

**计算机网络**

**课程实验报告**

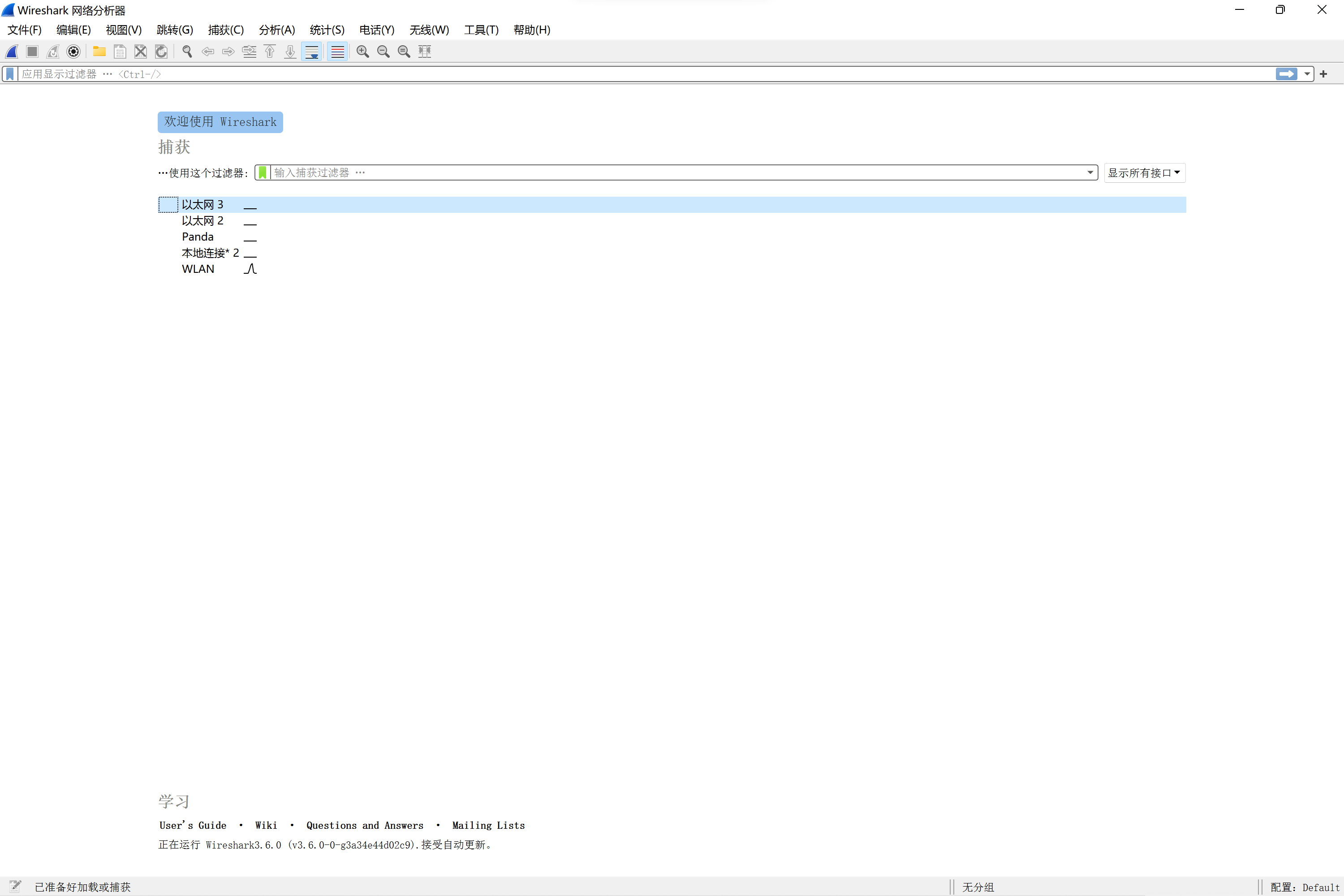
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 实验名称 | 利用Wireshark进行协议分析 | | | | | |
| 姓名 | 陈一帆 | | 院系 | 计算学部/软件工程 | | |
| 班级 | 1937102 | | 学号 | 1191000606 | | |
| 任课教师 | 李全龙 | | 指导教师 | 李全龙 | | |
| 实验地点 | 正心207 | | 实验时间 | 2021.11.20 | | |
| 实验课表现 | 出勤、表现得分(10) |  | 实验报告  得分(40) |  | 实验总分 |  |
| 操作结果得分(50) |  |
| 教师评语 | | | | | | |
|  | | | | | | |

****

|  |
| --- |
| 实验目的： |
| 熟悉并掌握Wireshark的基本操作，了解网络安全协议实体空间进行交互以及报文交换情况。 |
| 实验内容： |
| 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 6. 利用 Wireshark 分析 DNS 协议 7. 利用 Wireshark 分析 UDP 协议 8. 利用 Wireshark 分析 ARP 协议 |
| 实验过程： |
| 见下方。 |
| 实验结果： |
| 见下方。 |
| 问题讨论： |
| 见下方。 |
| 心得体会： |
| 本次实验让我充分了解了网络中各种协议及其格式，对计算机网络有了更深的理解。 |

