

**计算机网络**

**课程实验报告**

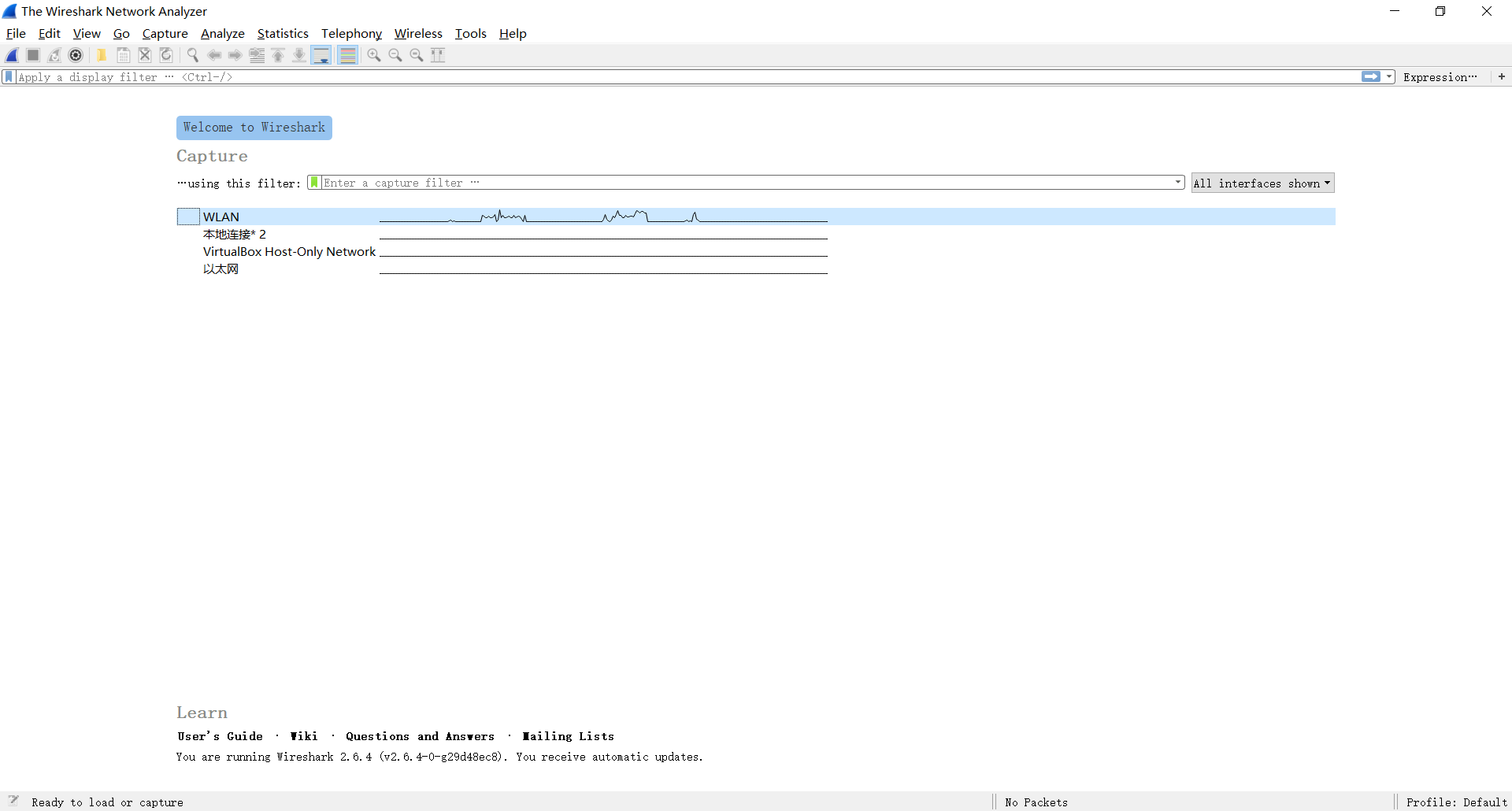
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 实验名称 | 利用 Wireshark 进行协议分析 | | | | | |
| 姓名 | 李国建 | | 院系 | 计算机学院 | | |
| 班级 | 1603107 | | 学号 | 1160300426 | | |
| 任课教师 | 聂兰顺 | | 指导教师 | 聂兰顺 | | |
| 实验地点 | 格物207 | | 实验时间 | 2018/11/23 | | |
| 实验课表现 | 出勤、表现得分(10) |  | 实验报告  得分(40) |  | 实验总分 |  |
| 操作结果得分(50) |  |
| 教师评语 | | | | | | |
|  | | | | | | |

****

|  |
| --- |
| 实验目的： |
| （注：实验报告模板中的各项内容仅供参考，可依照实际实验情况进行修改。）  本次实验的主要目的。  熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间进行交互以及报文交换的情况。 |
| 实验内容： |
| 概述本次实验的主要内容，包含的实验项等。  1) 学习 Wireshark 的使用  2) 利用 Wireshark 分析 HTTP 协议  3) 利用 Wireshark 分析 TCP 协议  4) 利用 Wireshark 分析 IP 协议  5) 利用 Wireshark 分析 Ethernet 数据帧  选做内容：  a) 利用 Wireshark 分析 DNS 协议  b) 利用 Wireshark 分析 UDP 协议  c) 利用 Wireshark 分析 ARP 协议 |
| 实验过程： |
| 以文字描述、实验结果截图等形式阐述实验过程，必要时可附相应的代码截图或以附件形式提交。  实验过程见下方。 |
| 实验结果： |
| 采用演示截图、文字说明等方式，给出本次实验的实验结果。  实验结果见下方。 |
| 问题讨论： |
| 对实验过程中的思考问题进行讨论或回答。  思考问题和回答，见下方。 |
| 心得体会： |
| 结合实验过程和结果给出实验的体会和收获。  本次实验，让我充分了解了网络中的各种协议及其格式，对计算机网络有了进一步的理解。 |

