**中国矿业大学计算机学院**

**2017级本科生计算机网络实验报告**

实验内容 协议报文分析

学生姓名 杨子桢 学 号 08173026

专业班级 信息安全17级1班

学 院 计算机科学与技术学院

任课教师 顾军

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程基础理论掌握程度** | 熟练 🞏 | 较熟练 🞏 | 一般 🞏 | 不熟练 🞏 |
| **综合知识应用能力** | 强 🞏 | 较强 🞏 | 一般 🞏 | 差 🞏 |
| **报告内容** | 完整 🞏 | 较完整 🞏 | 一般 🞏 | 不完整 🞏 |
| **报告格式** | 规范 🞏 | 较规范 🞏 | 一般 🞏 | 不规范 🞏 |
| **实验完成状况** | 好 🞏 | 较好 🞏 | 一般 🞏 | 差 🞏 |
| **工作量** | 饱满 🞏 | 适中 🞏 | 一般 🞏 | 欠缺 🞏 |
| **学习、工作态度** | 好 🞏 | 较好 🞏 | 一般 🞏 | 差 🞏 |
| **抄袭现象** | 无 🞏 | 有 🞏 姓名: | | |
| **存在问题** |  | | | |
| **总体评价** |  | | | |

综合成绩： 任课教师签字：

年 月 日

**实验编号：03**

**实验名称：协议报文分析**

**实验内容：**

1. 运用抓包工具，分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包。
2. 运用抓包工具，连续获取面向连接的互联网访问情形下的本机网卡数据包；对连续获取的数据包找到执行面向连接过程的报文，给出实现面向连接过程（TCP三次握手）的详细分析。
3. 分别对不同互联网访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义；要求分别获取WWW服务、Email服务、QQ通信和迅雷文件下载四种不同网络服务过程中的数据包。

**实验要求：**

（1）运用抓包工具，实时抓包，记录包状态变化；

（2）给出不同应用情境下的不同层次数据包的分析结果。

（3）透过Web服务访问，分析HTTP协议工作过程，总结HTTP协议特点；透过HTTP工作过程分析，获取TCP协议的工作过程，验证连接建立的三次握手过程，以及滑动窗口工作机制。

**预习要求：**

提前通过互联网或在实验室开始实验前登录实验管理服务器，点击预习链接，阅览或下载实验指导书——预习\网络协议\进阶-IP分组基本报文分析。

**操作与观察：**

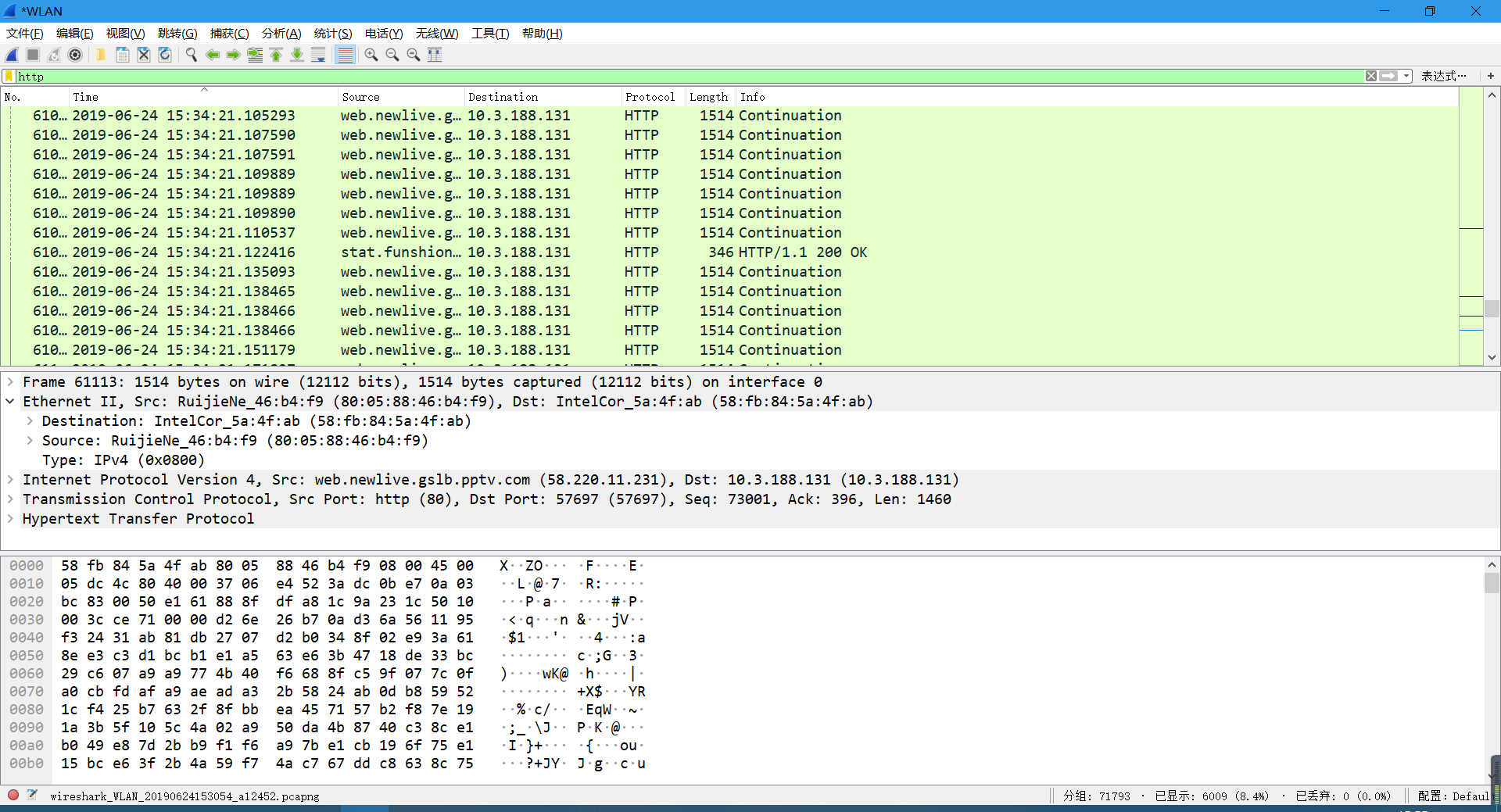
正确按照实验指导书步骤操作，观察记录下操作结果。

**实验报告要求：**

1. 按照实验要求，完成全部实验内容
2. 在标准实验报告书上填写全部实验操作记录和观察结果
3. 登录实验管理服务器，提交实验报告电子档。
4. 提交纸质版实验报告。

