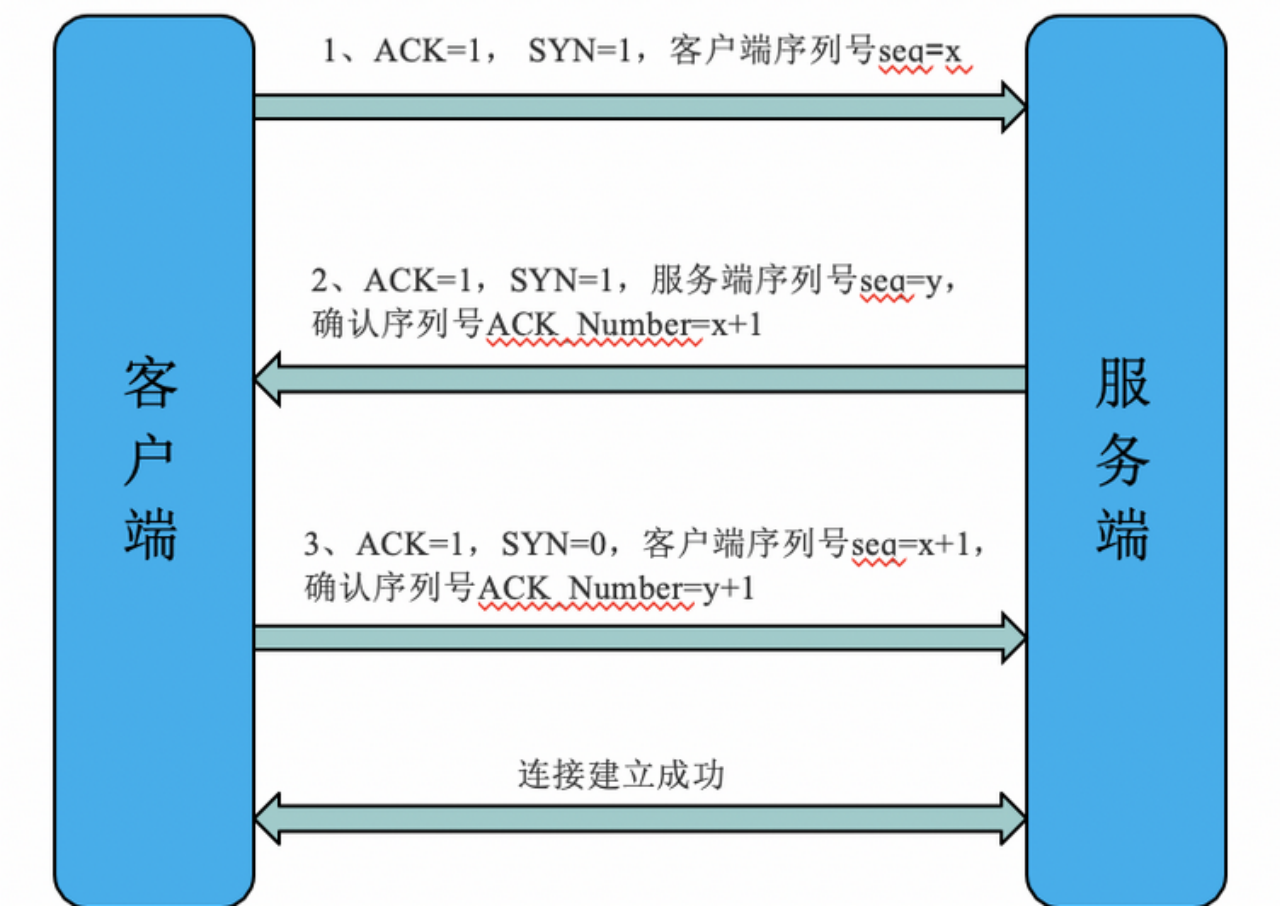
No.	Time	Source	Destination	Protocol	Length	Info	Sport	Dport
5280	21.204807	10.68.223.252	14.119.104.189	HTTP	407	GET / HTTP/1.1	51980	80
5311	21.247549	14.119.104.189	10.68.223.252	HTTP	539	HTTP/1.1 302 Found (text/html)	80	51980
7835	31.330116	10.68.223.252	1.192.137.94	HTTP	117	GET /getconf.php HTTP/1.1	52004	80
7843	31.365629	1.192.137.94	10.68.223.252	HTTP	1228	HTTP/1.1 200 OK	80	52004
10481	45.998888	2001:250:4402:1119:…	2001:250:4402:51::9	HTTP	680	GET / HTTP/1.1	52008	80
10488	46.010626	2001:250:4402:51::9	2001:250:4402:1119:…	HTTP	439	HTTP/1.1 304 Not Modified	80	52008
10976	49.057666	2001:250:4402:1119:…	2001:250:4402:51::9	HTTP	648	GET /system/resource/code/datainput.jsp?own…	52008	80
10981	49.067184	2001:250:4402:51::9	2001:250:4402:1119:…	HTTP	472	HTTP/1.1 200	80	52008
10990	49.144456	2001:250:4402:1119:…	2001:250:4402:51::9	HTTP	577	GET /favicon.ico HTTP/1.1	52008	80