实验过程和实验结果

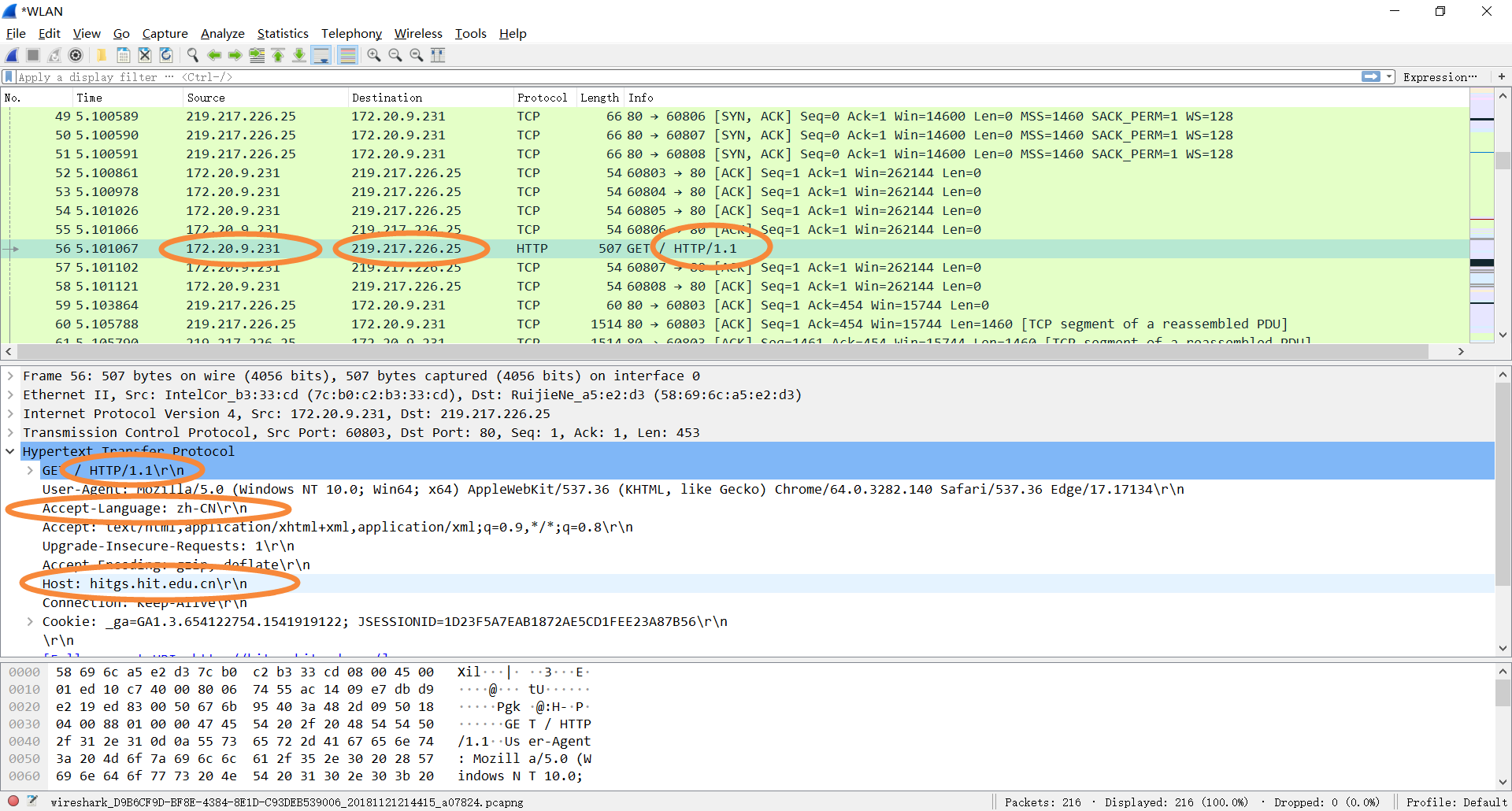
1. Wireshark 的使用



打开 Wireshark， 这里使用的是无线网连接，因此，双击 WLAN 即可进行实验

1. HTTP 分析
2. HTTP GET/response 交互

打开访问 <http://hitgs.hit.edu.cn/>



1. 你的浏览器运行的是 HTTP1.0，还是 HTTP1.1？

HTTP1.1

1. 你所访问的服务 器所运行 HTTP 协议的版本号是多少？

HTTP1.1

1. 你的浏览器向服务器指出它能接收何种语言版本的对象？

简体中文 （zh-CN 代表简体中文）

1. 你的计算机的 IP 地址是多少？

172.20.9.231

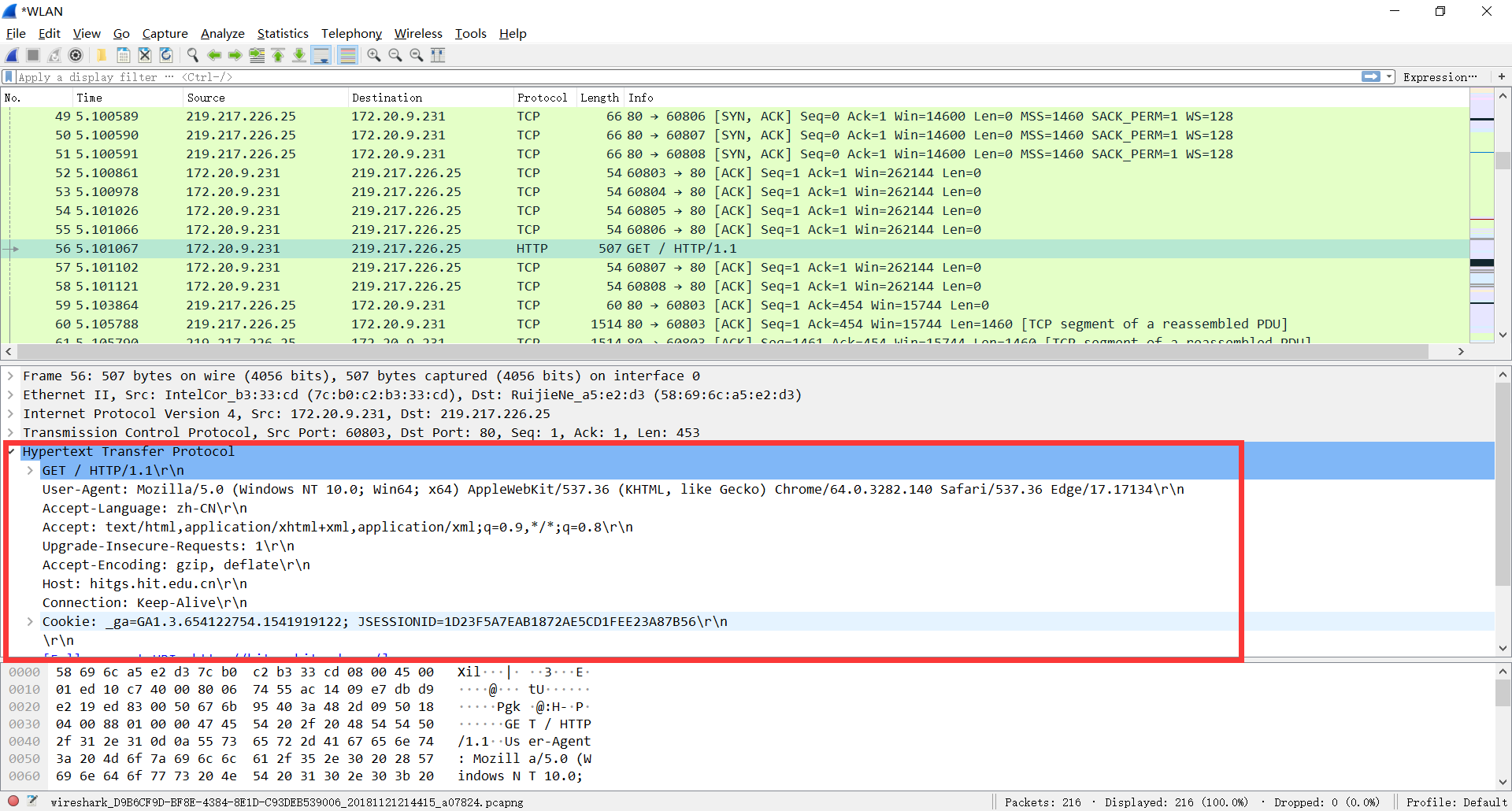
1. 服务器 http://hitgs.hit.edu.cn/ 的 IP 地址是多少？

219.217.226.25

1. 从服务器向你的浏览器返回的状态代码是多少？

200

1. HTTP 条件 GET/response 交互



1. 分析你的浏览器向服务器发出的第一个 HTTP GET 请求的内容， 在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？

没有

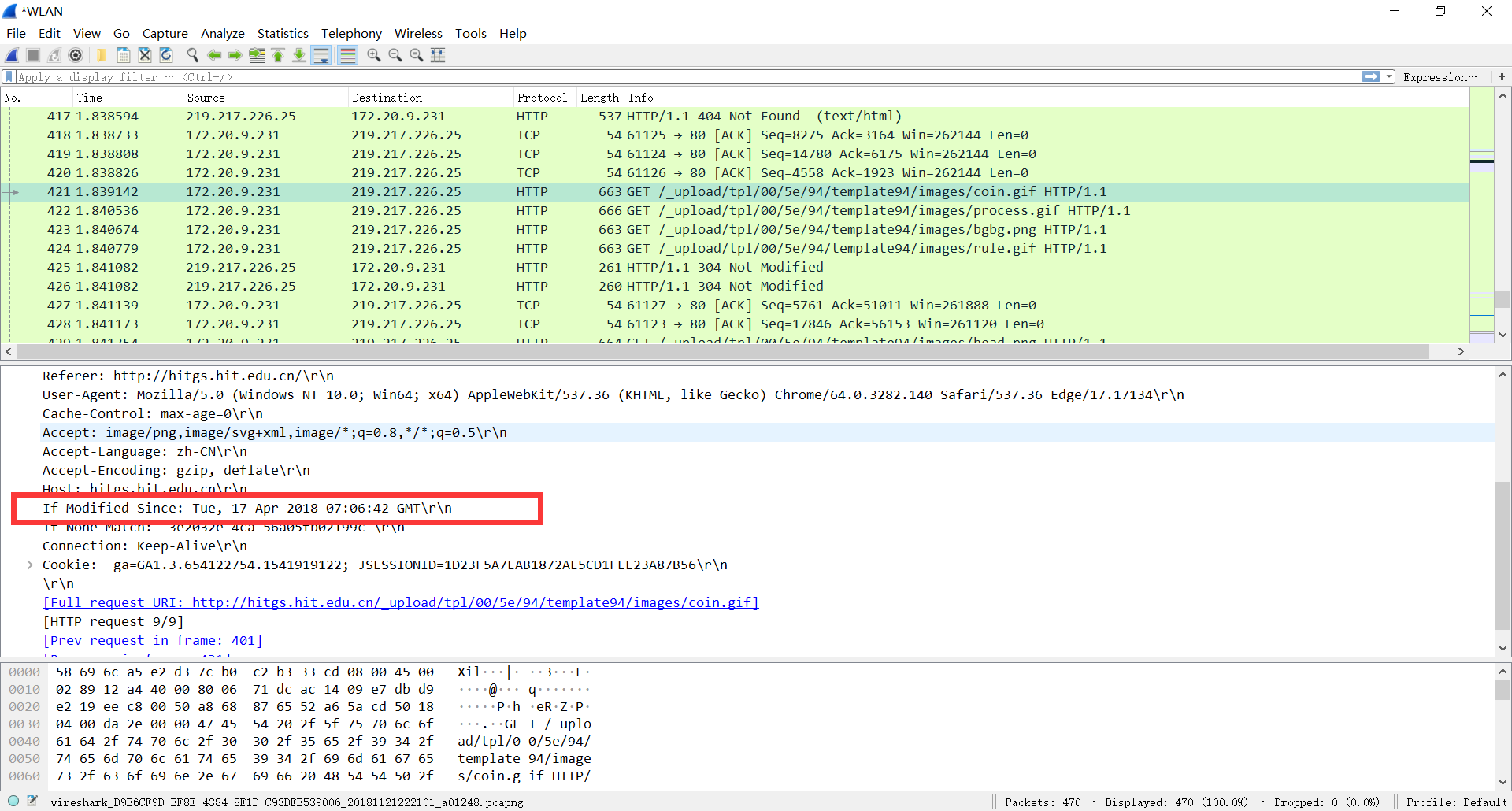
1. 分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？