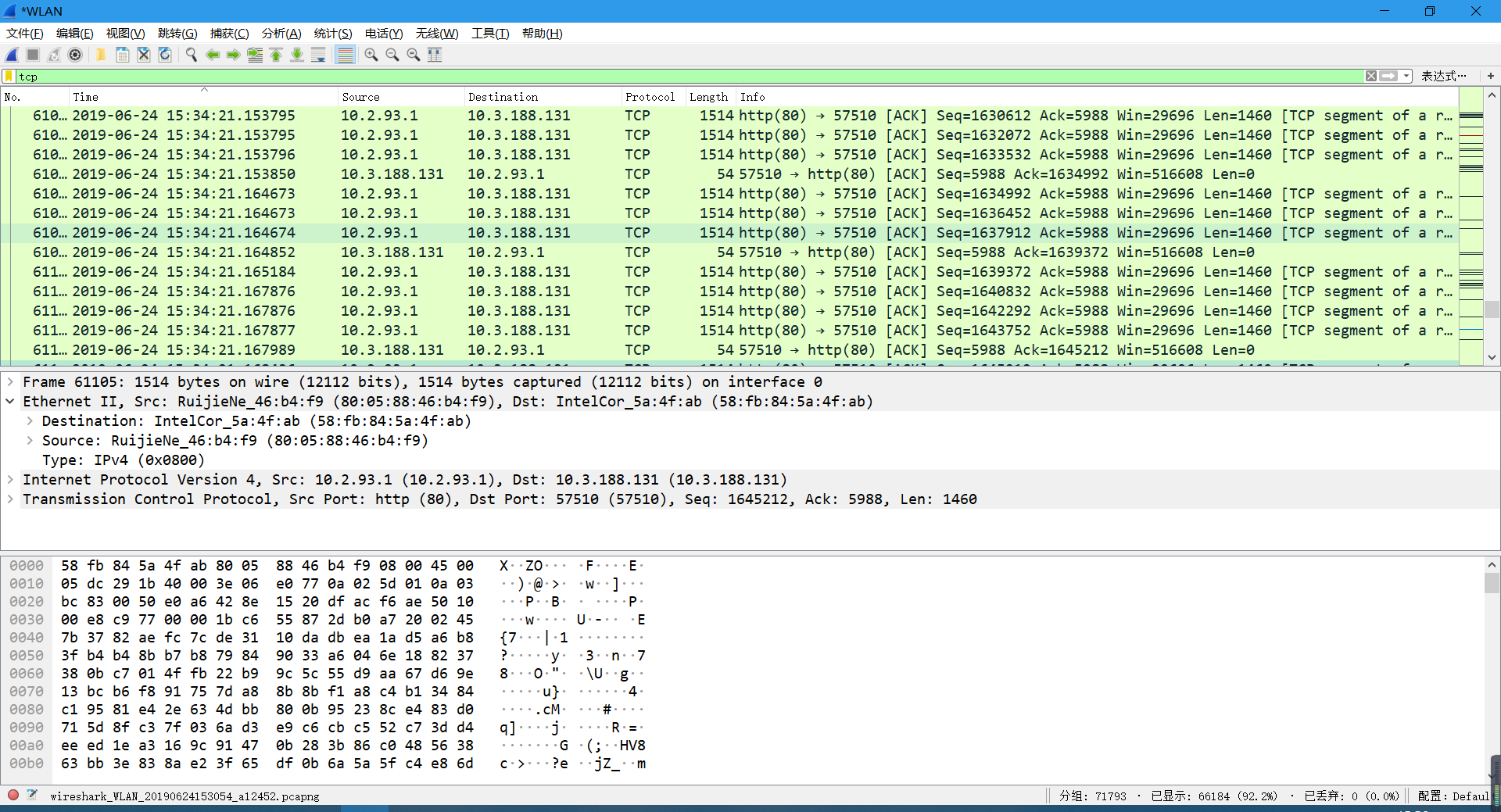
**实验报告内容：**

1. 运用抓包工具，分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包。
2. HTTP协议（HyperText Transfer Protocol，超文本传输协议）是用于从WWW服务器传输超文本到本地浏览器的传输协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示(如文本先于图形)等。如图3-1-1所示。



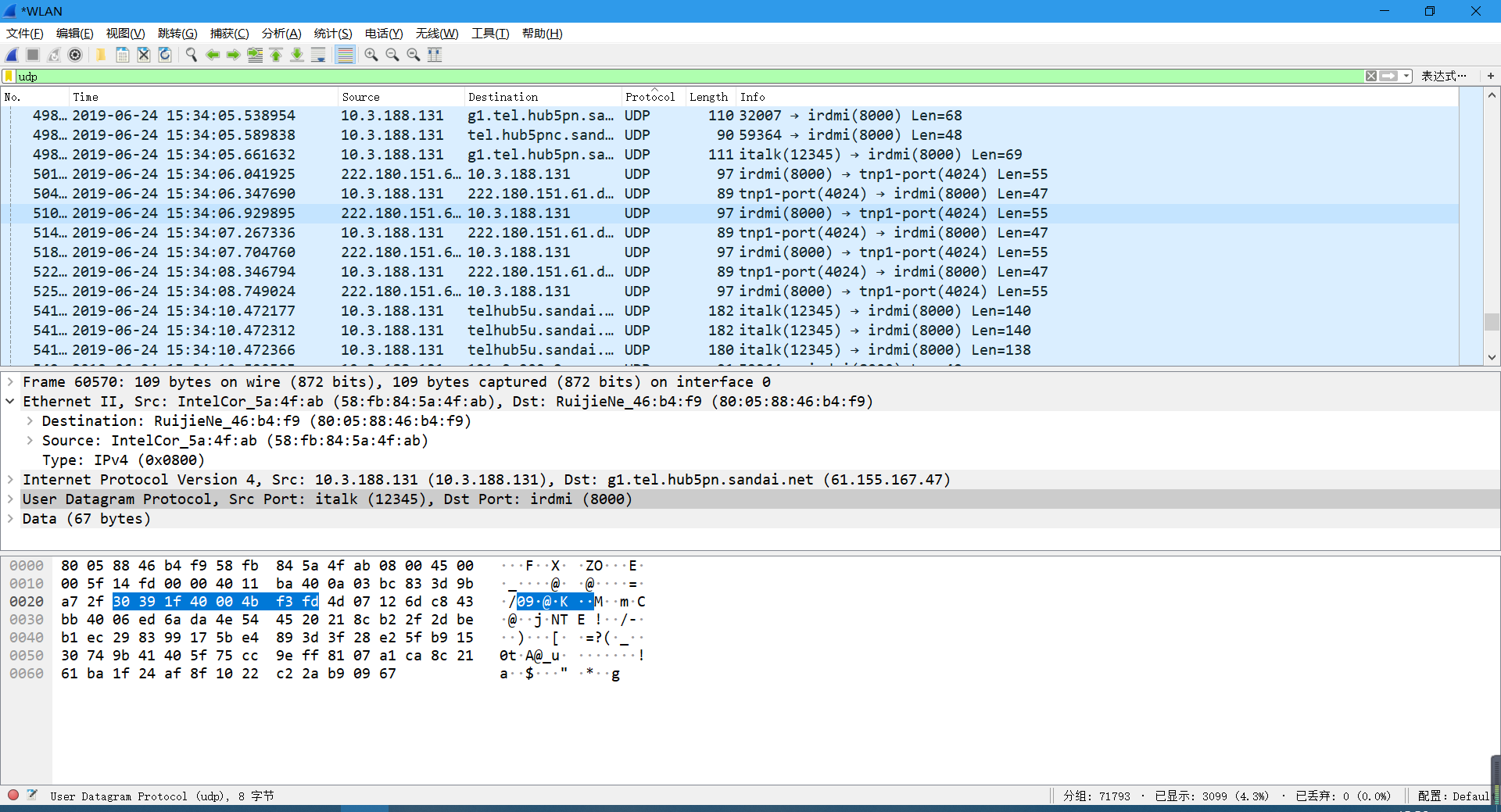
**图3-1-1**

1. TCP（Transmission Control Protocol [传输控制协议](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E6%8E%A7%E5%88%B6%E5%8D%8F%E8%AE%AE/9727741)）是一种面向连接的、可靠的、基于字节流的[传输层](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82/4329536)通信协议，由IETF的RFC 793定义。在简化的计算机网络OSI模型中，它完成第四层传输层所指定的功能，用户数据报协议（UDP）是同一层内[1]  另一个重要的传输协议。在因特网协议族（Internet protocol suite）中，TCP层是位于IP层之上，应用层之下的中间层。不同主机的应用层之间经常需要可靠的、像管道一样的连接，但是IP层不提供这样的流机制，而是提供不可靠的包交换。如图3-1-2所示。