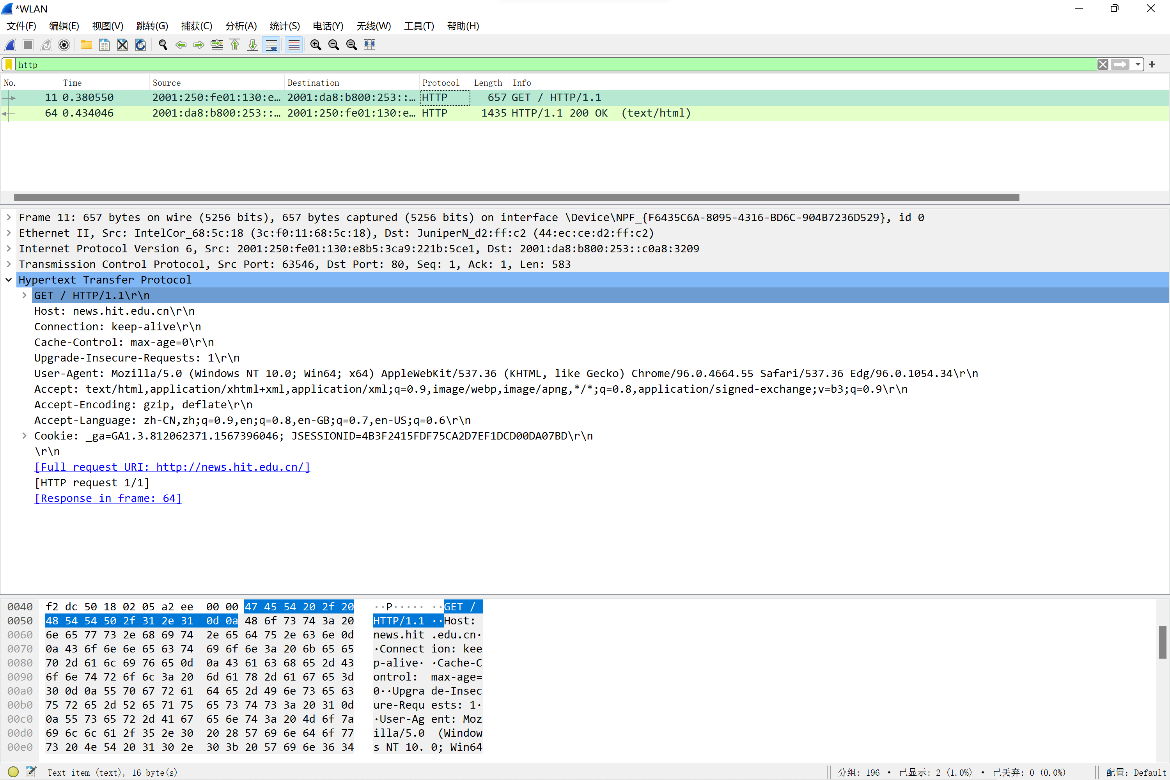
1. Wireshark的使用

打开Wireshark，观察网络情况，此时使用的时WLAN无线网络连接，选择WLAN接口。



1. HTTP分析
   1. HTTP GET/response交互

首先在Wireshark加入筛选条件http，然后在浏览器地址栏中输入<http://news.hit.edu.cn>，捕获两个包，如下：



Q：你的浏览器运行的是 HTTP1.0，还是 HTTP1.1？你所访问的服务器所运行 HTTP 协议的版本号是多少？

A：HTTP1.1；HTTP1.1。

Q：你的浏览器向服务器指出它能接收何种语言版本的对象？

A：zh-CN，简体中文

Q：你的计算机的IP地址多少？服务器的IP地址多少？

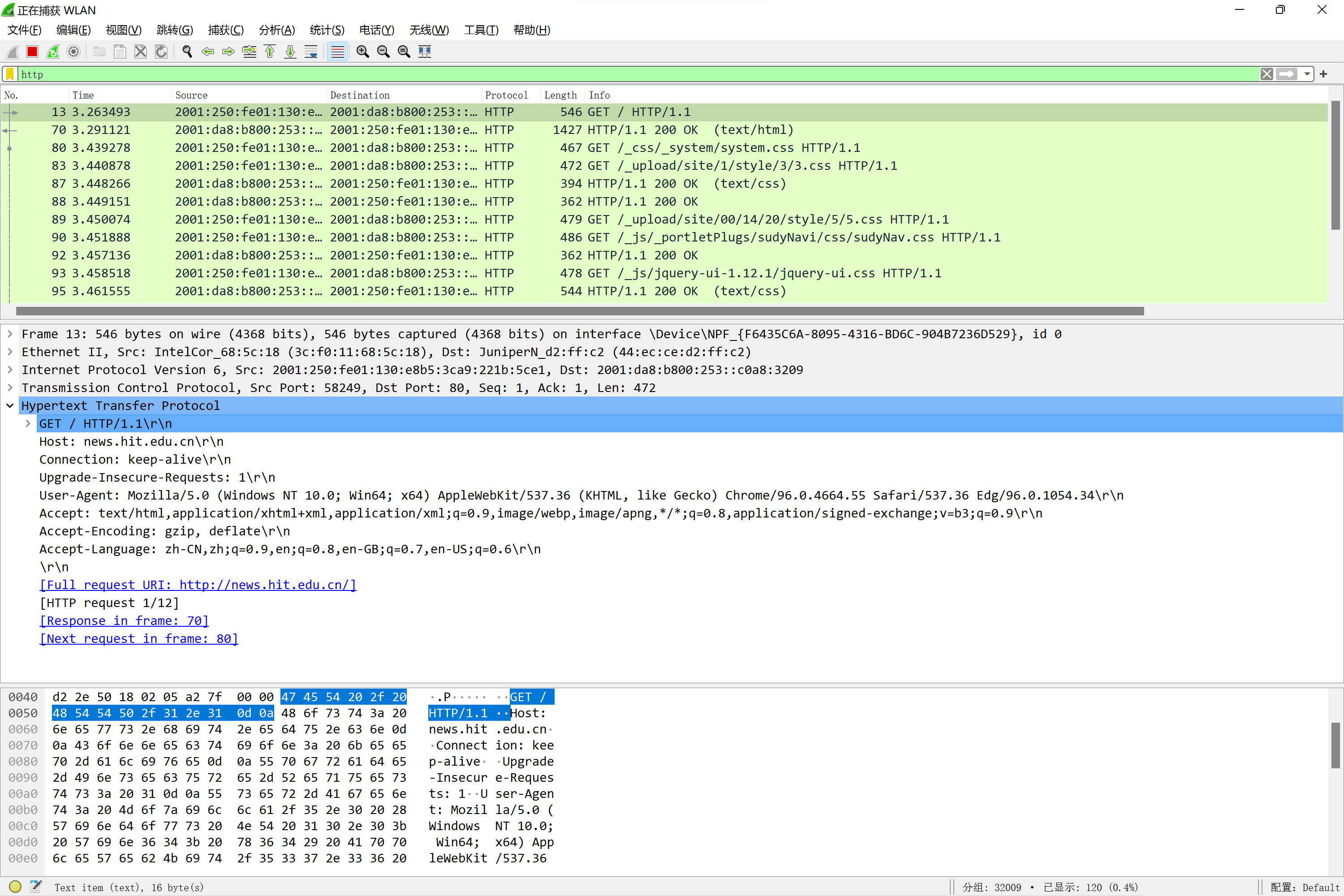
A：2001:250:fe01:130:e8b5:3ca9:221b:5ce1；2001:da8:b800:253::c0a8:3209。

Q：从服务器向你的浏览器返回的状态代码是多少？

A：200。

* 1. HTTP条件/response交互

在Edge浏览器设置中清楚掉所有的缓存后，重新输入<http://new.hit.edu.cn>，此时捕获情况如下图所示。



Q：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？

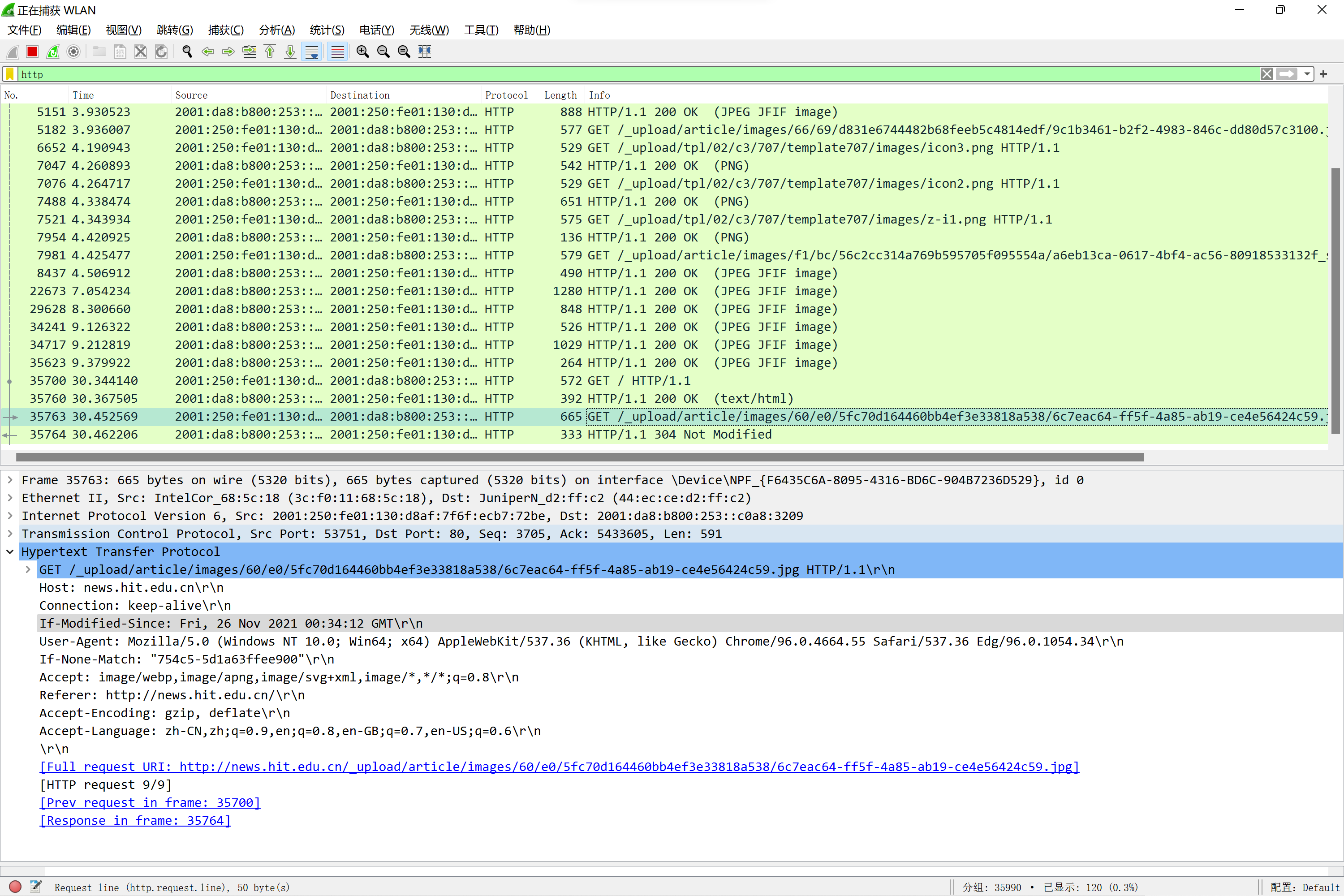
A：没有。

Q：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？

A：服务器明确的返回了文件的内容，因为返回的状态码是200，代表明确的返回了文件。

Q：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？

A：第一次访问网页发送的所以请求中均没有IF-MODIFIED-SINCE行，在浏览器中点击刷新之后，Wireshark捕获的GET请求中含有IF-MODIFIED-SINCE行，后面跟着的信息是If-Modified-Since: Fri, 26 Nov 2021 00:34:12 GMT，表示浏览器缓存的文件最后更新的时间。观察刷新前的响应报文，有些报文中注明了最后响应时间。