10994	49.171402	2001:250:4402:51::9	2001:250:4402:1119:…	HTTP	587	HTTP/1.1 404 Not Found (text/html)	80	52008
13533	63.081000	2001:250:4402:1119:…	240e:e1:aa00:4000::…	HTTP	883	POST /mmtls/000015f9 HTTP/1.1	52017	80
13562	63.231682	240e:e1:aa00:4000::…	2001:250:4402:1119:…	HTTP	387	HTTP/1.1 200 OK	80	52017
13629	63.479455	2001:250:4402:1119:…	240e:e1:aa00:4000::…	HTTP	822	POST /mmtls/000015f9 HTTP/1.1	52019	80
13630	63.479486	2001:250:4402:1119:…	240e:e1:aa00:4000::…	HTTP	804	POST /mmtls/000015f9 HTTP/1.1	52018	80
13660	63.670161	240e:e1:aa00:4000::…	2001:250:4402:1119:…	HTTP	435	HTTP/1.1 200 OK	80	52018
13707	63.808957	240e:e1:aa00:4000::…	2001:250:4402:1119:…	HTTP	1474	HTTP/1.1 200 OK	80	52019
22942	109.492126	10.68.223.252	81.70.136.143	HTTP	1244	POST /cgi-bin/httpconn?htcmd=0x6FF0087&uin=…	52032	14000
23157	110.226156	81.70.136.143	10.68.223.252	HTTP	236	HTTP/1.1 200 OK	14000	52032