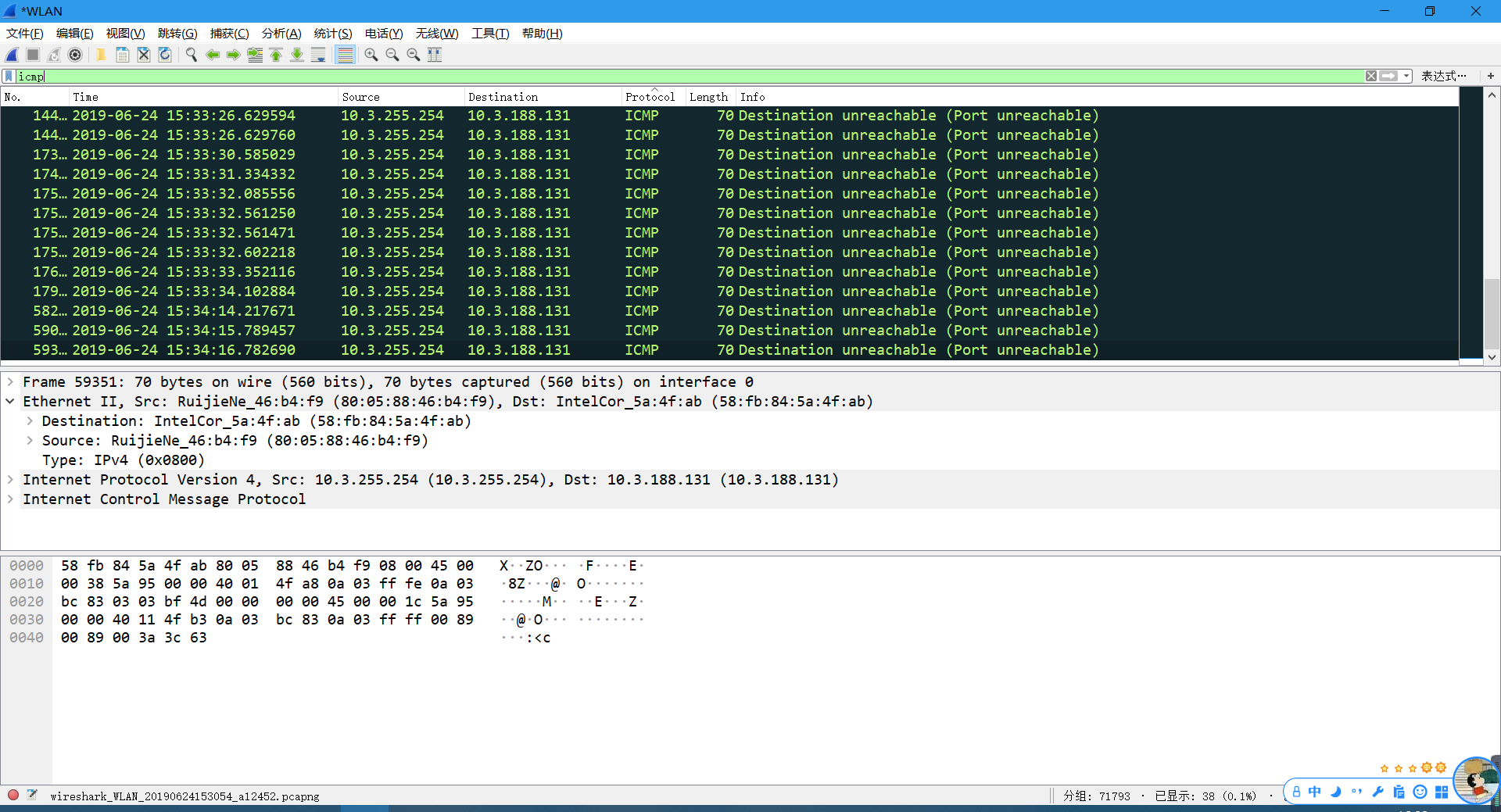
**图3-1-2**

1. UDP是[OSI](https://baike.baidu.com/item/OSI)参考模型中一种无连接的传输层协议，它主要用于不要求分组顺序到达的传输中，分组传输顺序的检查与排序由应用层完成[2]  ，提供面向事务的简单不可靠信息传送服务。UDP 协议基本上是[IP协议](https://baike.baidu.com/item/IP%E5%8D%8F%E8%AE%AE)与上层协议的接口。UDP协议适用[端口](https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3)分别运行在同一台设备上的多个[应用程序](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F)。如图3-1-3所示。



**图3-1-3**

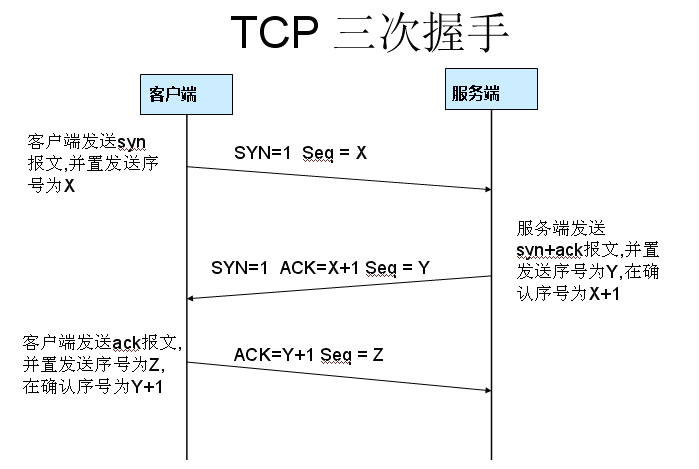
1. ICMP（Internet Control Message Protocol）Internet控制[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87/3164352)协议。它是[TCP/IP协议簇](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE%E7%B0%87)的一个子协议，用于在IP[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151)、[路由](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1)器之间传递控制消息。控制消息是指[网络通](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%80%9A)不通、[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151)是否可达、[路由](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1/363497)是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。如图3-1-4所示。



**图3-1-4**

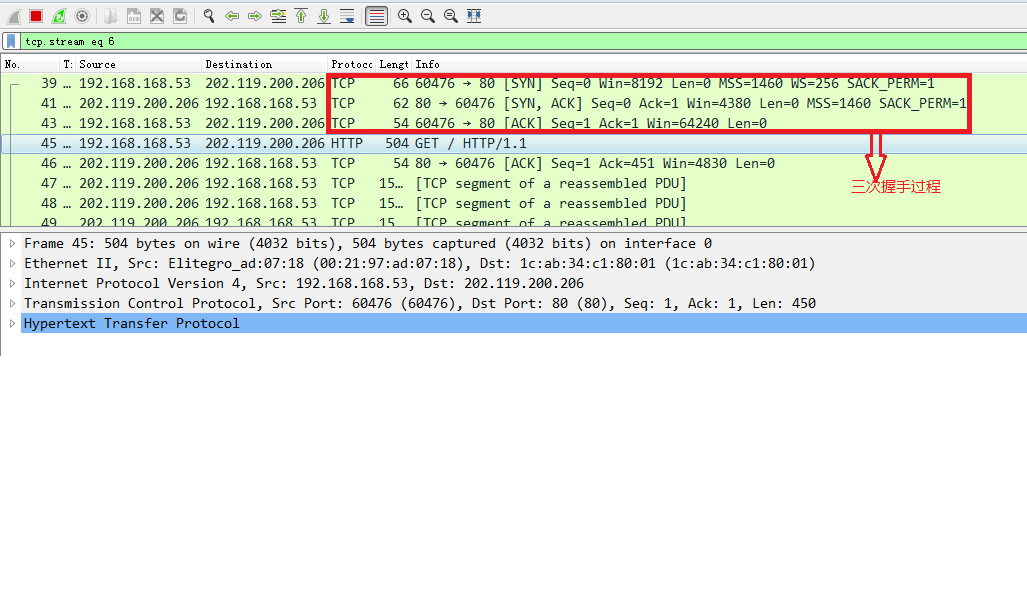
1. 运用抓包工具，连续获取面向连接的互联网访问情形下的本机网卡数据包；对连续获取的数据包找到执行面向连接过程的报文，给出实现面向连接过程（TCP三次握手）的详细分析。