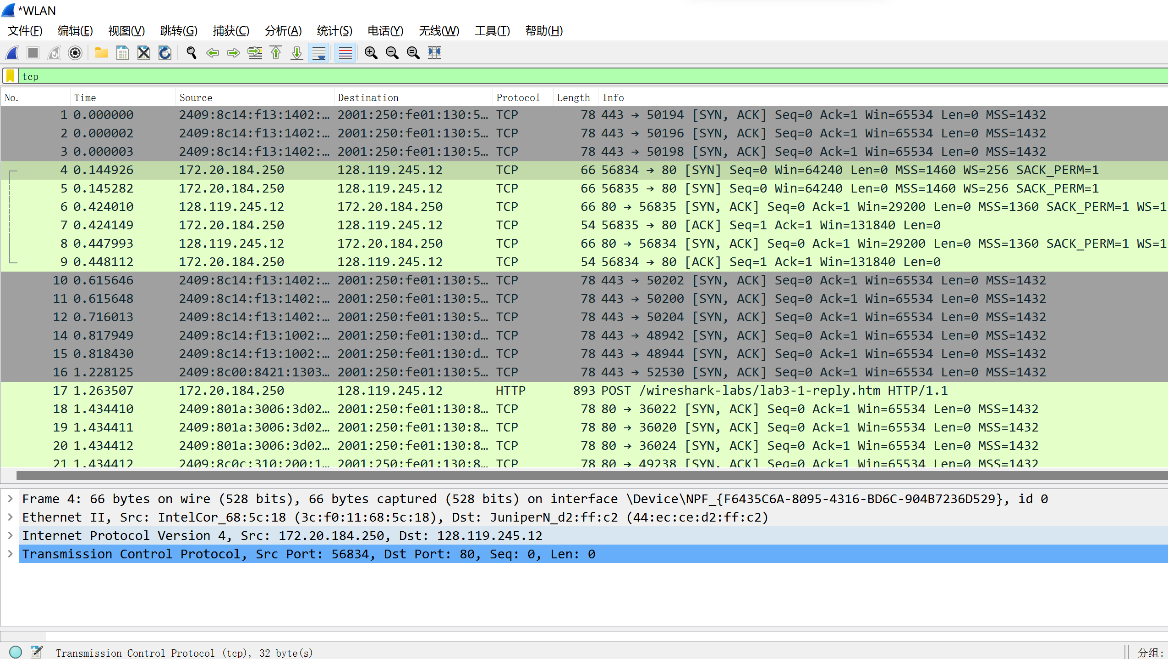


Q：服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是多少？服务器是否明确返回了文件的内容？请解释。

A：响应代码为304，服务器没有明确返回文件内容，因为服务器通过对IF-MODIFIED-SINCE行的分析结果是Not Modified，浏览器可以使用其保存的缓存，只要发送304告知其缓存是最新的即可。

1. TCP分析
   1. 俘获大量的由本地主机到远程服务器的 TCP 分组

按实验指导书操作后，得到以下报文。



* 1. 浏览追踪信息

Q：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？  
A：客户端主机IP：172.20.184.250，TCP端口号为56834。

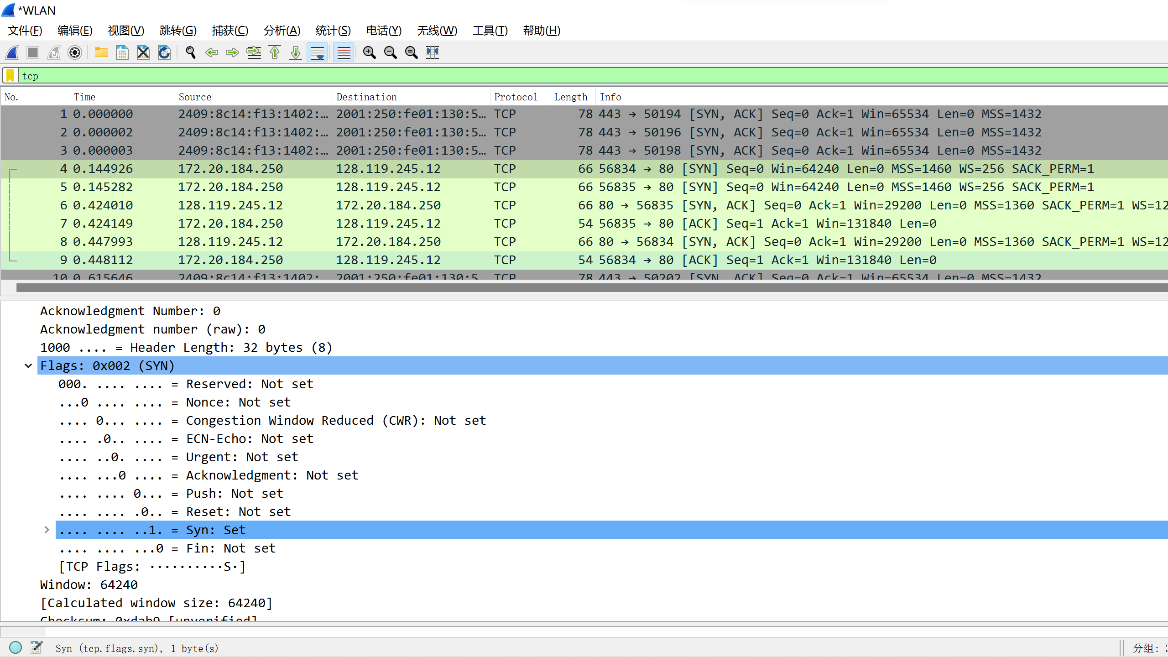
Q：Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来发送和接收 TCP 报文的端口号是多少？

A：服务器IP：128.119.245.12，TCP端口号为80。

* 1. TCP基础

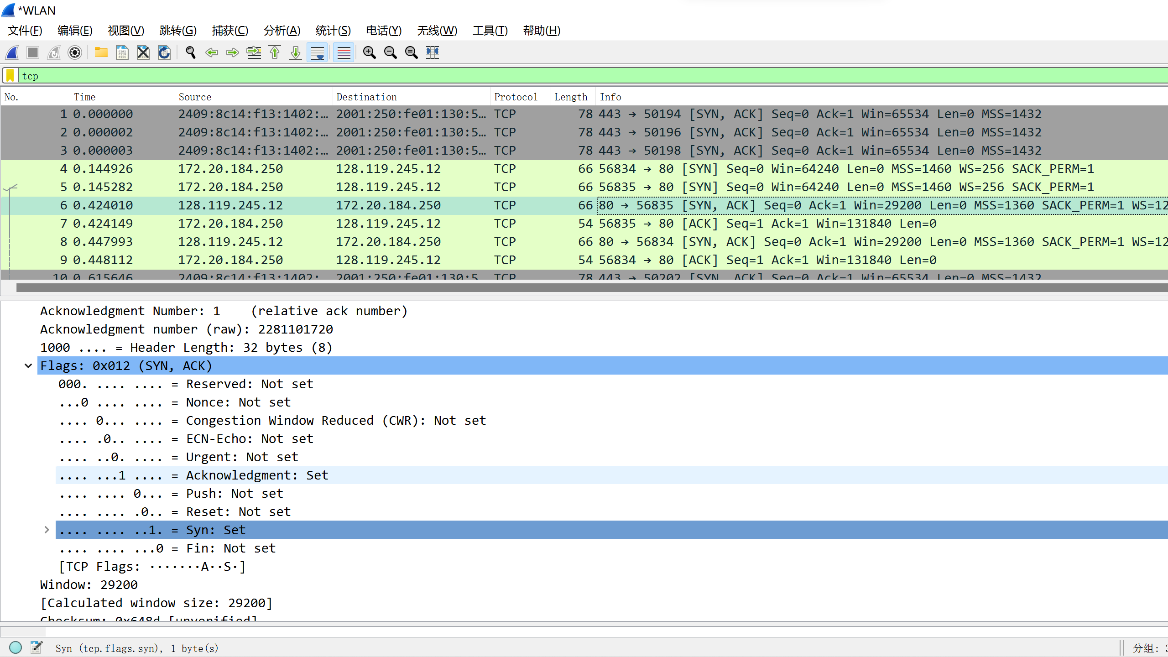
Q：客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号 （sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？

A：序号是0，通过价格SYN标志位设置为1来标记为SYN报文段。



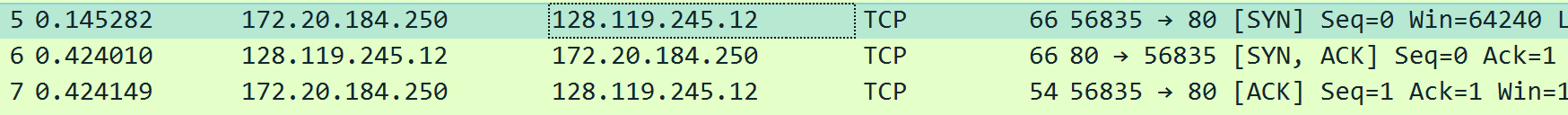
Q：服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段中，Acknowledgement 字段的值是多少？Gaia.cs.umass.edu 服务器 是如何决定此值的？在该报文段中，是用什么来标示该报文段是 SYNACK 报文段的？

A：序号是0，Acknowledgement字段的值为1。服务器是通过将客户端发送的序号加一来确定此值的，在此报文段中同样是根据标志位来确定该报文段是SYNACK报文段的。