服务器明确返回了文件的内容

返回的状态码是 200，代表明确返回了文件。

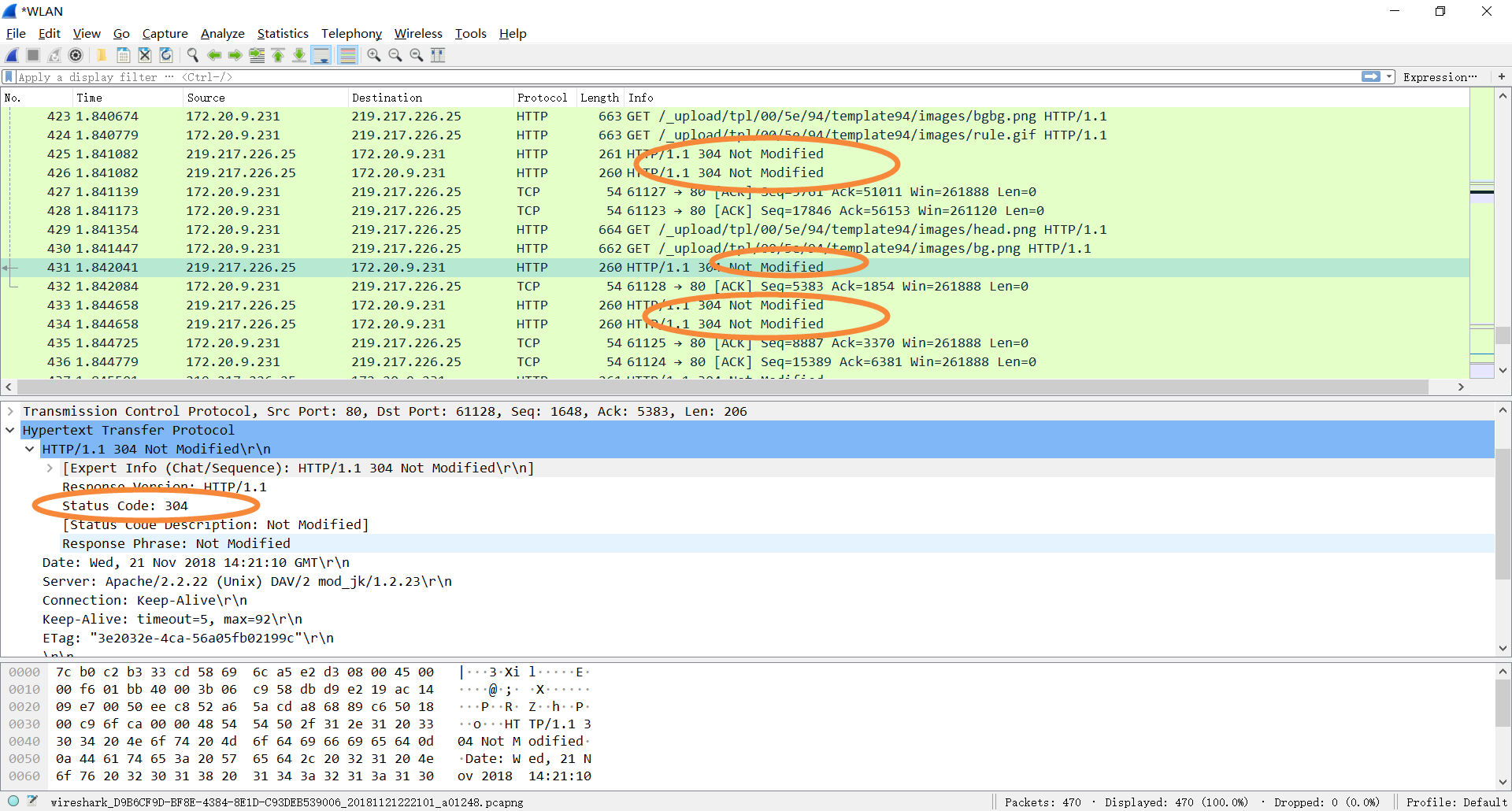
1. 分析你的浏览器向服务器发出的较晚的“HTTP GET”请求，在该请 求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？

有



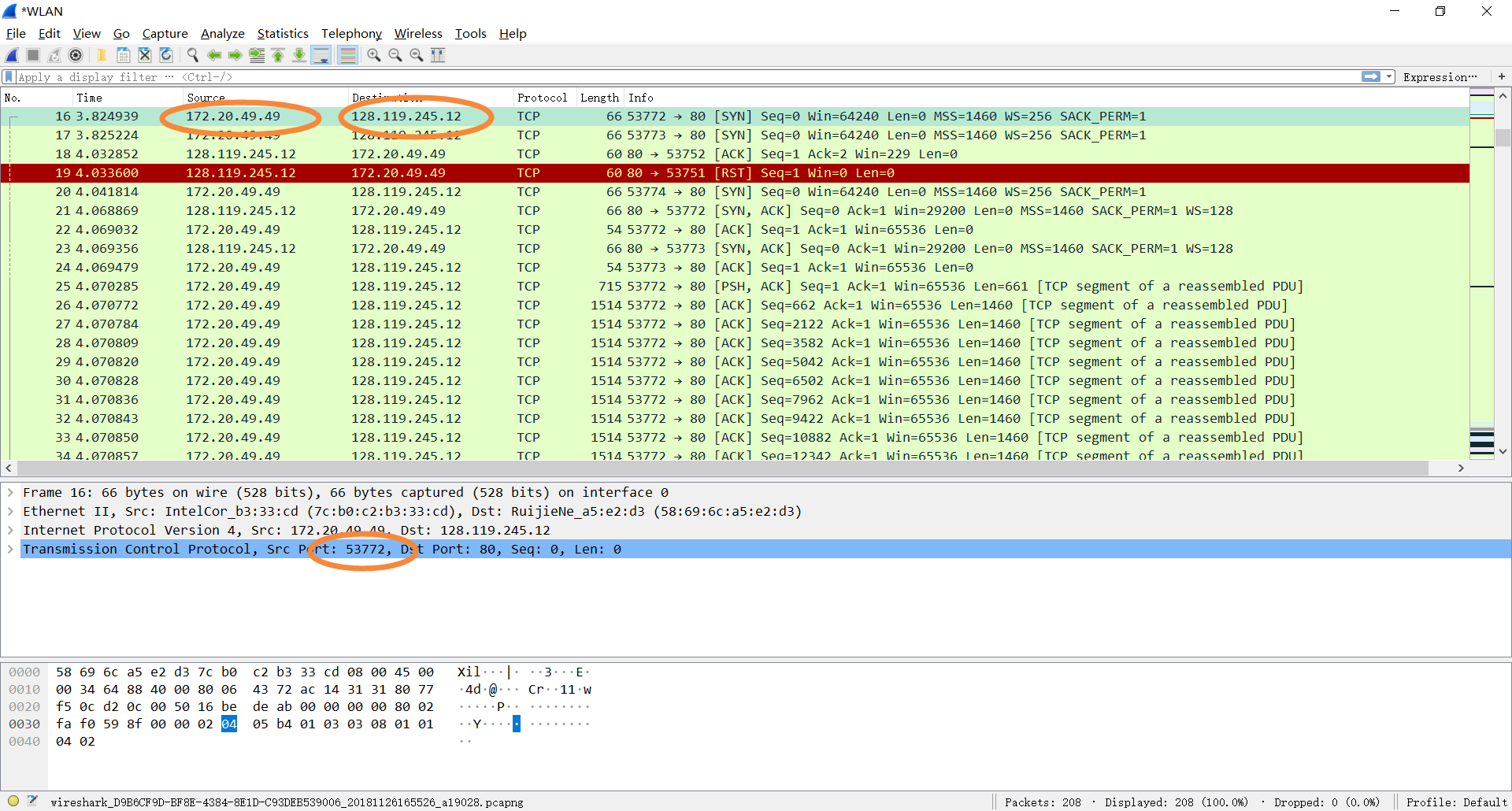
后面跟着的信息是： Tue, 17 Apr 2018 07:06:42 GMT 代表的是时间，缓存最后更新的时间。

1. 服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是多少？服务器是否明确返回了文件的内容？请解释。



请求响应中的 HTTP 状态代码（Status Code）为 304。 不会明确返回文件，因为服务器判断的结果为 Not Modified，客户端可以使用本地没有过期的缓存文件。

1. TCP 分析
2. 俘获大量的由本地主机到远程服务器的 TCP 分组



1. 浏览追踪信息
2. 向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址和 TCP 端口号是多少？