三次握手过程如下：



打开wireshark, 打开浏览器输入www.cumt.edu.cn

在wireshark中输入http过滤， 然后选中GET /HTTP/1.1的那条记录，右键然后点击"Follow TCP Stream"。如图3-2-1所示。

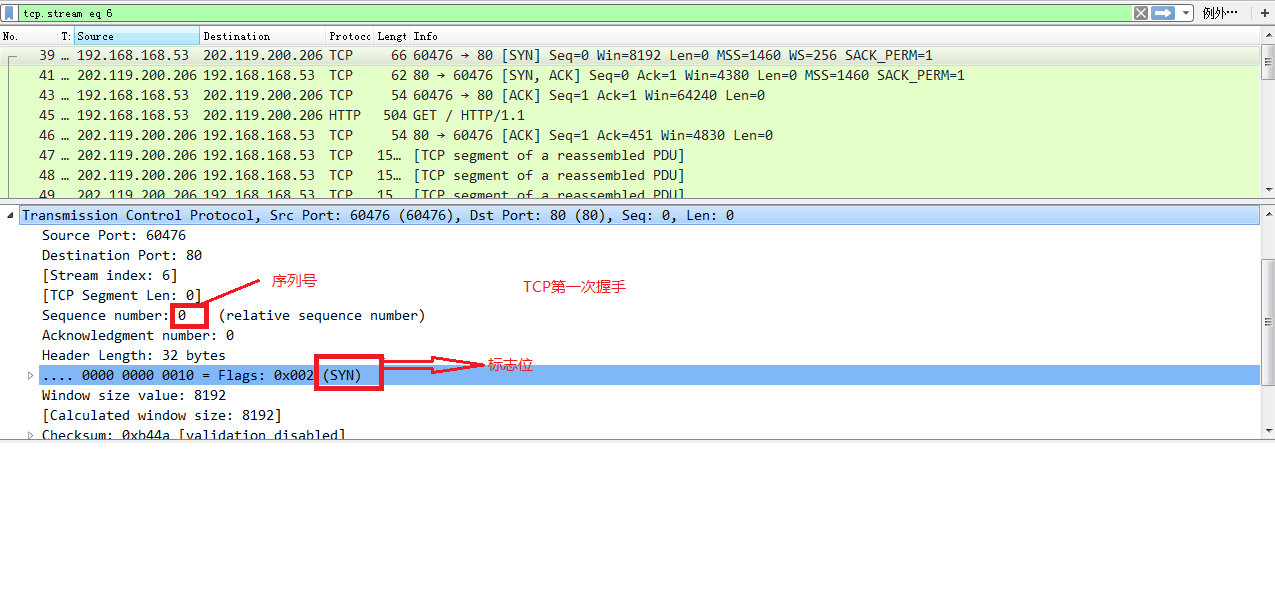


**图3-2-1**

图中可以看到wireshark截获到了三次握手的三个数据包。第四个包才是HTTP的， 这说明HTTP的确是使用TCP建立连接的。

（1）第一次握手数据包

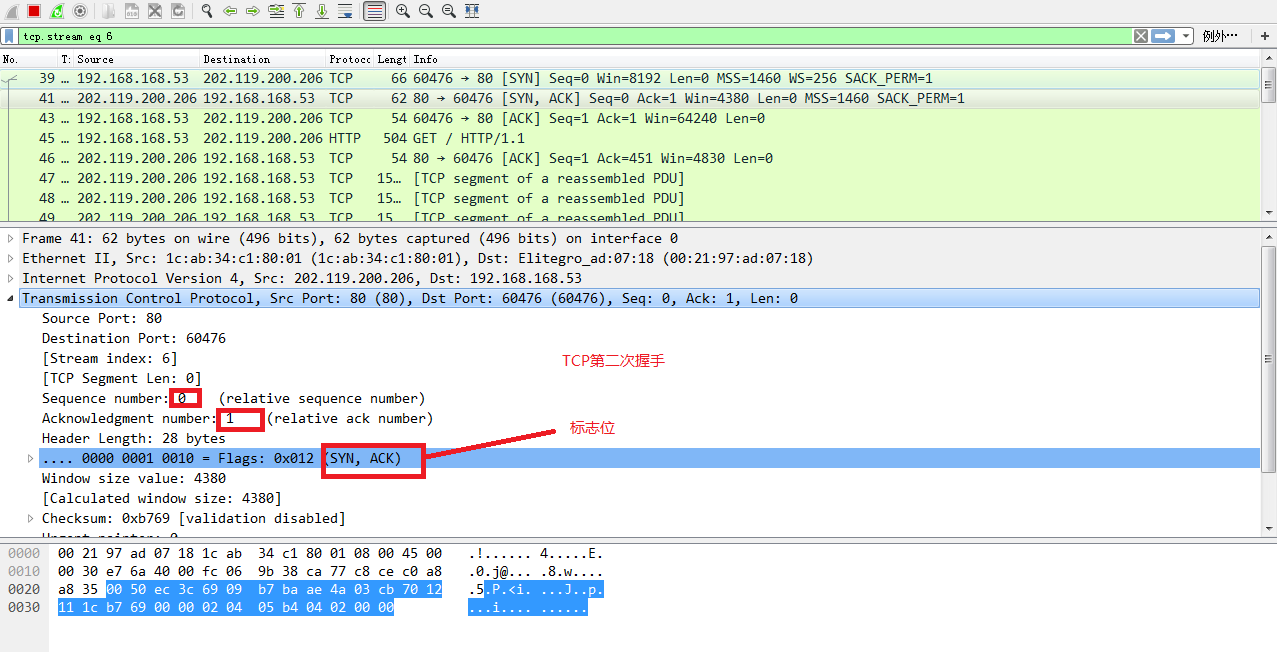
客户端发送一个TCP，标志位为SYN，序列号为0， 代表客户端请求建立连接。 如图3-2-2所示。



**图3-2-2**

（2）第二次握手的数据包

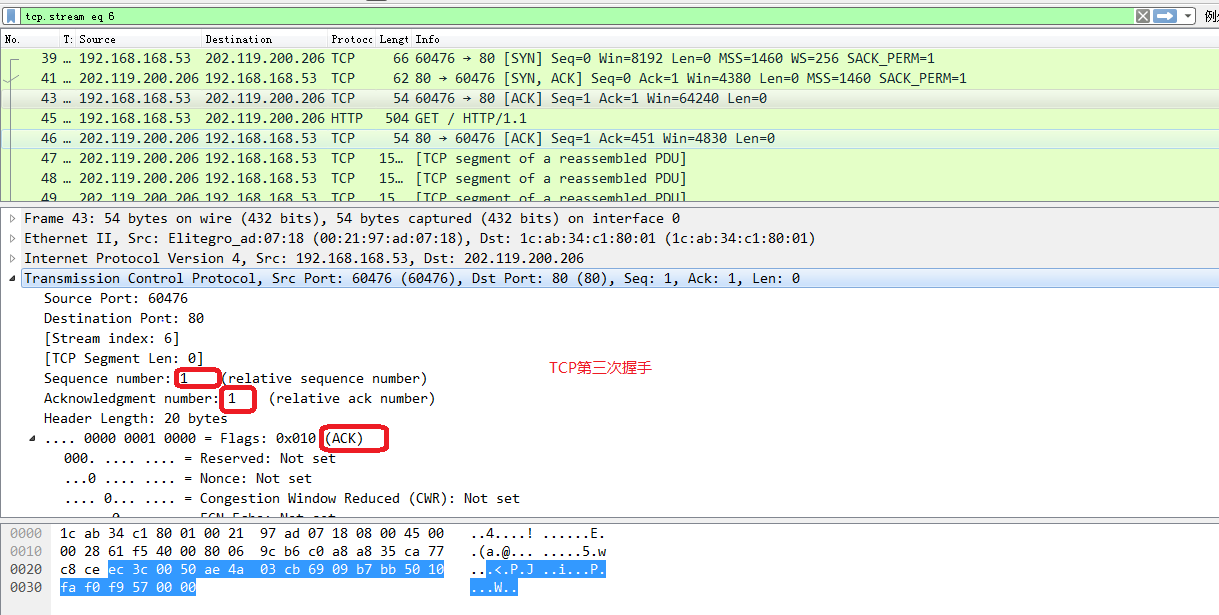
服务器发回确认包, 标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置1, 如图3-2-3所示。



**图3-2-3**

（3）第三次握手的数据包

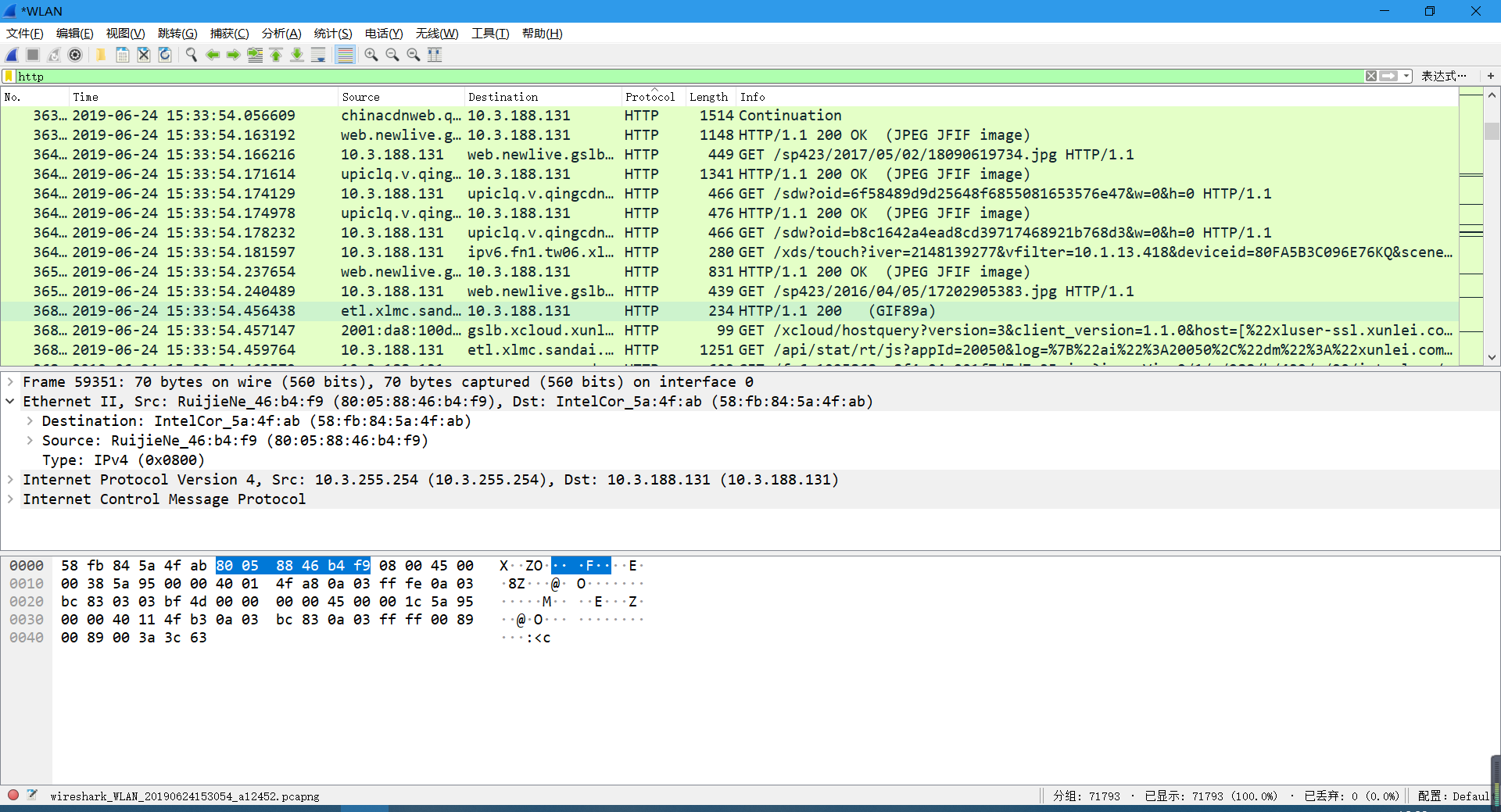
客户端再次发送确认包(ACK) SYN标志位为0,ACK标志位为1.并且把服务器发来ACK的序号字段+1,放在确定字段中发送给对方.并且在数据段放写ISN的+1, 如图3-2-4所示。