Q：你能从捕获的数据包中分析出TCP三次握手过程吗？

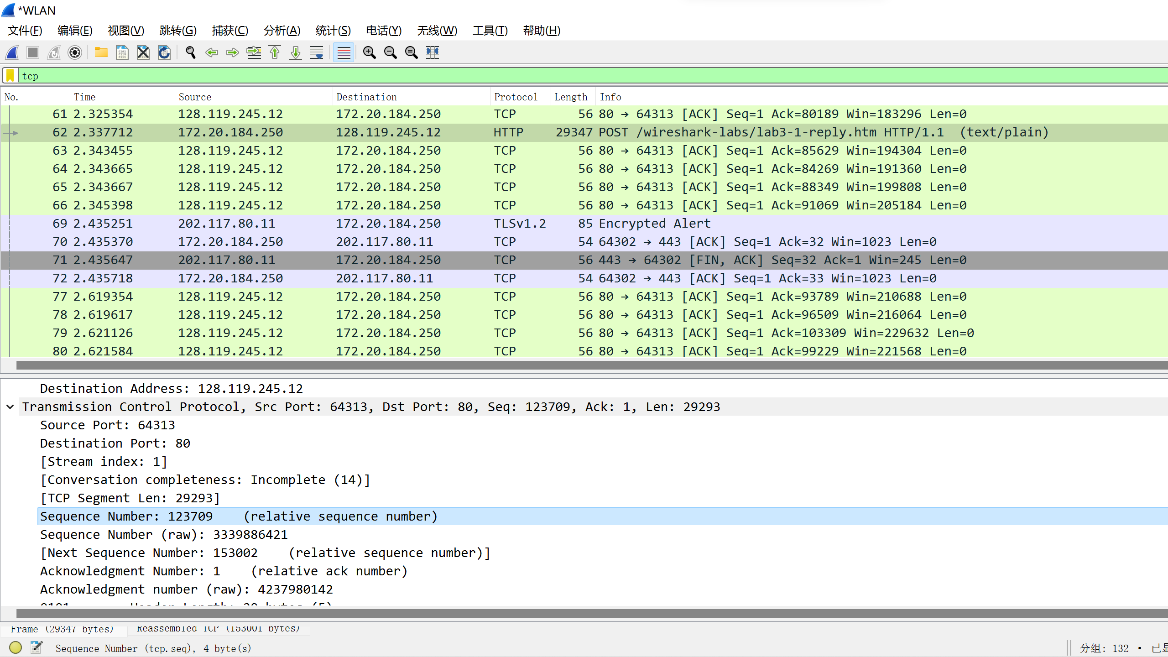
A：如下图：



客户端首先发送SYN报文段，且Wireshark为了报文段方便读取初始化Seq=0。然后服务器同样返回SYN报文段，Ack取值为客户端发送的Seq值加一，Seq取值为0。最后客户端返回Seq为1，是在第一次握手所取Seq的基础上加一，Ack为1，来自于第二次握手服务器所发Seq值加一。

Q：包含 HTTP POST 命令的 TCP 报文段的序号是多少？

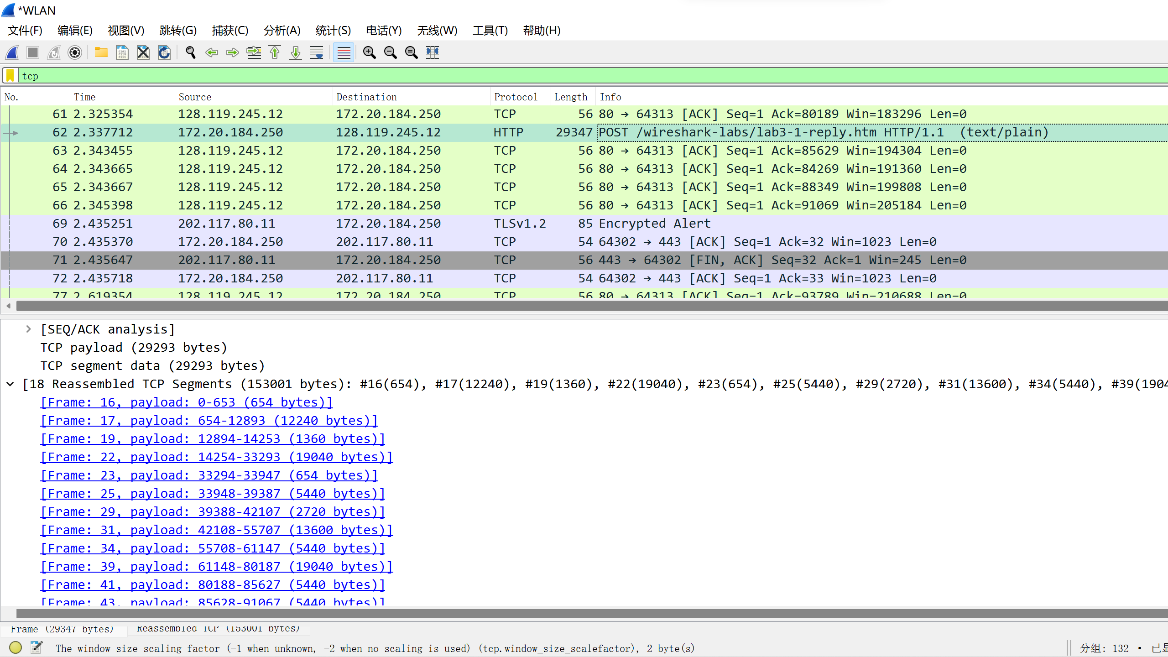
A：如下图所示



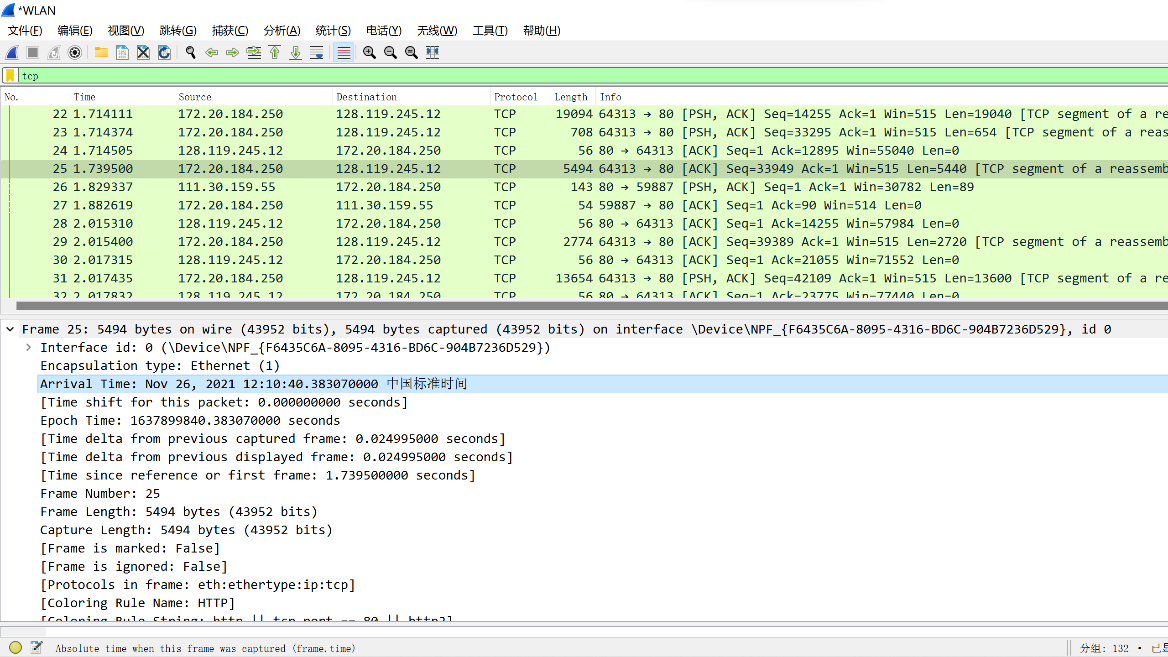
序号为123709。这是经过Wireshark初始化过的，而没有初始化过的则是3339886421。