客户端主机的 IP 地址：172.20.49.49

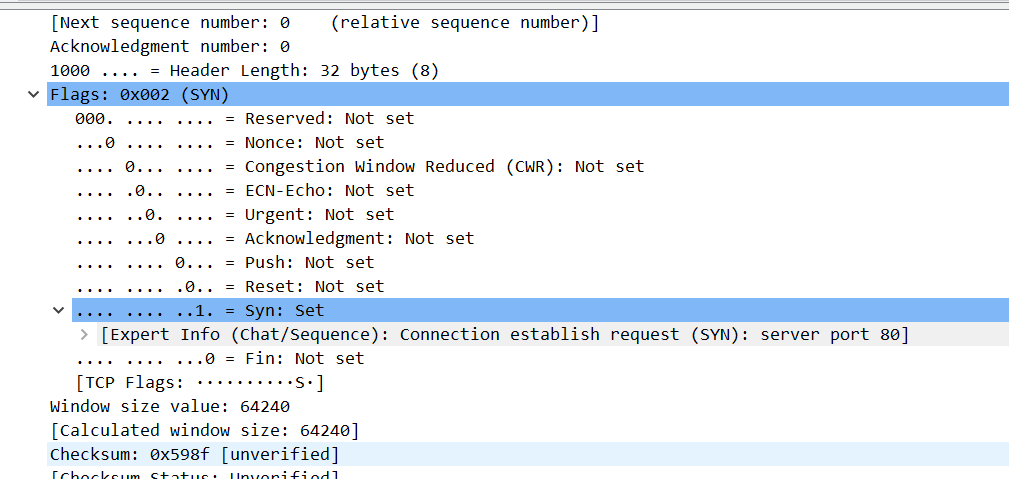
TCP 端口号：53772

1. Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来发送和接收 TCP 报文的端口号是多少？

Gaia.cs.umass.edu 服务器的 IP 地址：128.119.245.12

用来发送和接收 TCP 报文的端口号是：80

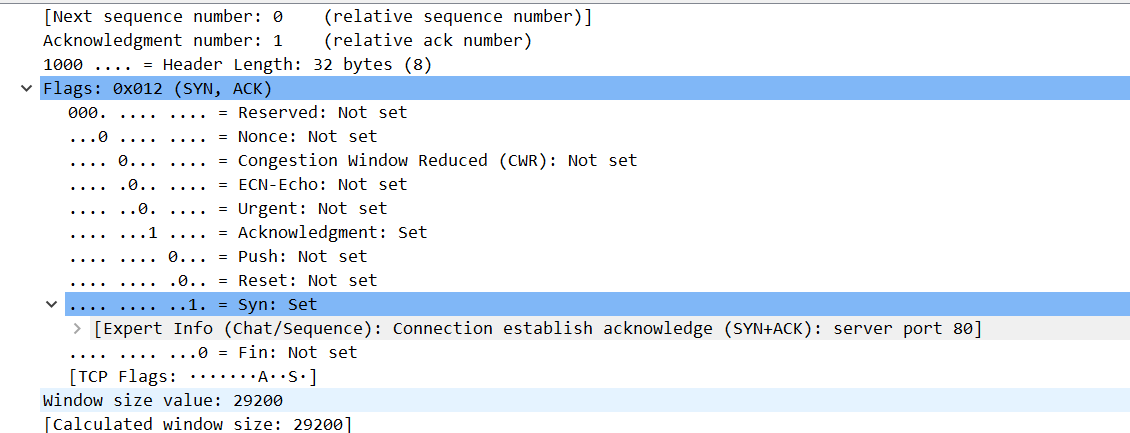
1. TCP 基础
2. 客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号 （sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？



如图，初始化 TCP 连接的 TCP SYN 报文段的序号是 0；

通过 Flags 标志位，表示该报文段是 SYN 报文段（将其中的 SYN 位置为 1）

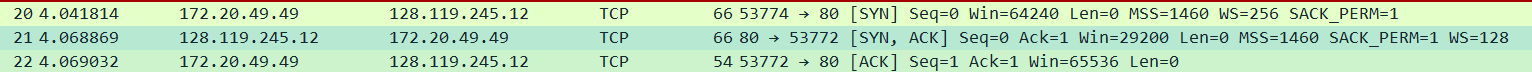
1. 服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段 中，Acknowledgement 字段的值是多少？Gaia.cs.umass.edu 服务器 是如何决定此值的？在该报文段中，是用什么来标示该报文段是 SYNACK 报文段的？



如图所示，服务器端向客户端发送的报文段序号为 0；

服务器发的 acknowledgment number 字段是根据上一次客户端发给服务器的 seq+1 得到的； 通过Flags标志位中的SYN位和ACK位都是1来确定该报文段是一个SYN ACK 报文段的。