**图3-2-4**

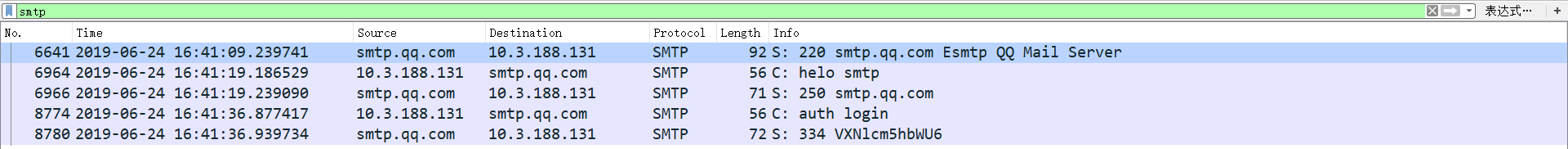
就这样通过了TCP三次握手，建立了连接

1. 分别对不同互联网访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义；要求分别获取WWW服务、Email服务、QQ通信和迅雷文件下载四种不同网络服务过程中的数据包。
2. WWW服务



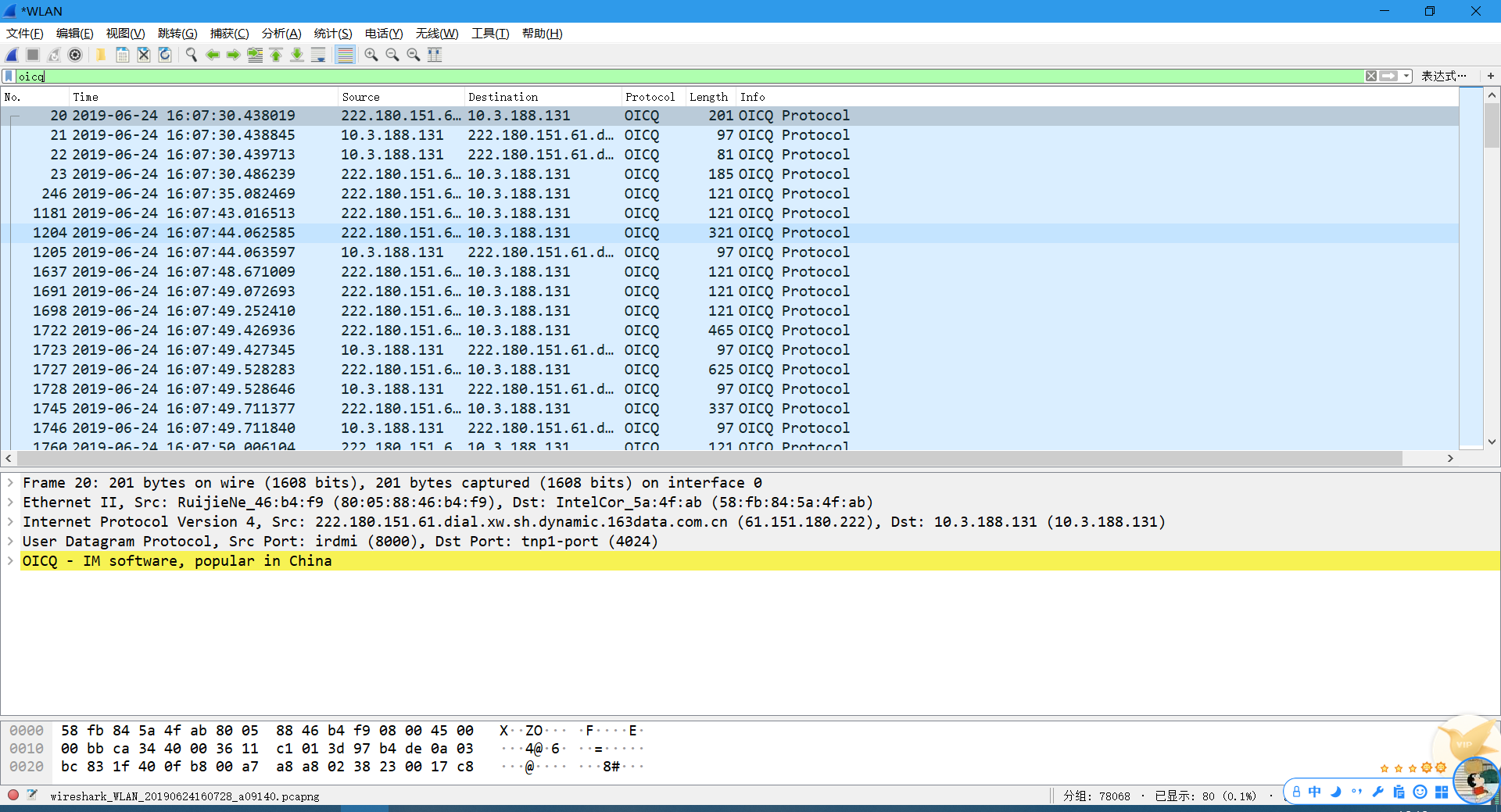
**图3-3-1**

1. Email服务



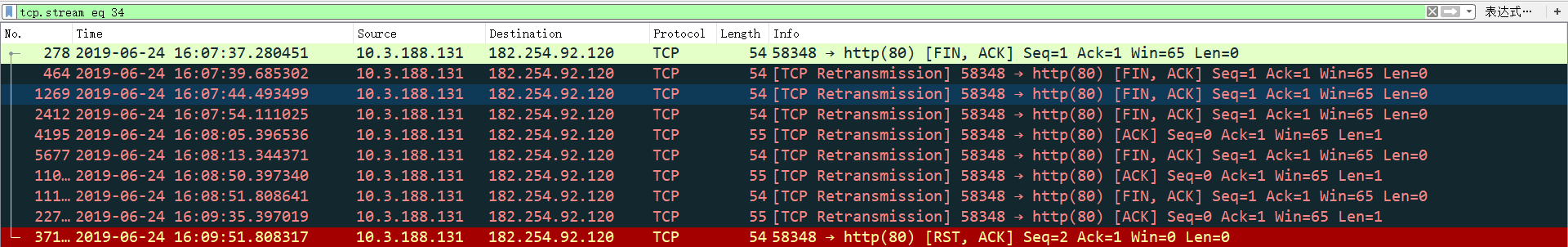
**图3-3-2**

1. QQ通信



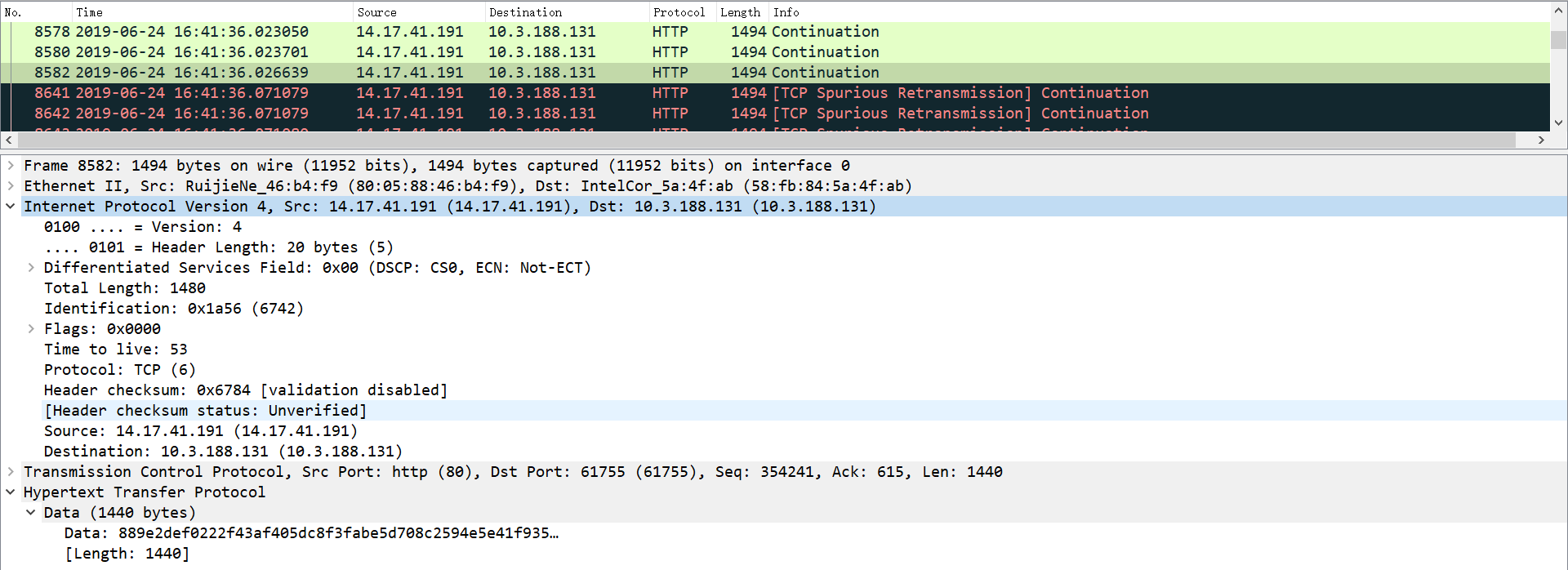
**图3-3-3**

1. 迅雷文件下载



**图3-3-4**

1. HTTP数据包分析：

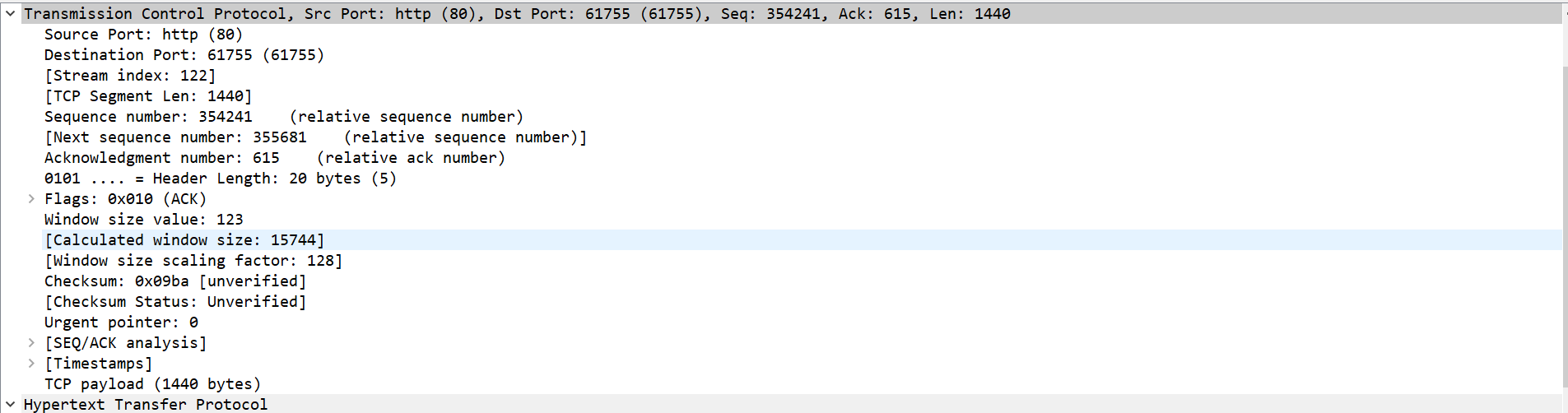


**图3-3-5**

A. 第一行，数据链路层帧的序号为8582，捕获字节数等于传送字节数：1494字节；