Q：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？

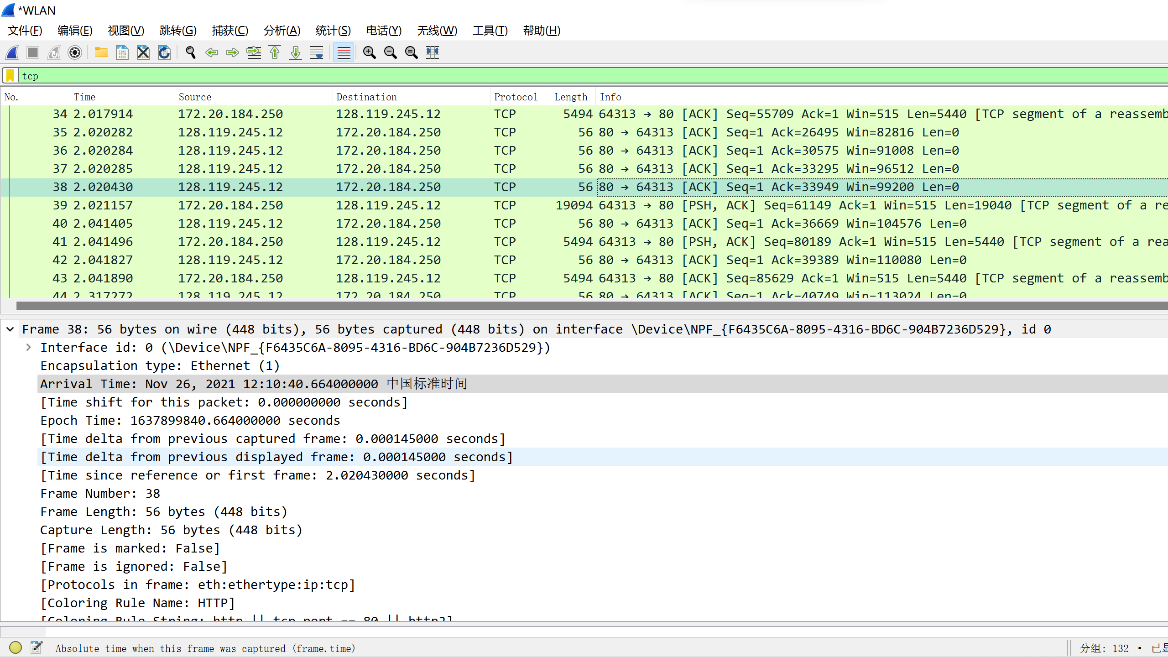
A：第6个报文段的序号为33949。



是在2021/11/26 12:10:40.38307抵达的。其相对时间是在TCP连接建立之后，POST请求发送之前。

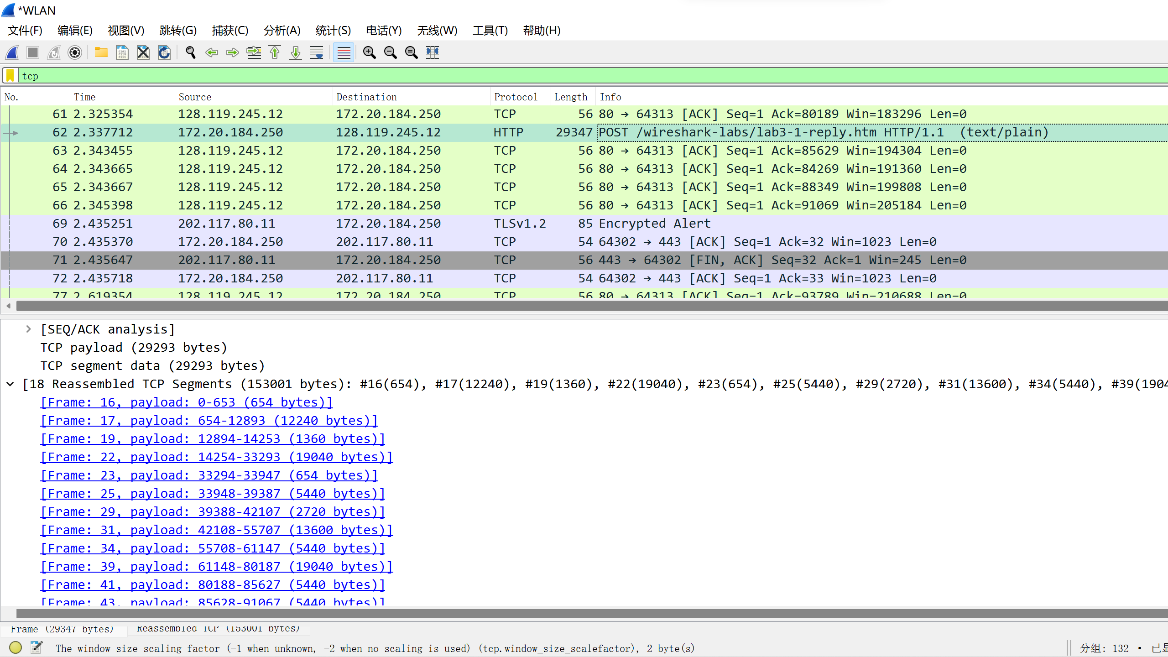


该报文对应的ACK被接收时间为2021/11/26 12:10:40.664。



Q：前六个 TCP 报文段的长度各是多少？

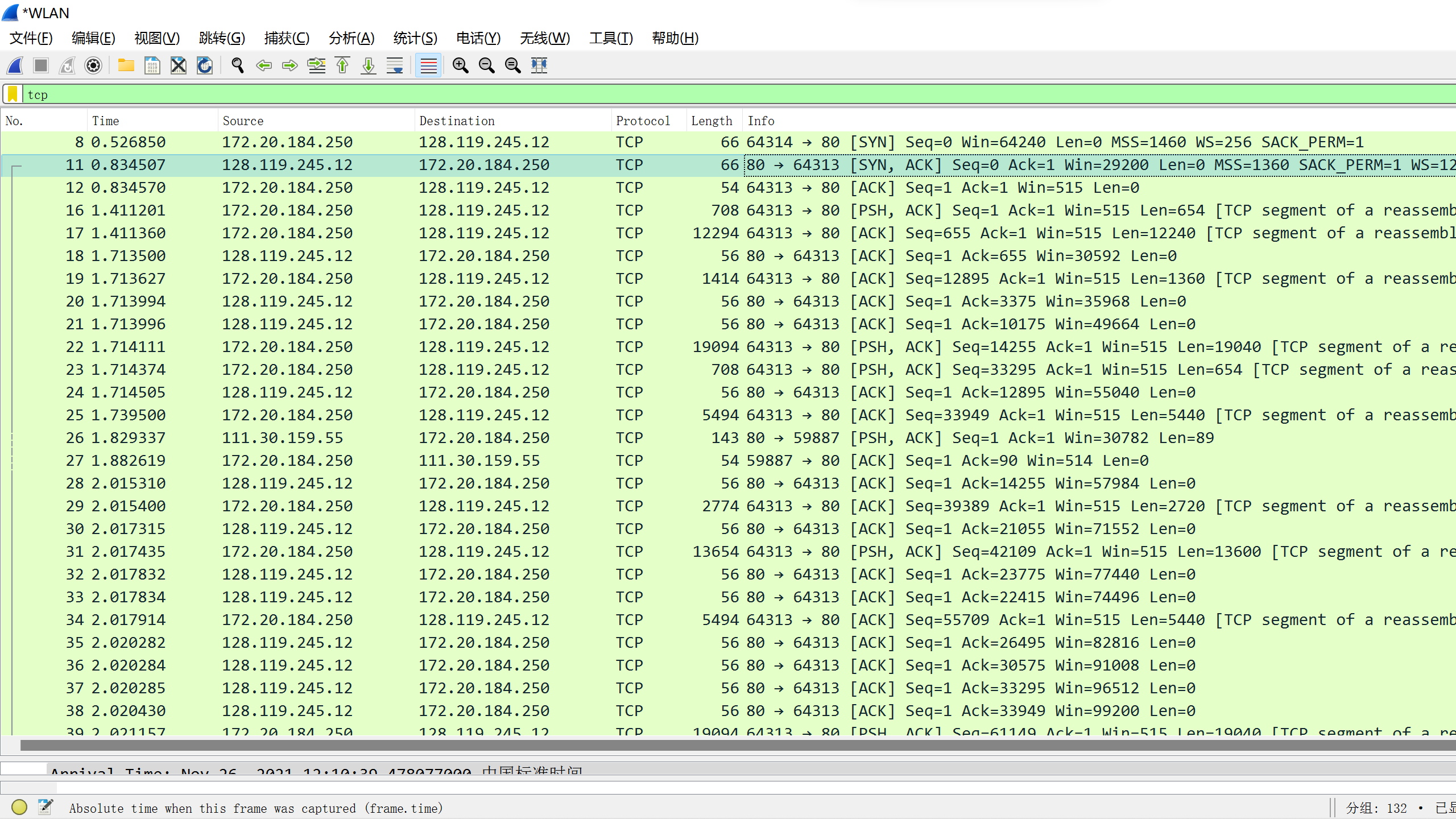
A：如图所示



长度分别为654B、12240B、1360B、19040B、654B、5440B。

Q：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？

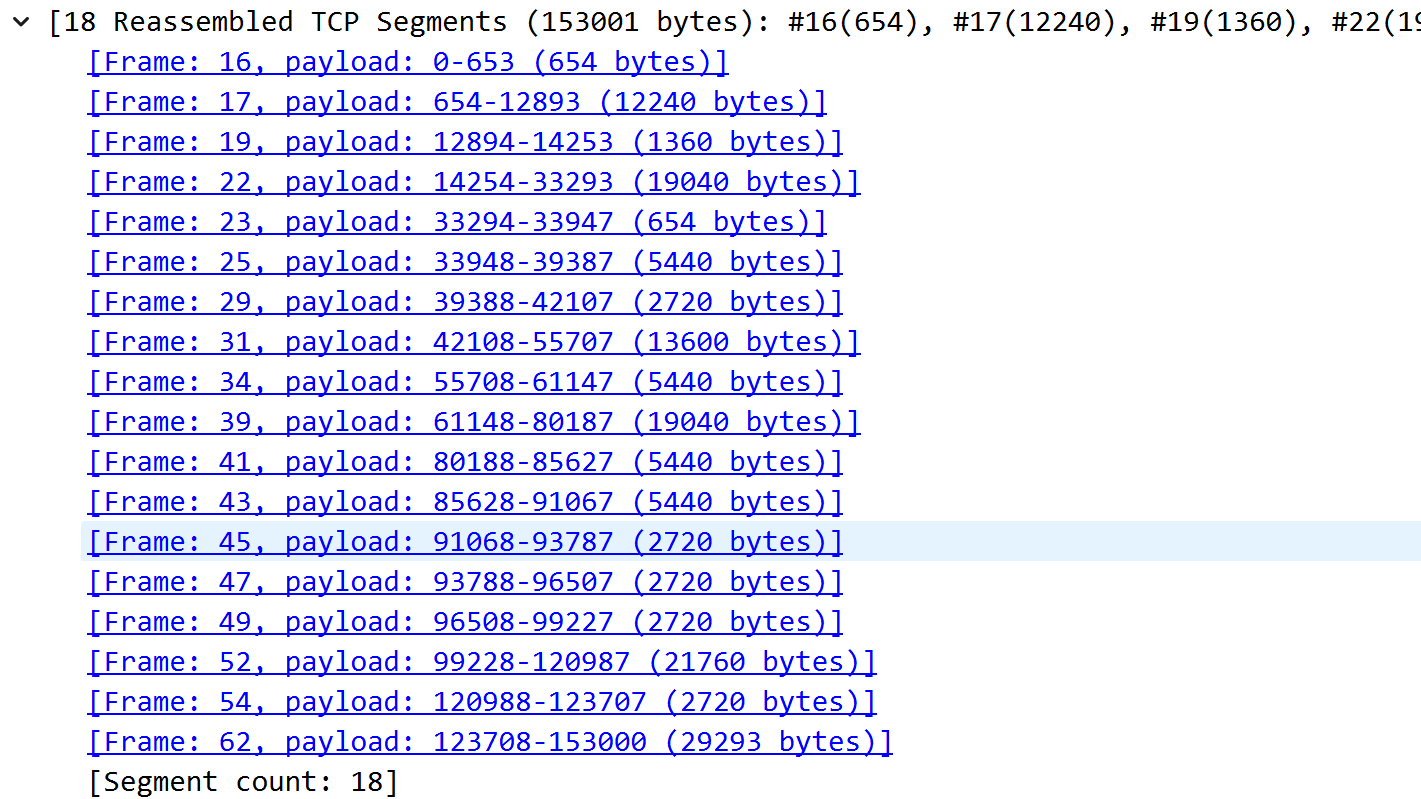
A：在此处接收端应该是指服务器。服务器会在发给客户端的报文中注明接收端可用缓存空间的大小。如下图所示，可用缓存空间最小为29200。