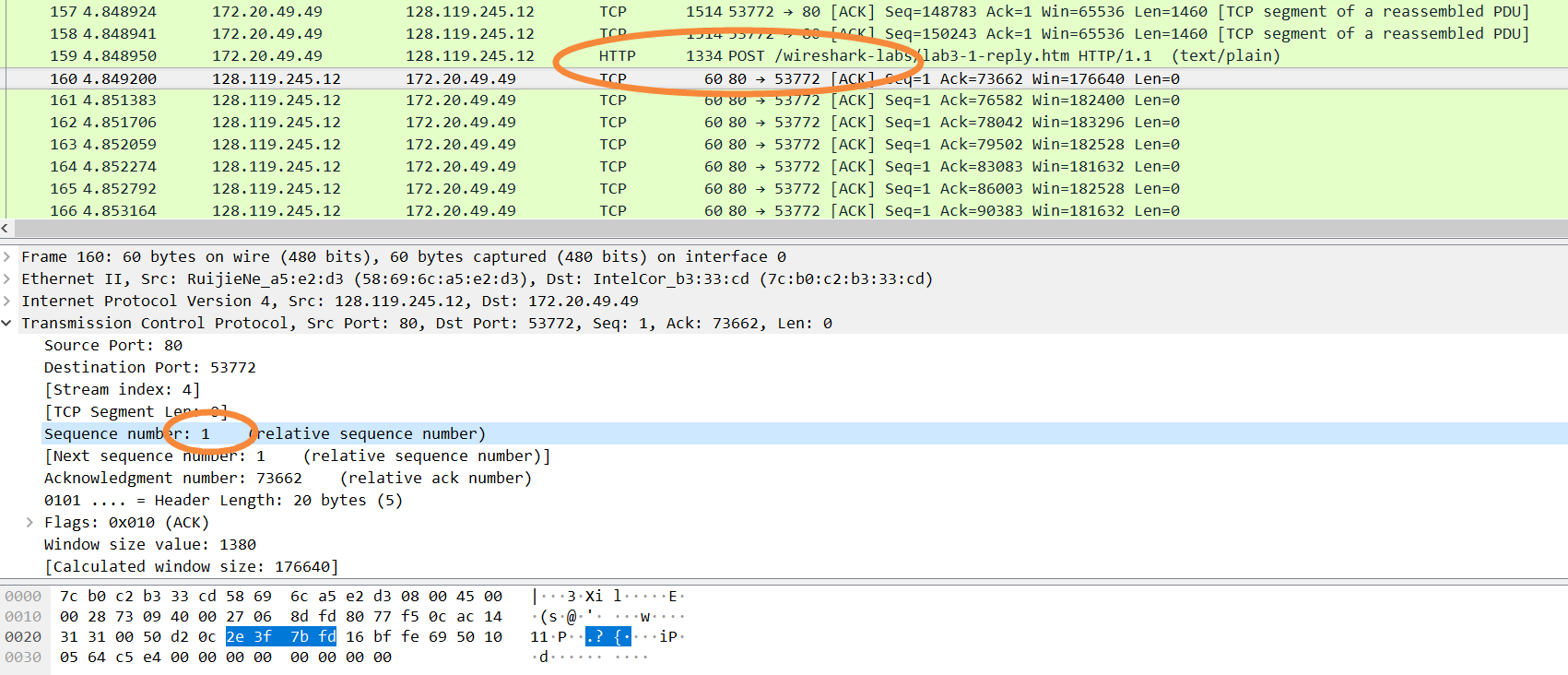
1. 你能从捕获的数据包中分析出 tcp 三次握手过程吗？

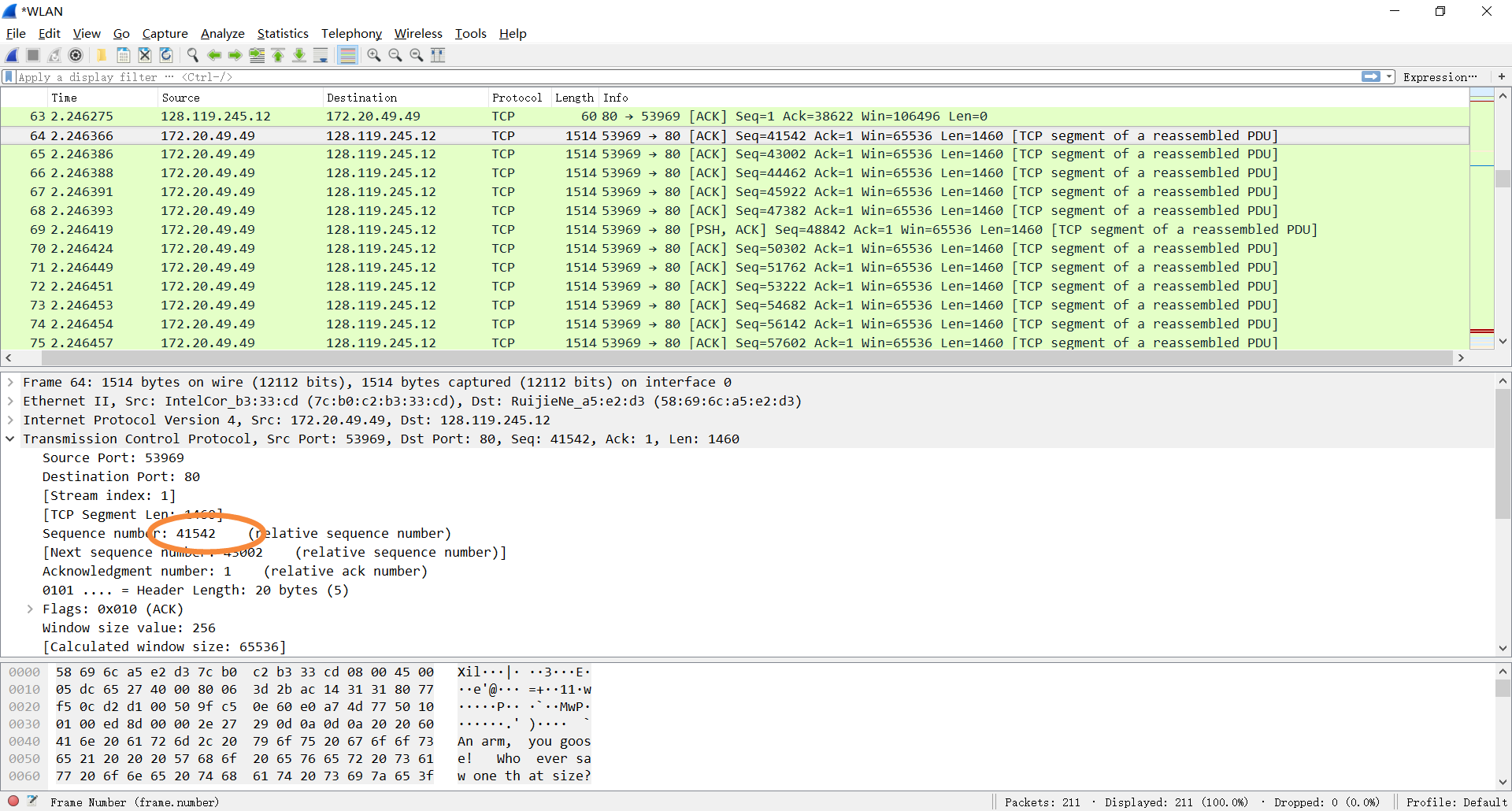


客户端先向服务器发送 seq = 0 的建立连接的请求

然后服务器向客户端返回 seq = 0, ack = 1 的响应

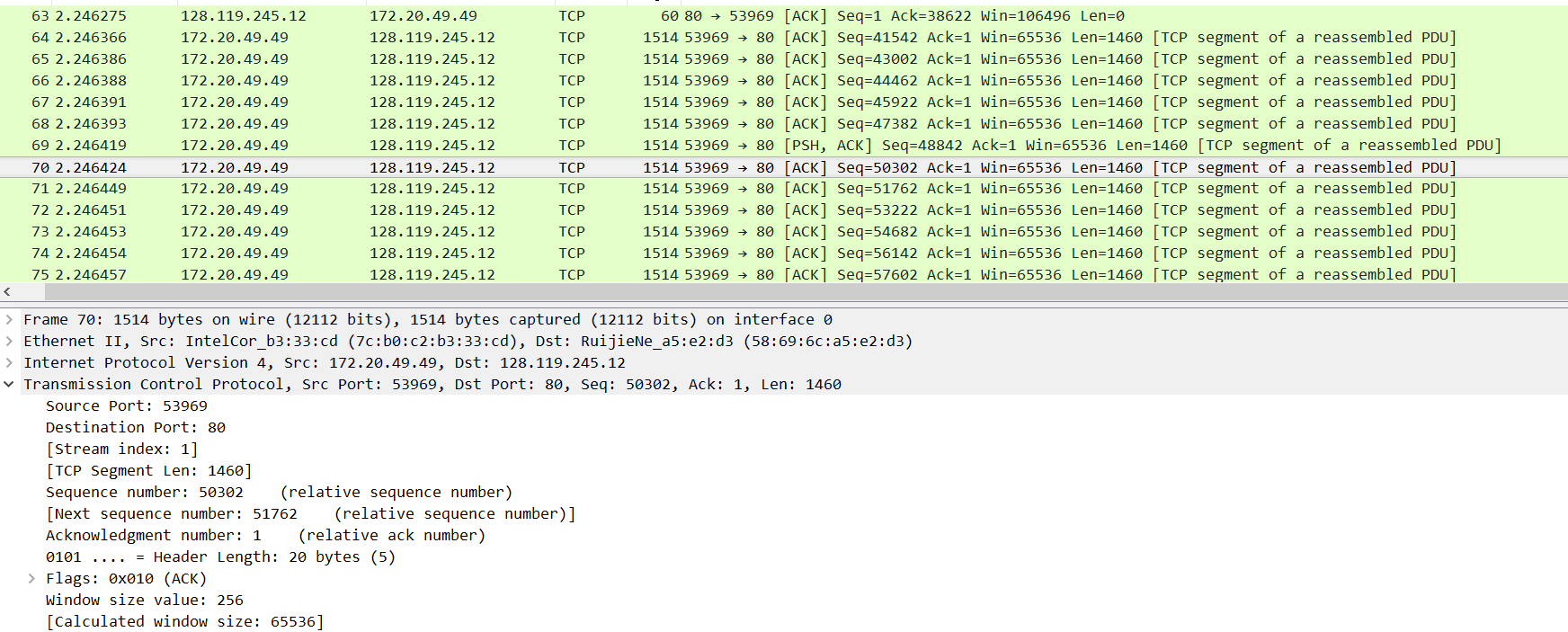
1. 包含 HTTP POST 命令的 TCP 报文段的序号是多少？





序列号是 41542

1. 如果将包含 HTTP POST 命令的 TCP 报文段看作是 TCP 连接上的 第一个报文段，那么该 TCP 连接上的第六个报文段的序号是多少？是何时发送的？该报文段所对应的 ACK 是何时接收的？