B. 第二行，以太网，数据链路层。源Mac地址为80:05:88:46:b4:f9；目标Mac地址为58:fb:84:5a:4f:ab；

C. 第三行，IPV4协议，是网络层；源IP地址为14.17.41.191；目标IP地址为10.3.188.131，首部长度为20字节，总长度是1480字节；

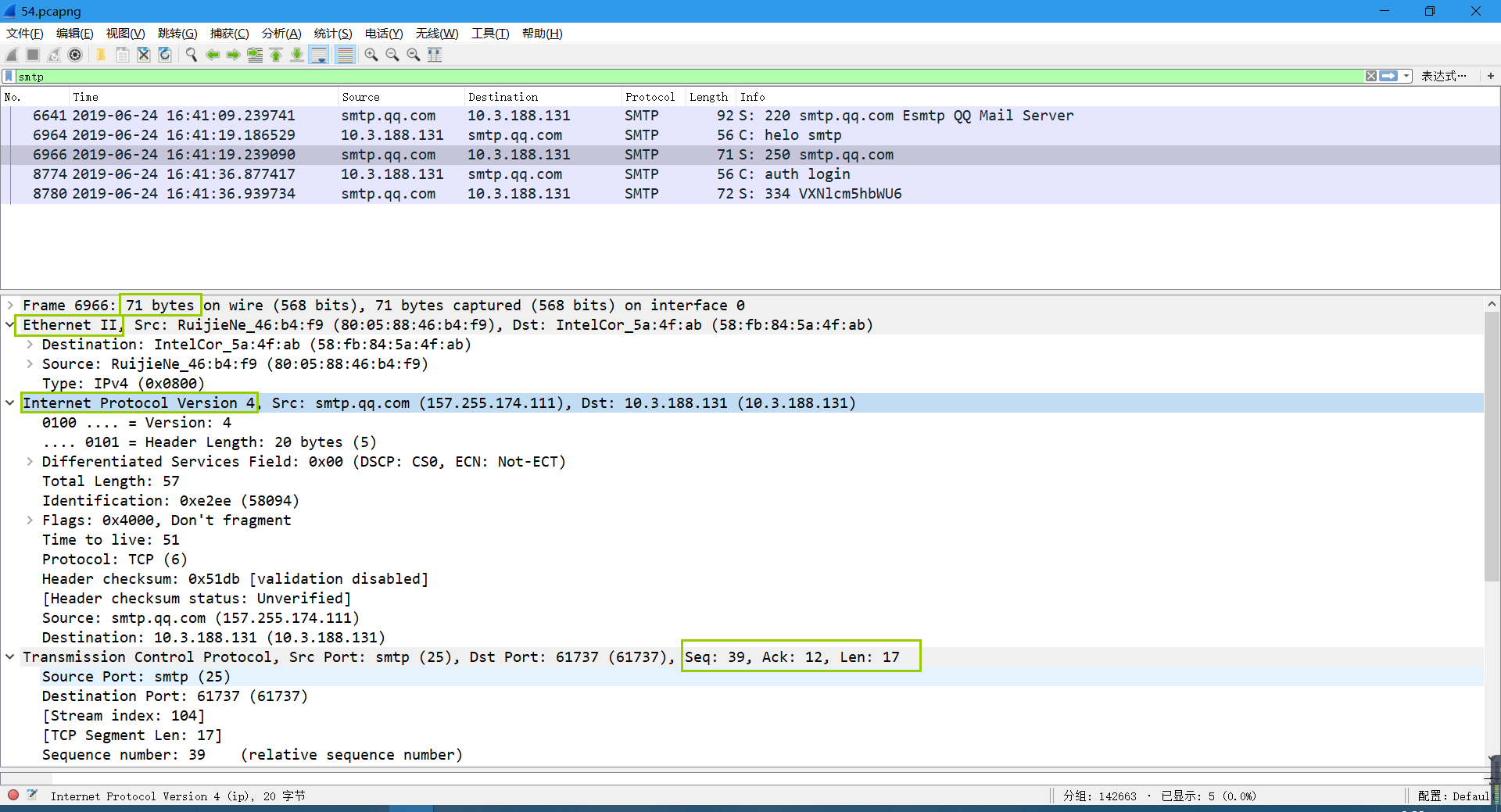


**图3-3-6**

D. 第四行，TCP协议，是传输层；源端口(80)，目标端口(61755)，其中序号seq是354241号，确认号ack是615号，窗口大小是15744，数据总长度是1440字节。

E. 第五行，应用层数据长度为1440字节，可知TCP首部也是20字节。

6.SMTP数据包分析：

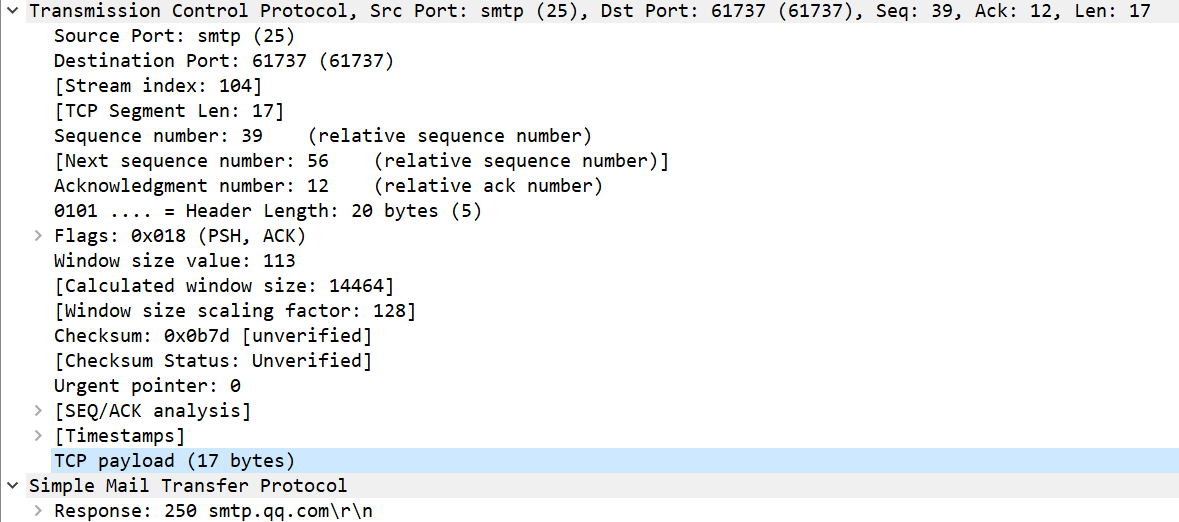


**图3-3-7**

A. 第一行，数据链路层帧的序号为6966，捕获字节数等于传送字节数：71字节；

B. 第二行，以太网，数据链路层。源Mac地址为80:05:88:46:b4:f9；目标Mac地址为58:fb:84:5a:4f:ab；