不会，接收端窗口大小会不断增加，不会不够用。

Q：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？

A：此时未在其中发现重传的报文段。



因为报文中序号无重复。

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

A：TCP连接传输的数据大小、以及所用时间如图所示。



此时传输的数据为153001B，用时一共为1.817095s，传输速率为153001\*8/1.817095= 673607bps≈0.67Mbps

1. IP分析
   1. 通过执行traceroute捕获数据包

第一个ICMP Echo Request消息，Packet Details部分如下图所示。



Q：你主机的IP地址是什么？

A：172.20.184.250.

Q：在IP数据包头中，上层协议（upper layer）字段的值是什么？

A：值为1，表示ICMP

Q：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

A：20字节，静载为36B，因为pingplotter默认发的IP包大小为56B，56-20=36B。

Q：该IP数据包的净载大小的？

A：36B。

Q：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

A：未分片。可以通过IP数据包首部的标志位来看，分别表示：保留位、DF(Don’t Fragment)、MF(More Fragment)。由于该数据包DF=0，表示允许分片，但是MF=0，表示其后续没有其他片段，并且标志位后为偏移位，由于偏移位为0，可以确认该数据包前没有其他分片，因此可以确定该数据包没有分片。

* 1. 对捕获的数据包进行分析

Q：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？

A：TTL、ID、Header Checksum

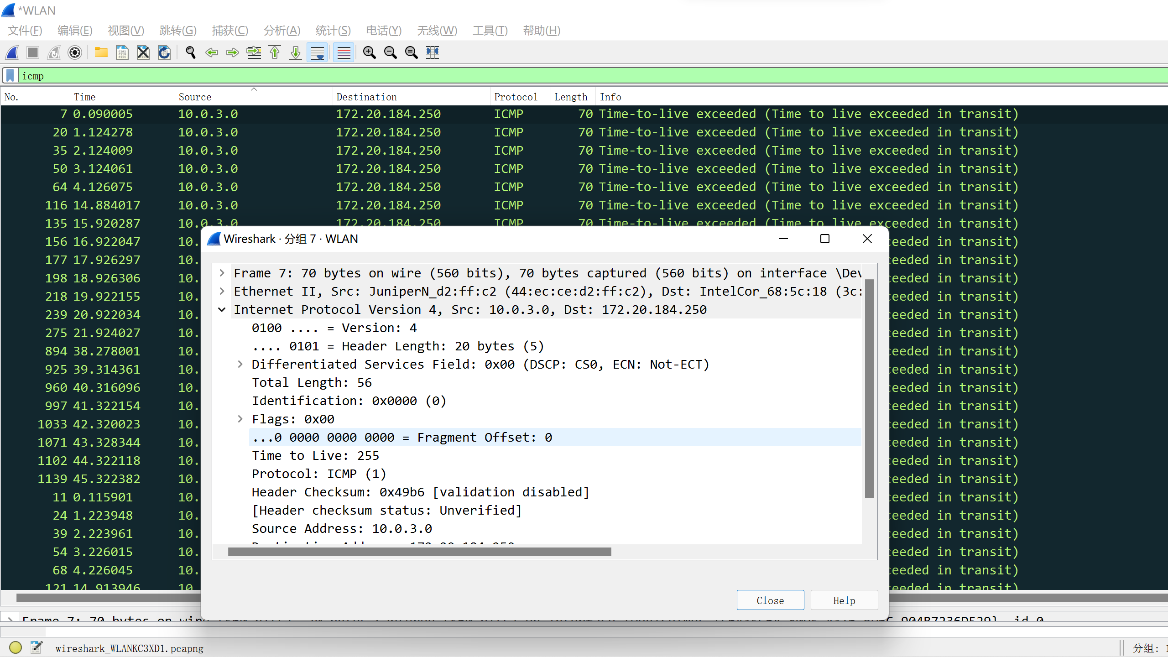
Q：哪些字段必须保持常量？哪些字段必须改变？为什么？

A：ID必须改变，因为主机每发一个IP分组，ID都要加一。TTL必须改变，因为每转发一次，TTL便减一。Checksum必须改变，因为IP分组头部其他字段改变了，而每次跳转Checksum都需要重新计算。除此之外，其他字段均保持不变。

Q：描述你看到的IP数据包Identification字段值的形式。

A：例如：0x66ca。Identification总长度为16位，一共为4个16进制数。

找到最近的路由器（第一跳）返回给你主机的ICMP TTL exceeded消息。如下图所示。



Q：Identification字段和TTL字段的值是什么？

A：Identification：0，TTL：255。

Q：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？

A：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。

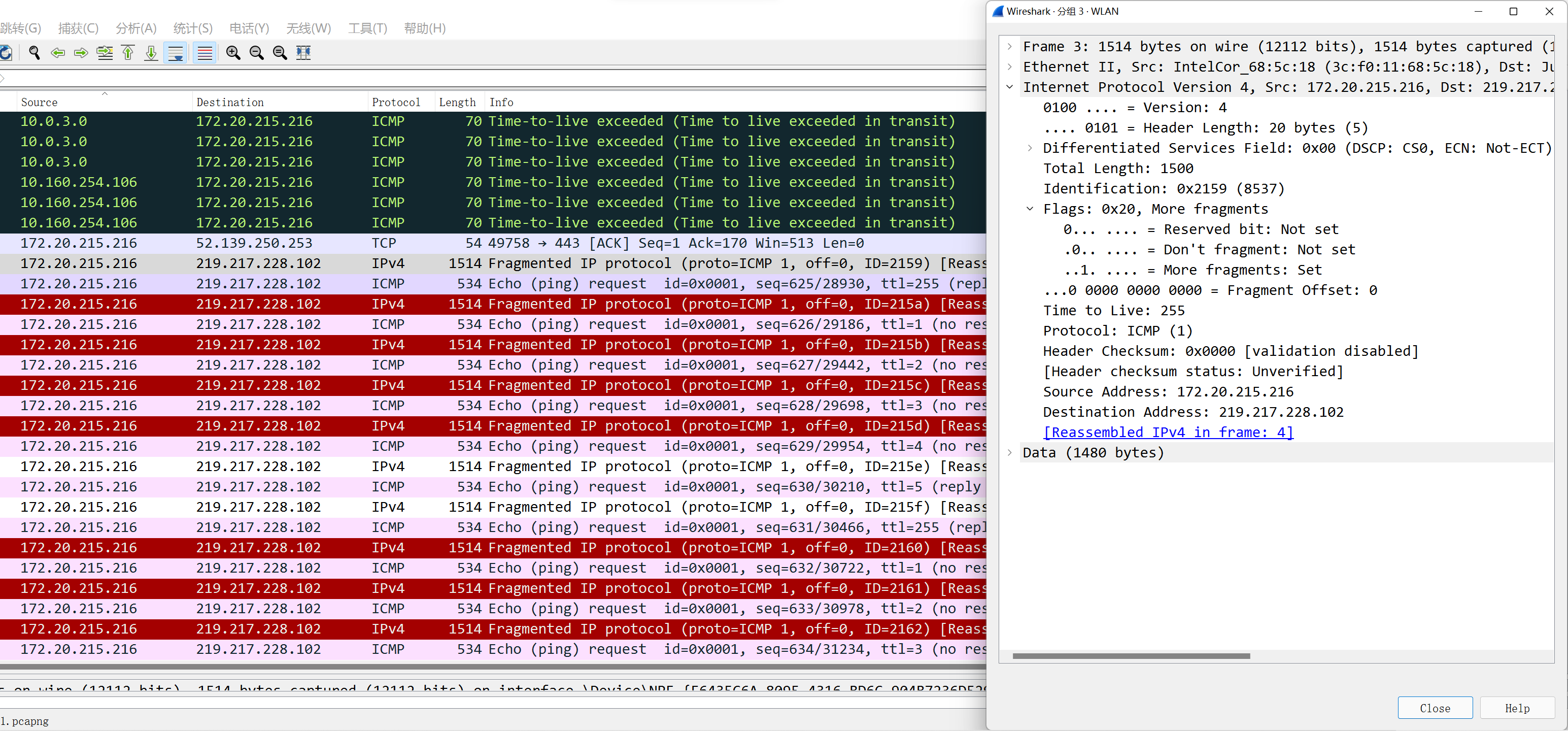
将包大小改为2000字节后选取你的主机发送的第一个ICMP Echo Request消息。