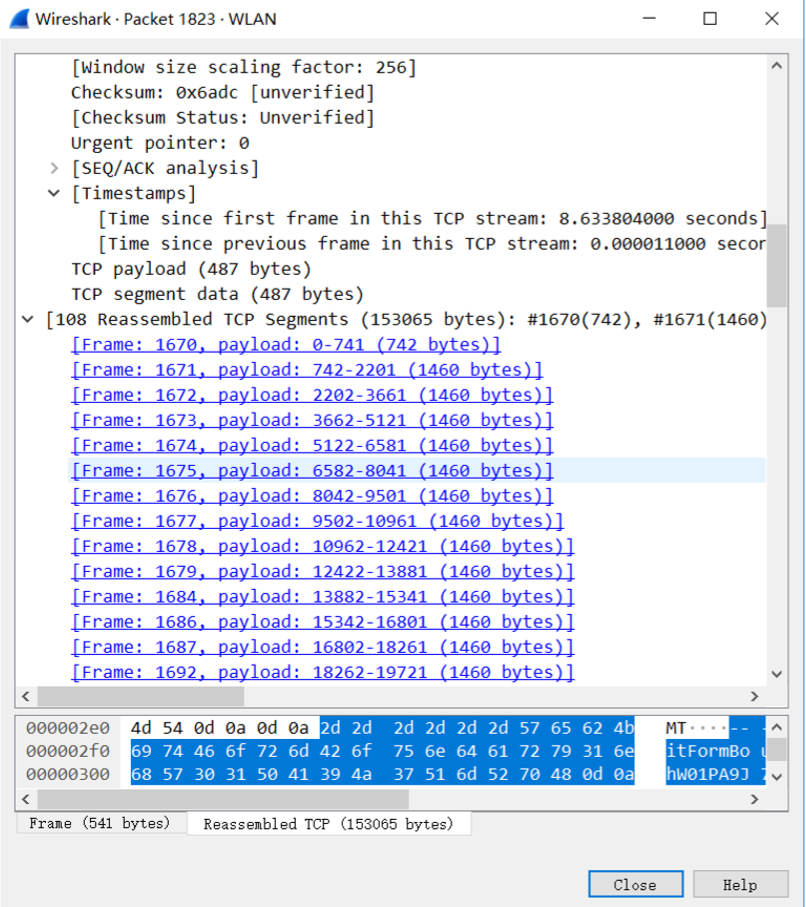


第六个报文段的序号是：5032

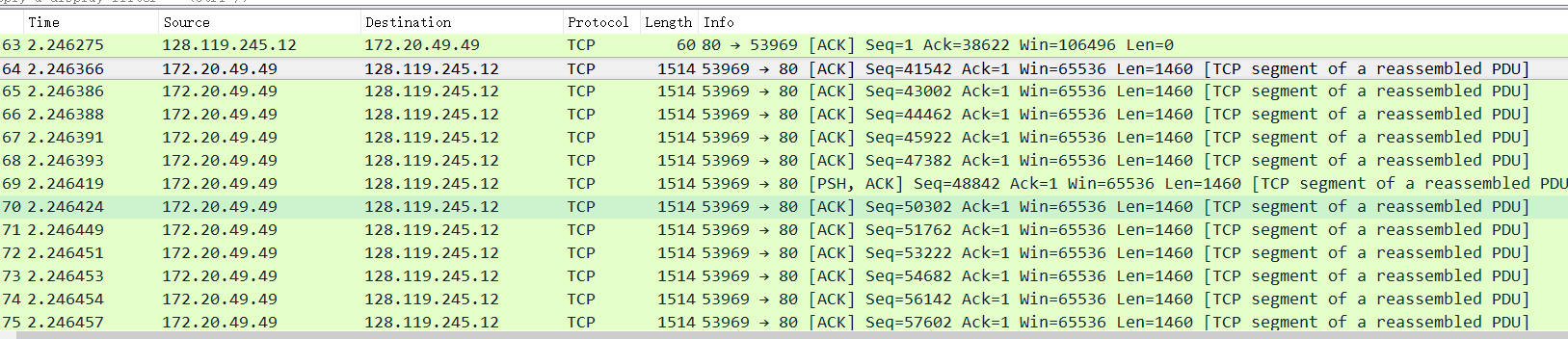
在 http post 发送之前，tcp 连接建立之后发送

对应的 ACK 是服务器返回的第六个 ack

1. 前六个 TCP 报文段的长度各是多少？

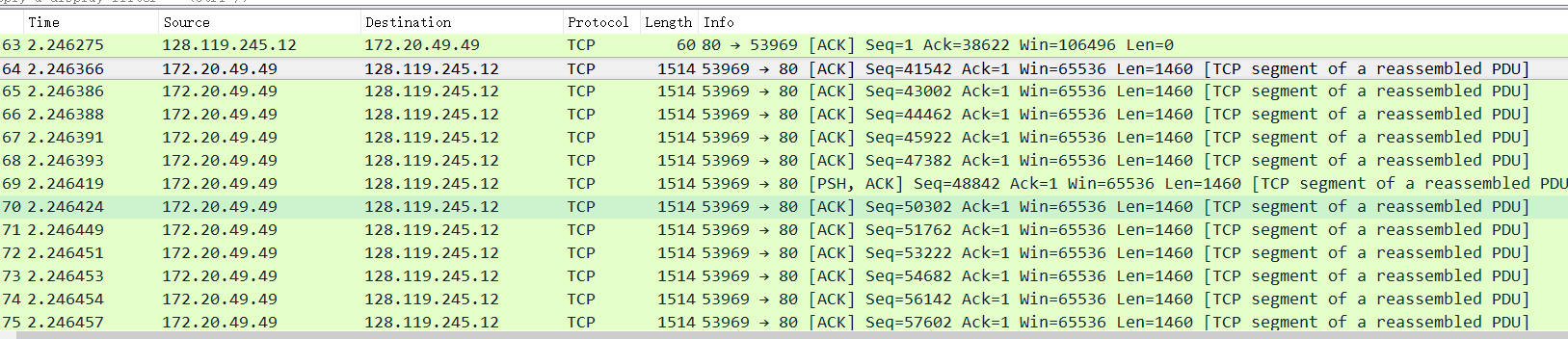


1. 在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？ 限制发送端的传输以后，接收端的缓存是否仍然不够用？