C. 第三行，IPV4协议，是网络层；源IP地址为157.255.174.111,目标IP地址为10.3.188.131，首部长度为20字节，总长度是57字节；

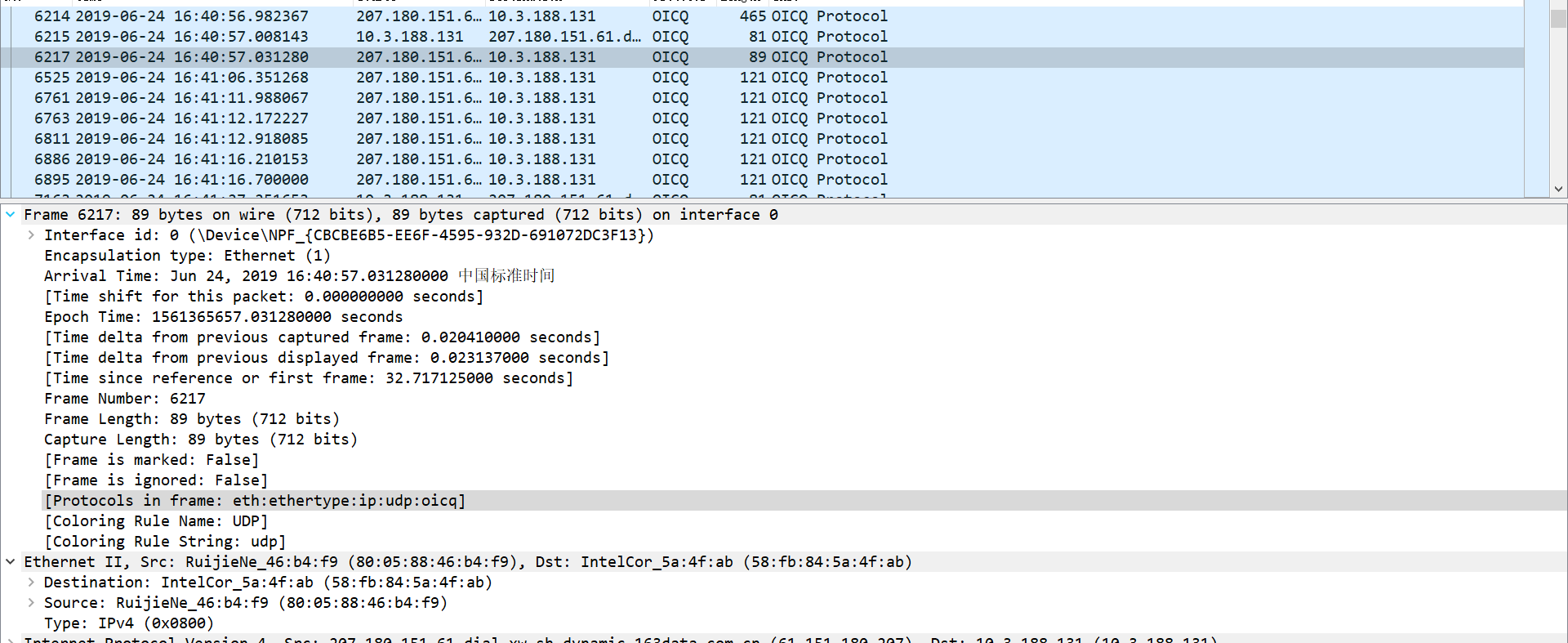


**图3-3-8**

D. 第四行，TCP协议，是传输层；源端口(25)，目标端口(61737)，其中序号seq是39号，确认号ack是12号，窗口大小是113，数据总长度是17字节。检验和是0x0d7c,紧急指针Urgent pointer置0 .

E. 第五行，应用层数据长度为17字节，数据内容是smtp对主机的回应，表示已连接。另外可知TCP首部也是20字节。

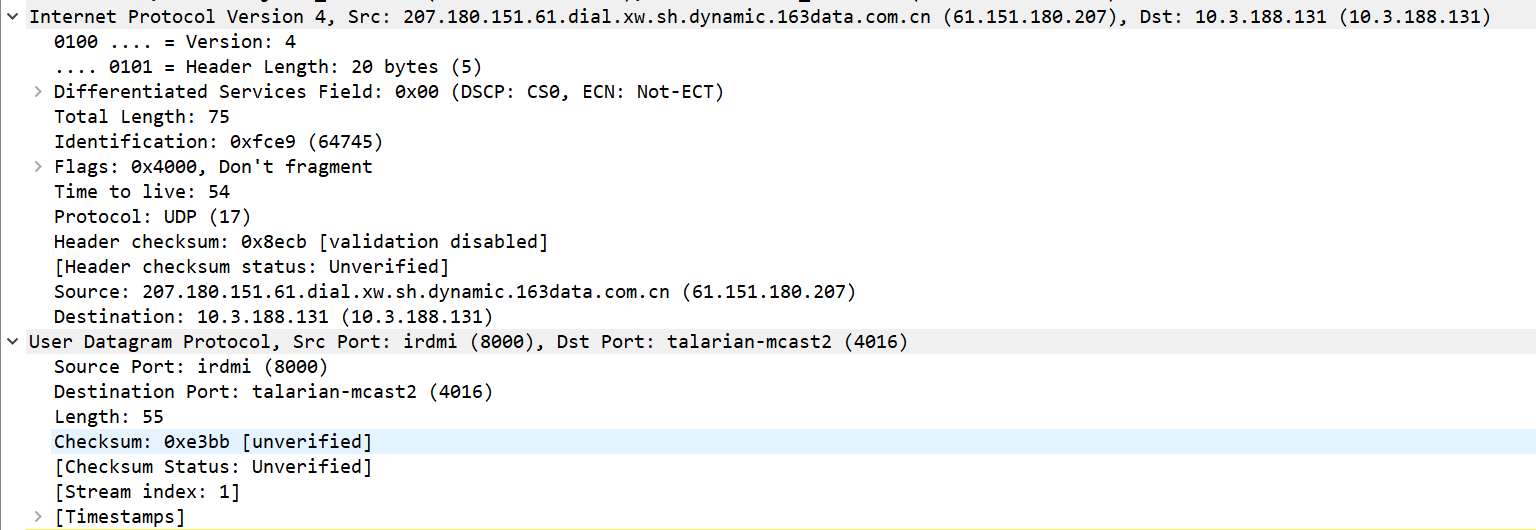
7.OICQ数据包分析



**图3-3-9**

A. 第一行，数据链路层帧的序号为6217，捕获字节数等于传送字节数：712字节；

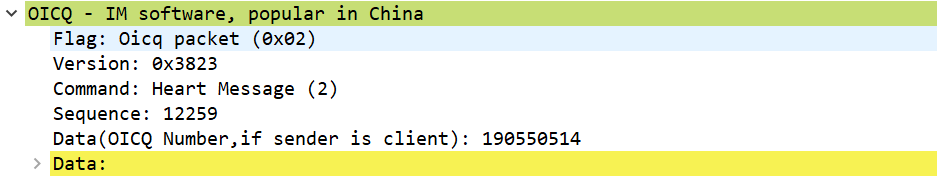
B. 第二行，以太网，数据链路层。源Mac地址为80:05:88:46:b4:f9；目标Mac地址为58:fb:84:5a:4f:ab；