Q：该消息是否被分解成不止一个IP数据报？

A：是

Q：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？

A：该IP分片情况如下。



可以看到标志位中More Fragment为1，表示其后还有分组，并且该分组长度只有1500字节，因此可以判断出有分片，并且该分片的偏移量为0，说明它是第一个分片，长度为1500字节，观察其后一个IP分片，发现其ID与第一个分片的ID相同，符合我们的验证。

将包大小改为2000字节后选取你的主机发送的第一个ICMP Echo Request消息。

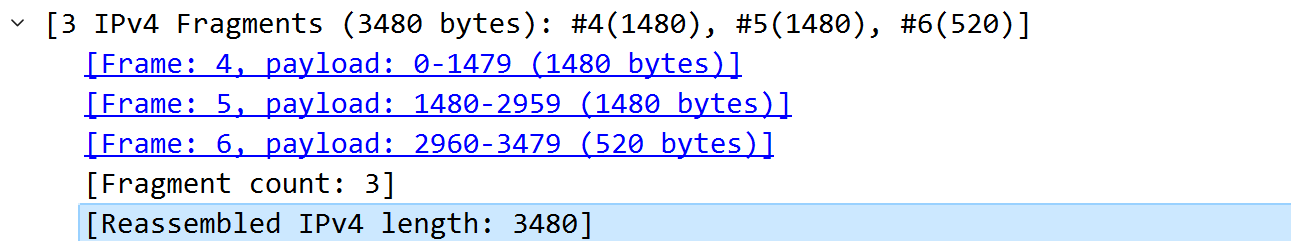
Q：原始数据包被分成了多少片？

A：2片。

* 1. 找到在将包大小改为3500字节后你的主机发送的第一个ICMP Echo Request消息

Q：原始数据包被分为了多少片

A：如下图所示，除去数据头一共3480B。



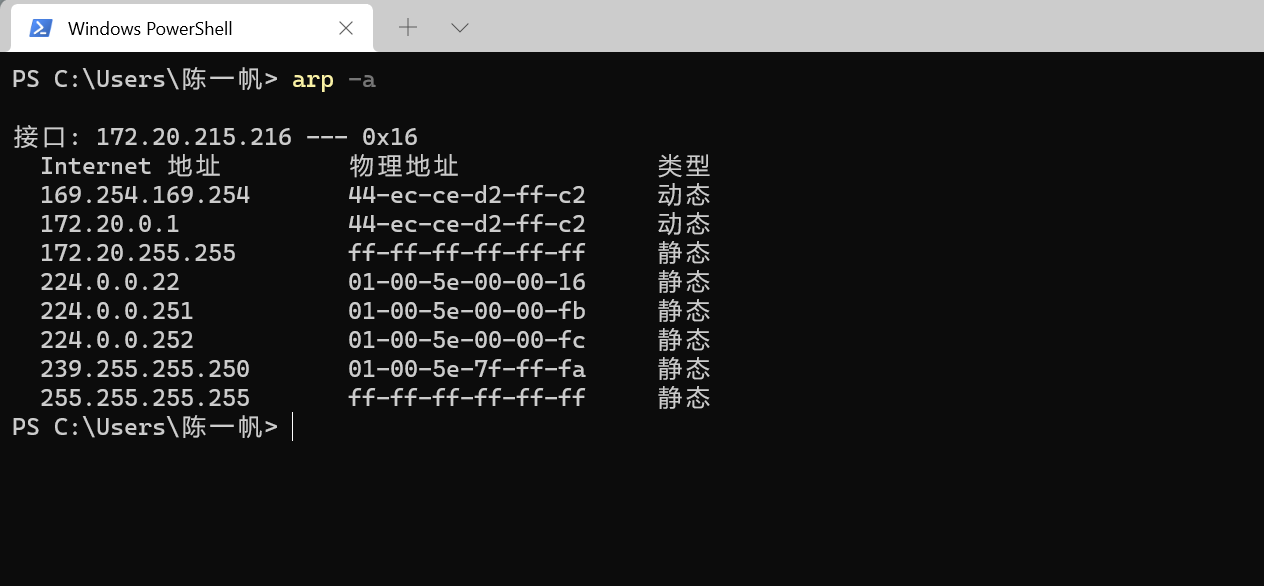
一共被分为3个字节。

Q：这些分片中IP数据报头部哪些字段发生了变化

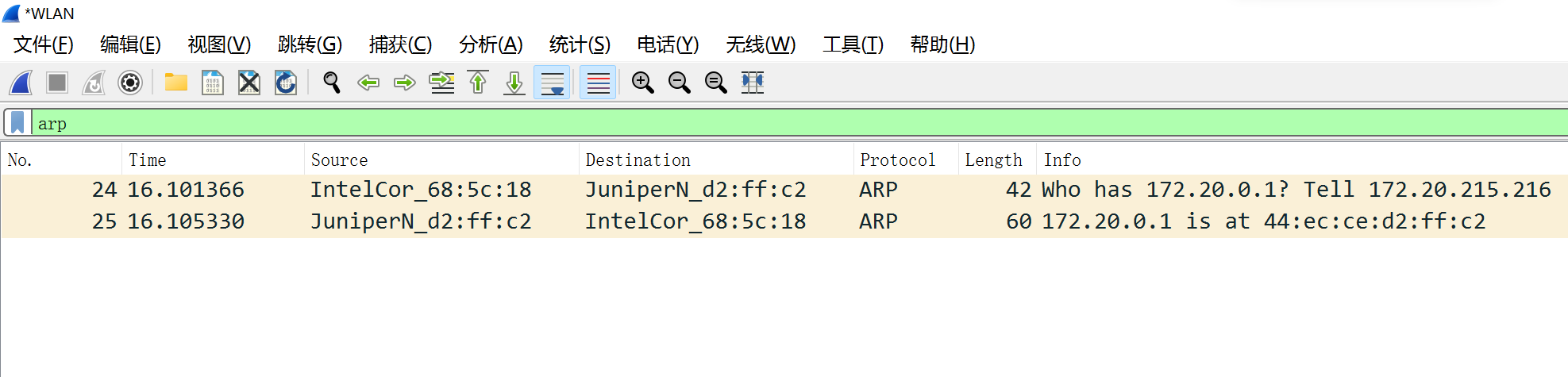
A：片偏移，标志位（MF），Header Checksum

1. 抓取ARP数据包

在命令行中输入arp -a查看主机上arp缓存的情况。



Ping某个IP地址有



Q：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?