接收端公示的最小的可用缓存空间是65536，该窗口大小一直增加， 没有出现接收端的缓存是否仍然不够用的情况。

1. 在跟踪文件中是否有重传的报文段？进行判断的依据是什么？



没有重传。

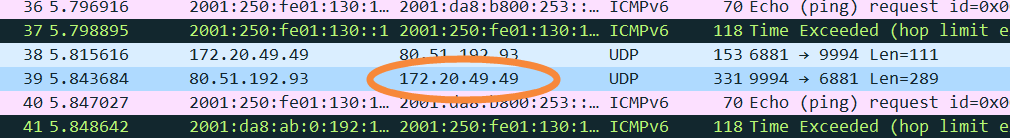
判断依据：客户端发送的报文序列号没有出现重复。

1. TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。

数据总长度：152685+108\*54=164422B 时间间隔：1.74586s

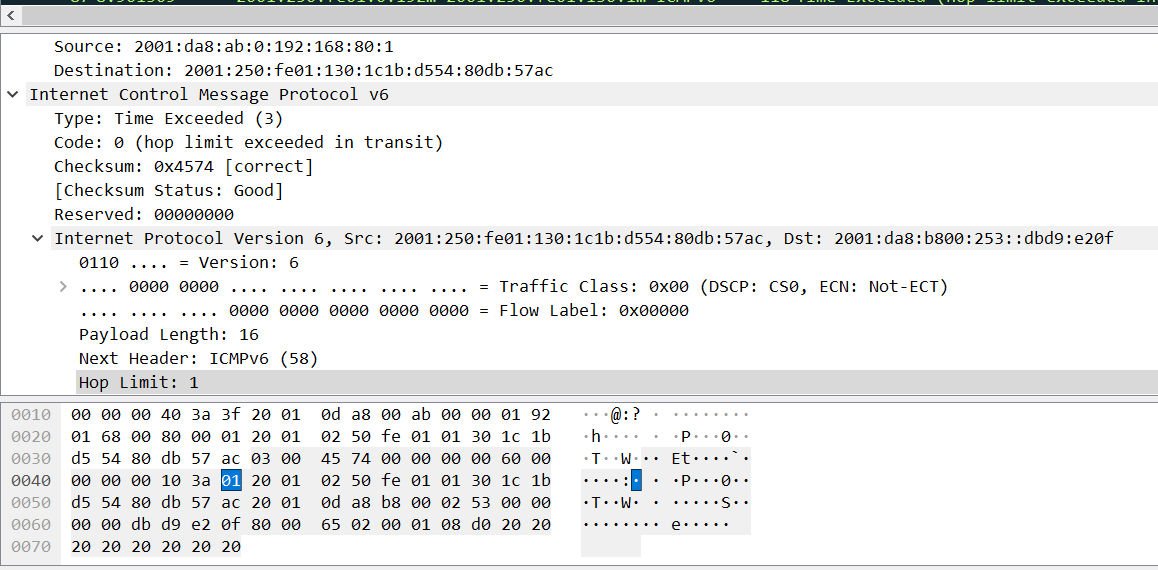
吞吐量：164422/1.74 = 9.6\*105bps

1. IP 分析
2. 你主机的IP地址是什么？

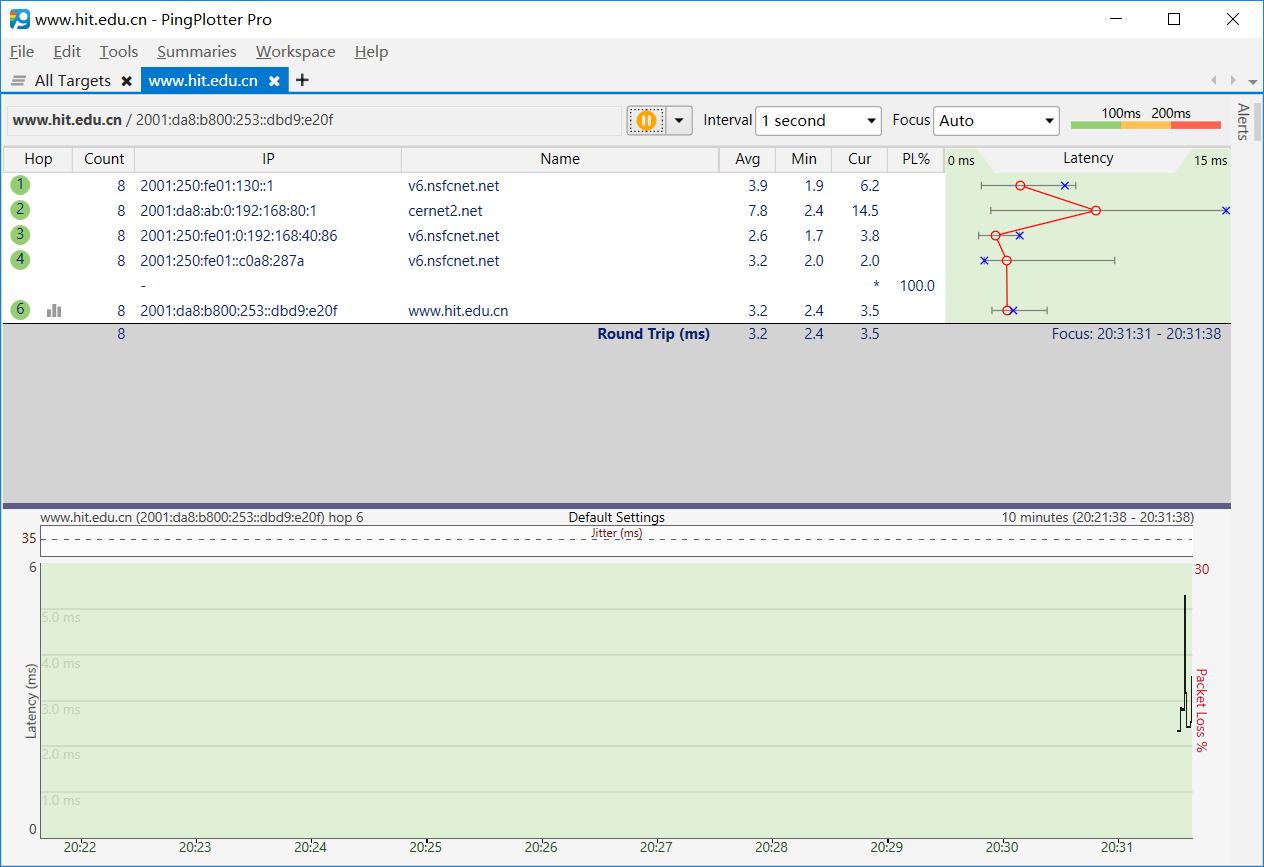


172.20.49.49

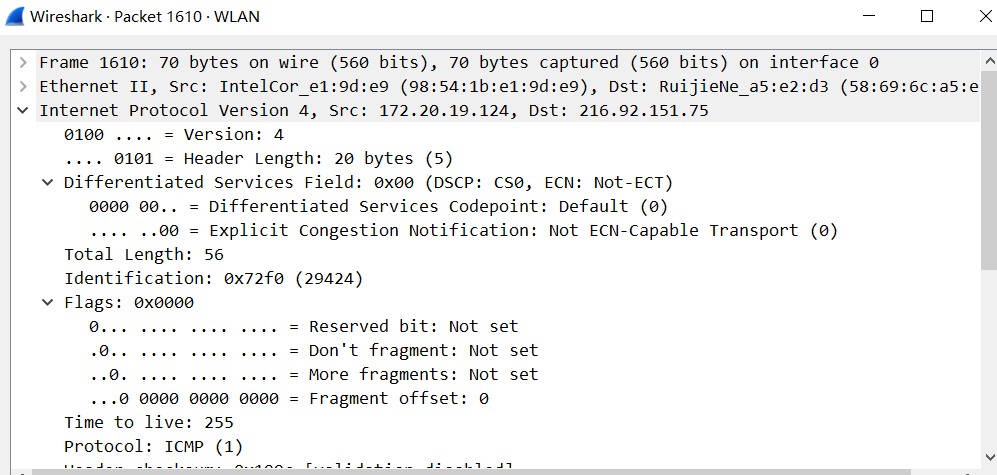
1. 在IP数据包头中，上层协议（upper layer）字段的值是什么？



01



1. IP头有多少字节？该IP数据包的净载为多少字节？并解释你是怎样确定



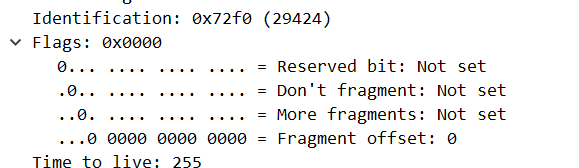
IP 头有 20 字节

IP 包的净载为 Total Length-Header Length=56B-20B=36B

1. 该IP数据包的净载大小的？

36B

1. 该IP数据包分片了吗？解释你是如何确定该P数据包是否进行了分片



没有分片

因为没有分片的偏移量

1. 你主机发出的一系列ICMP消息中IP数据报中哪些字段总是发生改变？

TTL、ID鉴别码、头部校验和

1. 哪些字段必须保持常量？哪些字段必须改变？为什么？

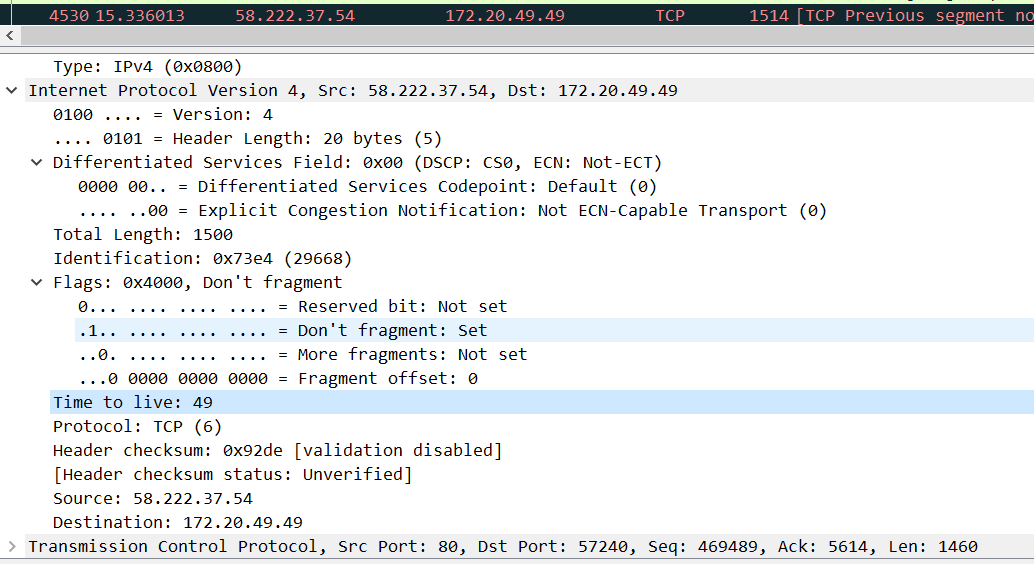
保持常量：IP版本等

必须改变：TTL、ID鉴别码、头部校验和

1. 描述你看到的IP数据包Identification字段值的形式。

加一递增的16位

1. Identification字段和TTL字段的值是什么？



Identification字段：29668

TTL字段的值：49

1. 最近的路由器（第一跳）返回给你主机的ICMP Time-to-live exceeded消息中这些值是否保持不变？为什么？

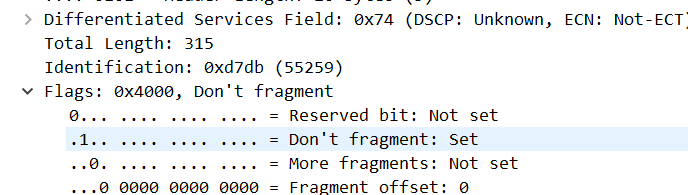
不变，因为是第一跳的路由器返回的Time-to-live exceeded消息。因为是第⼀跳路由器发回的数据报

1. 该消息是否被分解成不止一个IP数据报？



分成了两片

1. 观察第一个IP分片，IP头部的哪些信息表明数据包被进行了分 片？IP头部的哪些信息表明数据包是第一个而不是最后一个分 片？该分片的长度是多少



标识位中，第二个More fragments为1，表示为分片，且不是最后一个分片。

1. 原始数据包被分成了多少片？

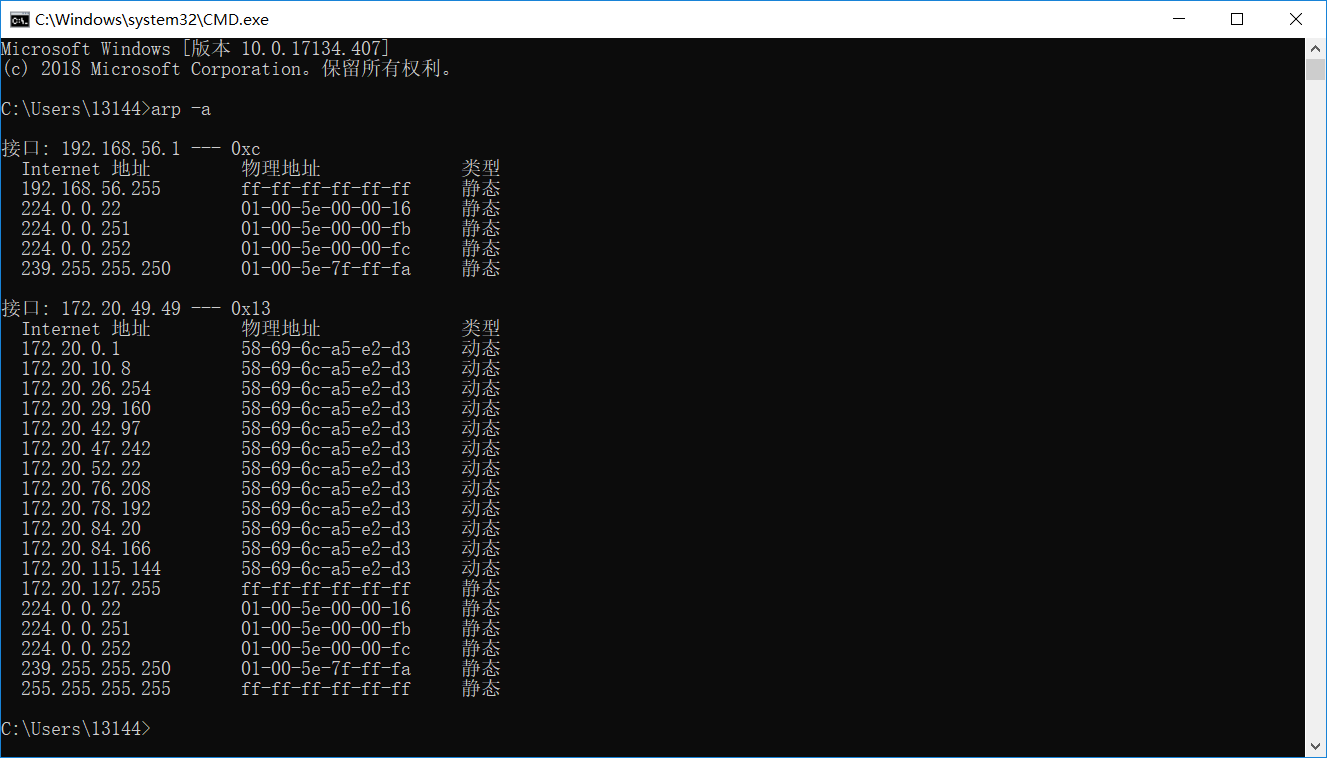


分为3片

1. 这些分片中IP数据报头部哪些字段发生了变化？

前两片More fragments均为1，最后一片为0，且第二片的分片offest为1480，最后一片为2960。

1. 抓取 ARP 数据包
2. 利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机 上 ARP 缓存的内容。说明 ARP 缓存中每一列的含义是什么?