52019端口：四次挥手中的前三次

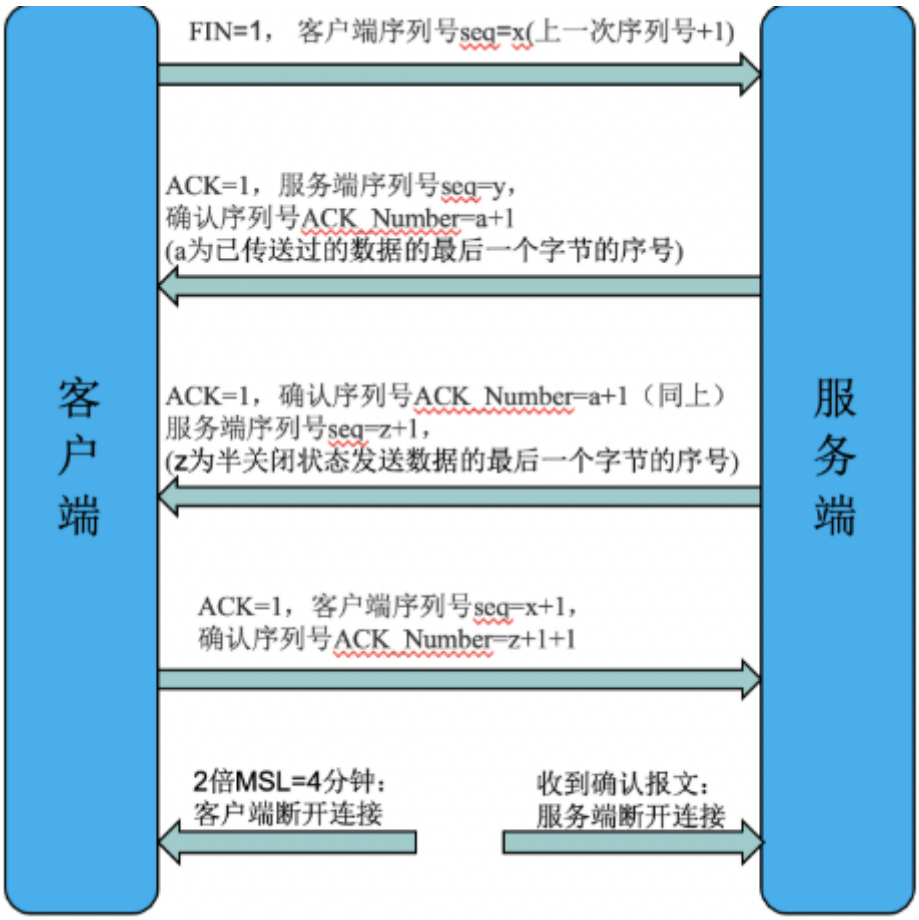
No.	Time	Source	Destination	Protocol	Length	Info	Sport	Dport
13695	63.792418	IntelCor_f3:df:90	Broadcast	ARP	56	Who has 10.69.141.125? Tell 10.68.160.175		
13696	63.792418	d2:f5:f5:cd:cd:c4	Broadcast	ARP	56	Who has 10.68.0.1? Tell 10.68.182.75		
13697	63.792418	CloudNet_23:09:d7	Broadcast	ARP	56	Who has 10.68.149.169? Tell 10.69.211.175		
13698	63.792418	IntelCor_16:1a:c5	Broadcast	ARP	56	Who has 10.69.140.188? Tell 10.68.102.94		
13699	63.792418	CloudNet_23:09:d7	Broadcast	ARP	56	Who has 10.68.149.171? Tell 10.69.211.175		
13700	63.798097	42:80:7c:27:f9:0c	Broadcast	ARP	56	Who has 10.69.47.247? Tell 10.69.233.78		
13701	63.798097	IntelCor_4c:71:97	Broadcast	ARP	56	Who has 10.68.0.1? Tell 10.69.39.252		
13702	63.798119	240e:e1:aa00:4000:…	2001:250:4402:1119:…	TCP	1494	80 → 52019 [ACK] Seq=1 Ack=749 Win=64640 Le…	80	52019
13703	63.798296	240e:e1:aa00:4000:…	2001:250:4402:1119:…	TCP	1494	80 → 52019 [PSH, ACK] Seq=1421 Ack=749 Win=…	80	52019
13704	63.798296	240e:e1:aa00:4000:…	2001:250:4402:1119:…	TCP	1494	80 → 52019 [ACK] Seq=2841 Ack=749 Win=64640…	80	52019
13705	63.798338	2001:250:4402:1119:…	240e:e1:aa00:4000:…	TCP	74	52019 → 80 [ACK] Seq=749 Ack=4261 Win=66560…	52019	80
13706	63.808933	92:02:b1:72:2a:cb	Broadcast	ARP	56	Who has 10.69.168.193? Tell 10.69.120.69		
13707	63.808957	240e:e1:aa00:4000:…	2001:250:4402:1119:…	HTTP	1474	HTTP/1.1 200 OK	80	52019
13708	63.809024	2001:250:4402:1119:…	240e:e1:aa00:4000:…	TCP	74	52019 → 80 [ACK] Seq=749 Ack=5661 Win=65280…	52019	80
13709	63.809114	240e:e1:aa00:4000:…	2001:250:4402:1119:…	TCP	74	80 → 52019 [FIN, ACK] Seq=5661 Ack=749 Win=…	80	52019
13710	63.809139	2001:250:4402:1119:…	240e:e1:aa00:4000:…	TCP	74	52019 → 80 [ACK] Seq=749 Ack=5662 Win=65280…	52019	80
13711	63.809412	2001:250:4402:1119:…	240e:e1:aa00:4000:…	TCP	74	52019 → 80 [FIN, ACK] Seq=749 Ack=5662 Win=…	52019	80
13712	63.813464	a2:80:80:b0:1d:20	Broadcast	ARP	56	Who has 10.69.168.193? Tell 10.68.130.12		

知识补充：三次握手与四次挥手

三次握手



四次挥手



最后的四次挥手原理讲解可以参考如下的讲解

https://blog.csdn.net/weixin_41033105/article/details/123861500

https://blog.csdn.net/m0_52650621/article/details/127797022