A：ARP命令如上图所示，接口表示本机IP地址。每一行表示IP对应的MAC地址。

Q：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？、

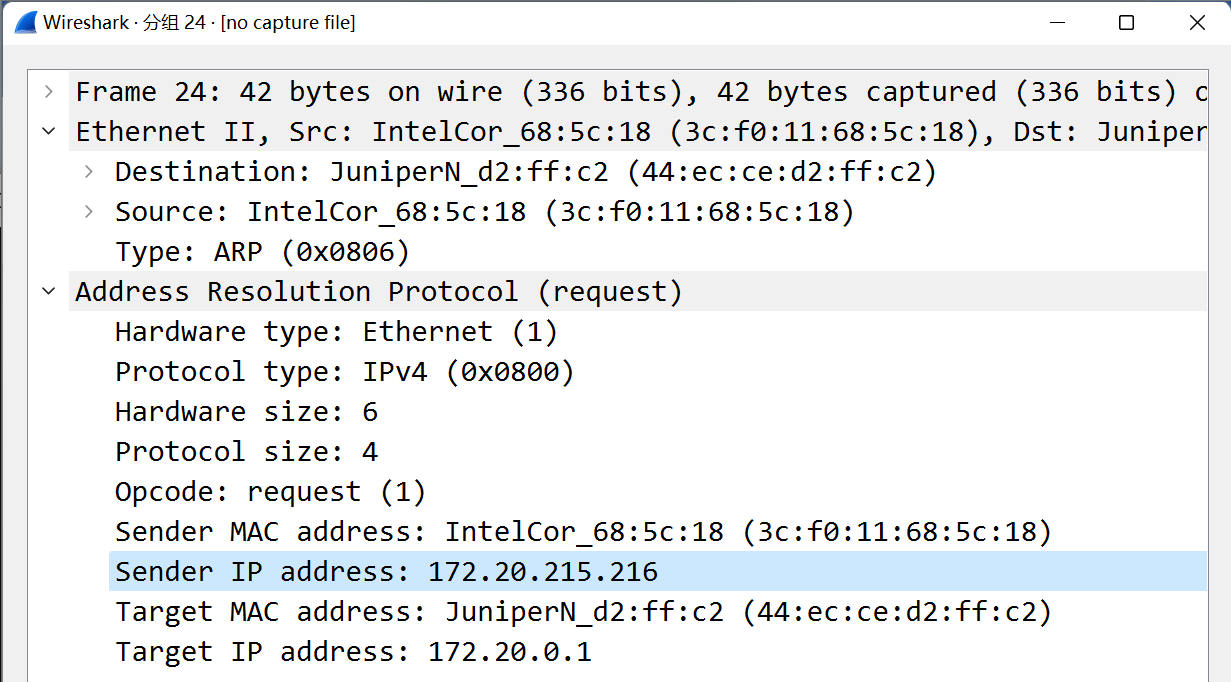
A：格式如下：

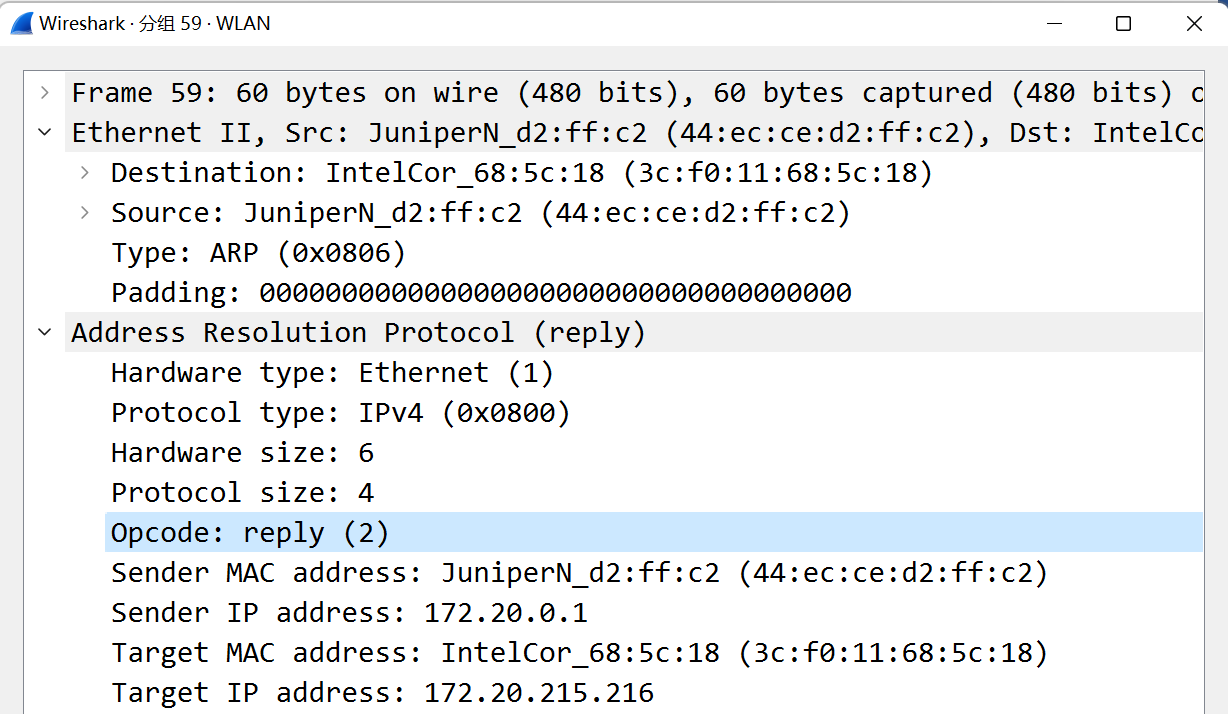


9部分：硬件类型（2 字节），协议类型（2 字节），硬件地址长度（1 字节），协议地址长度（1 字节），OP（2 字节)，发送端 MAC 地址（6 字节），发送端 IP 地址（4 字节），目的 MAC 地址（6 字节），目的 IP 地址（4字节）

Q：如何判断一个ARP数据是请求包还是应答包？

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



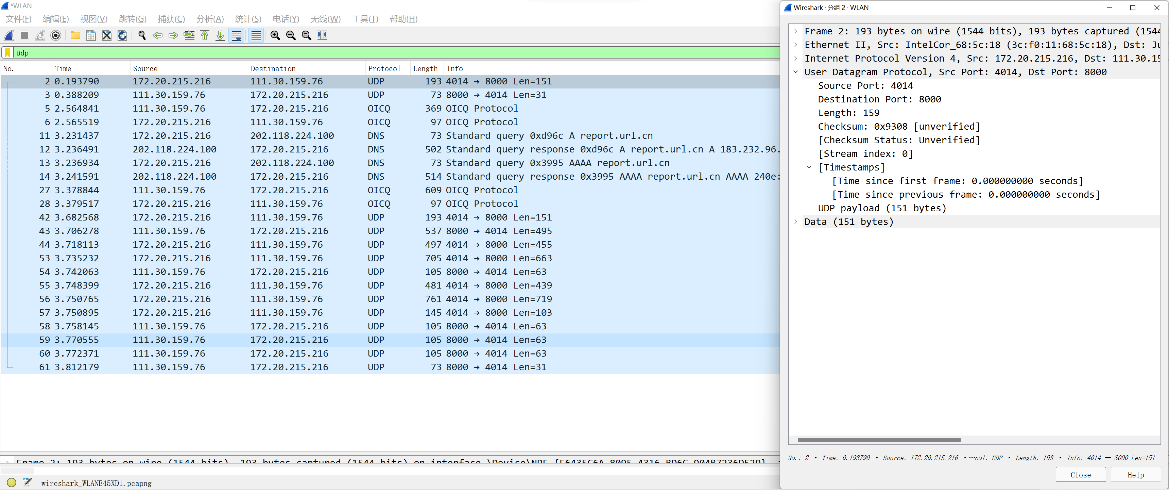


Q：为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明确目的局域网地址的帧中传送？

A：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

如下图所示。



Q：消息是基于UDP的还是TCP的？

A：UDP

Q：你的主机IP地址是什么？目的主机IP地址是什么？

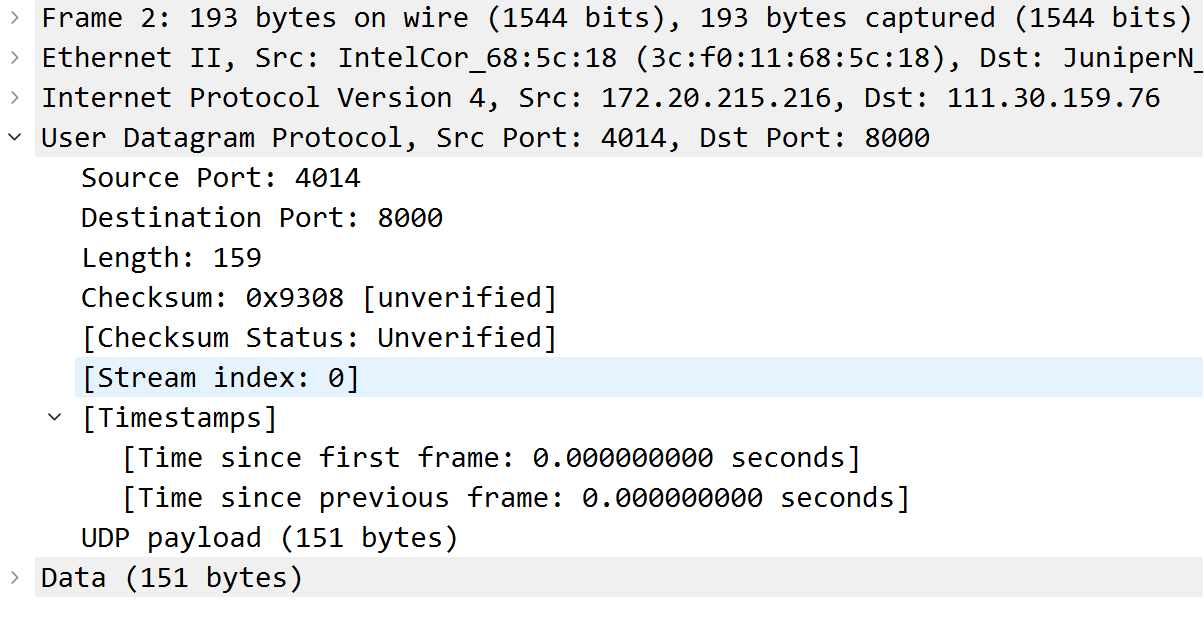
A：本机IP：172.20.215.216。目的主机IP：111.30.159.76

Q：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

A：本机端口：4014。目的主机端口：8000。

Q：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？

A：UDP数据包的格式如下图所示。



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（2个字节）、目的端口号（2个字节）、数据报长度（2个字节）、校验和（2个字节）。

Q：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？

A：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分析

DNS报文如图所示。