每个IP地址所对应的物理地址及其类型，动态或是静态。

1. ARP数据包的格式是怎样的？由几部分构成，各个部分所占的字节数是多少？

数据报格式：

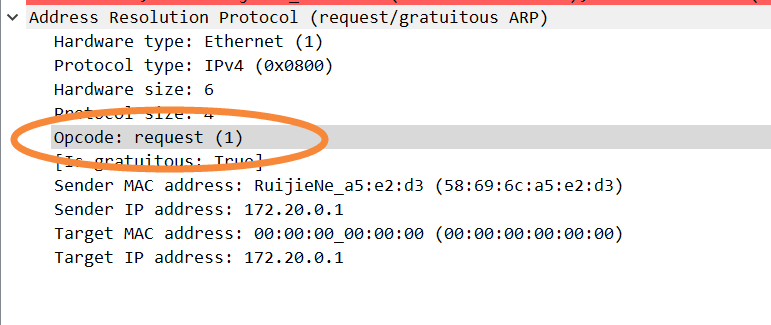


9部分：硬件类型（2 字节），协议类型（2 字节），硬件地址长度（1 字节），协议地址长度（1 字节），OP（2 字节)，发送端 MAC 地址（6 字节），发送端 IP 地址（4 字节），目的 MAC 地址（6 字节），目的 IP 地址（4字节）

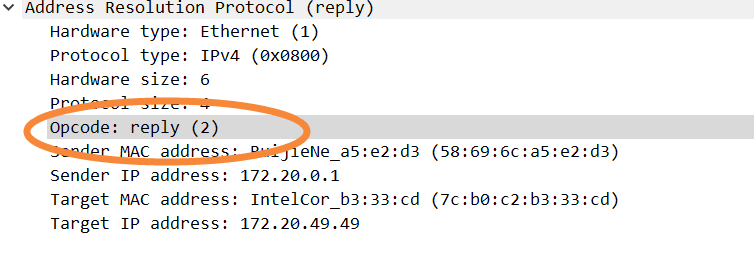
1. 如何判断一个ARP数据是请求包还是应答包？

检测OP字段，当OP为0x0001时为请求包，OP为0x0002时为应答包。

请求包：



应答包：

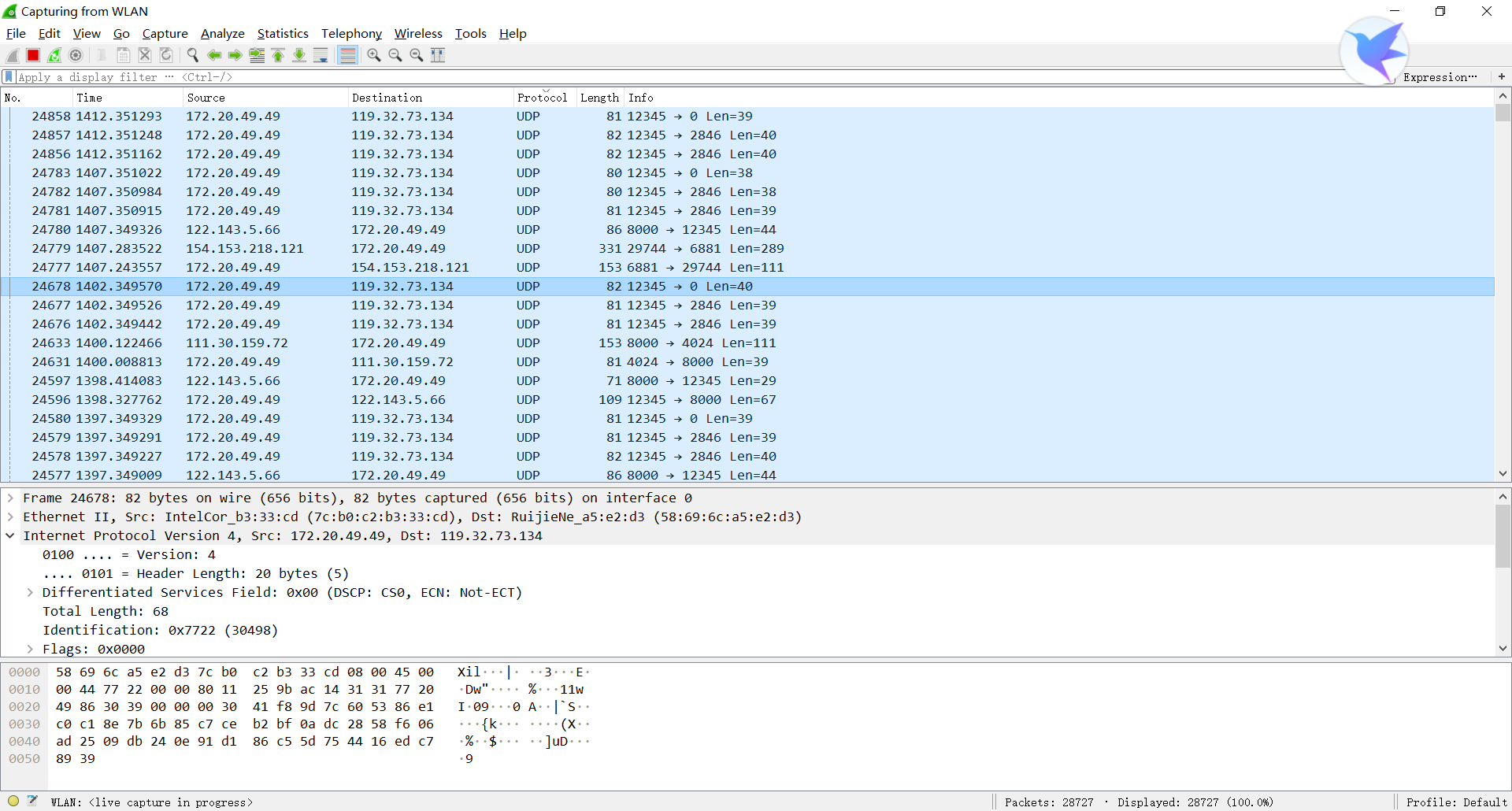


1. 为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明确目的局域网地址的帧中传送？

ARP查询不知道目的IP地址所对应的MAC地址，需要广播。

ARP响应由查询报文知道查询主机的MAC地址，且局域网中的其他主机不需要此次查询的结果。

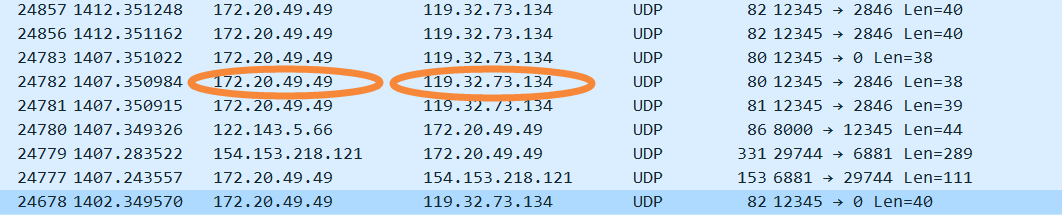
1. 抓取 UDP 数据包



1. 消息是基于UDP的还是TCP的？

UDP

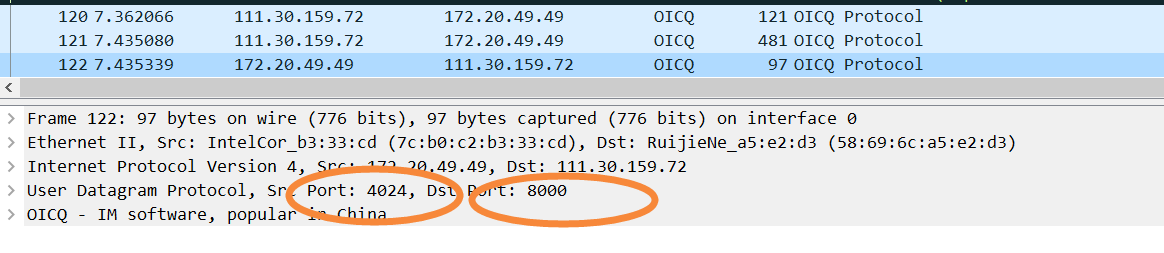
1. 你的主机ip地址是什么？目的主机ip地址是什么？



主机ip地址:172.20.49.49

目的主机ip地址:119.32.73.134

1. 你的主机发送QQ消息的端口号和QQ服务器的端口号分别是多 少？



发送QQ消息的端口号:4024

QQ服务器的端口号:8000

1. 数据报的格式是什么样的？都包含哪些字段，分别占多少字节？

UDP数据报格式包括首部和数据，其中数据存放具体内容。首部有源端口号、目的端口号、数据报长度、校验和。

分别占多少字节:

源端口号占2个字节、目的端口号占2个字节、数据报长度占2个字节、校验和占2个字节。

1. 为什么你发送一个ICQ数据包后，服务器又返回给你的主机一个 ICQ数据包？这UDP的不可靠数据传输有什么联系？对比前面的 TCP协议分析，你能看出UDP是无连接的吗？

服务器需返回接受的结果给客户端。

服务器仅提供一次返回的ACK，不能保证数据没有丢失。

UDP数据报没有序列号，过程中也没有三次握手发送数据，每次只发送一个数据报，然后等待响应。

1. 利用 WireShark 进行 DNS 协议分析

在控制台回车执行完毕后停止抓包.Wireshark 捕获的 DNS 报文 如图所示。