**图3-3-10**

C. 第三行，IPV4协议，是网络层；源IP地址为61.151.180.207目标IP地址为10.3.188.131，首部长度为20字节，总长度是75字节；

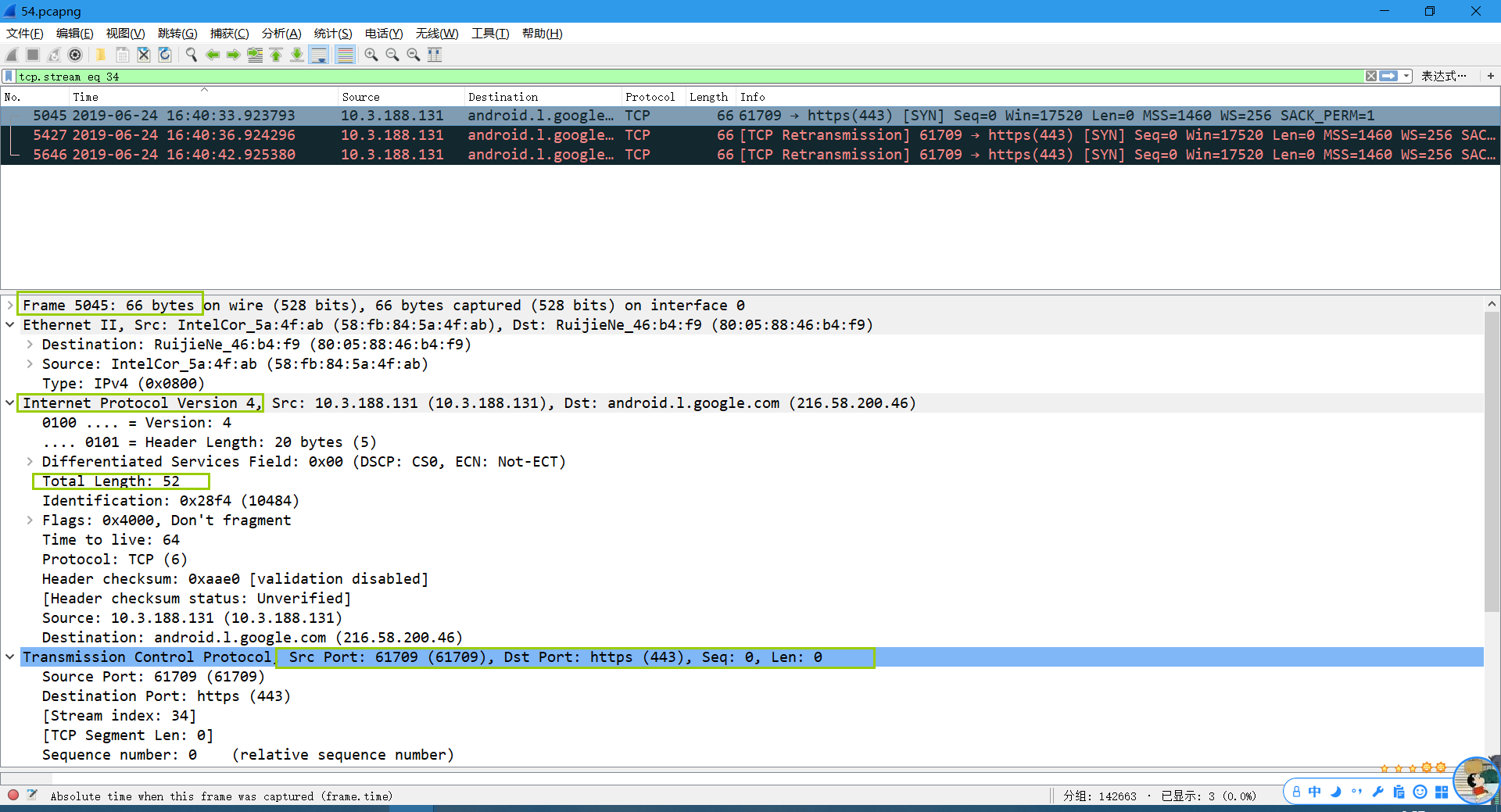
D. 第四行，UDP协议，是传输层；源端口(8000)，目标端口(4016)，数据总长度是55字节。检验和是0x。



**图3-3-11**

E. 第五行，应用层数据长度推算为35字节，数据内容是oicq包。

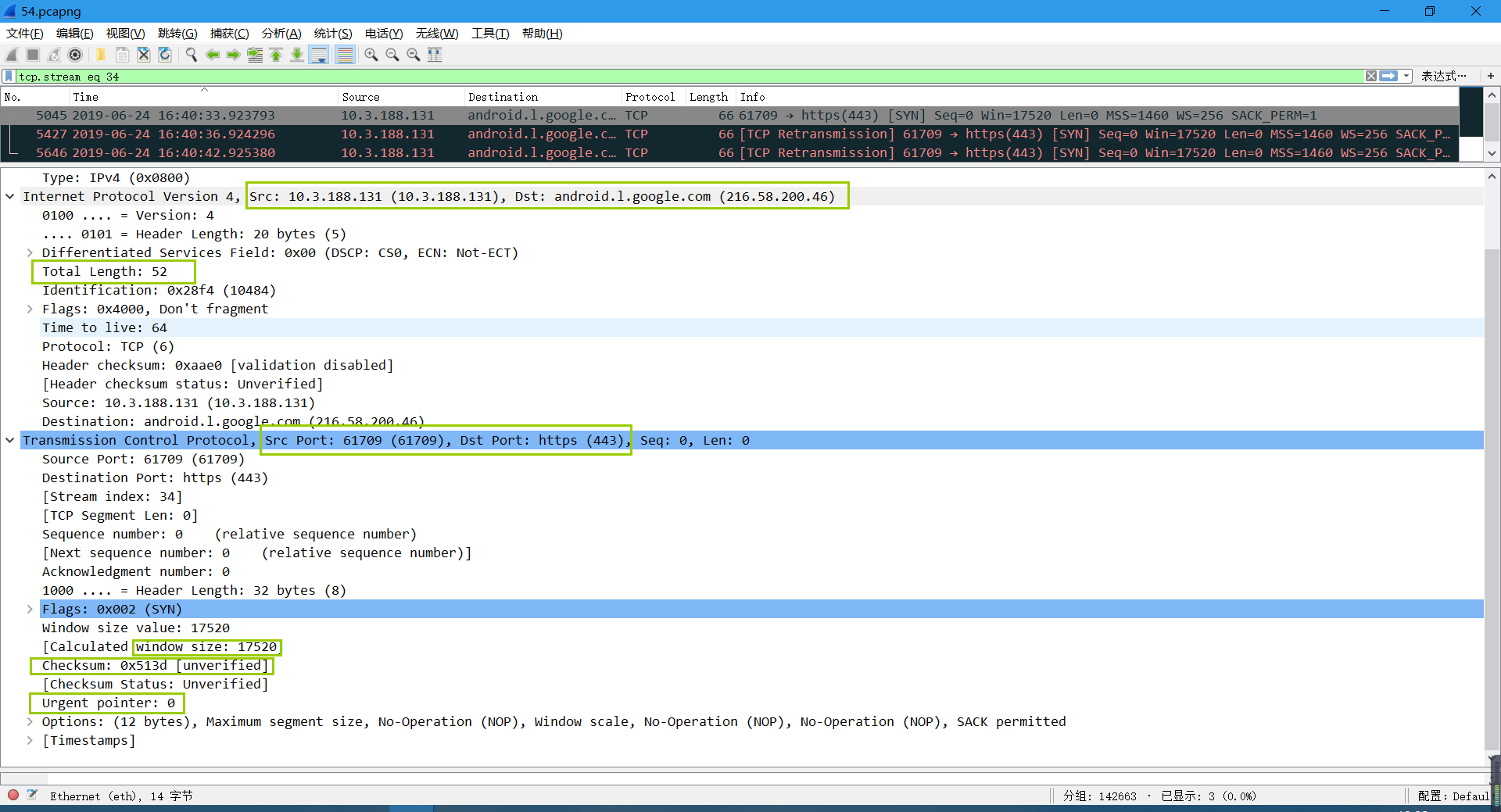
8.迅雷下载数据包分析



**图3-3-12**

A. 第一行，数据链路层帧的序号为5054，捕获字节数等于传送字节数：66字节；

B. 第二行，以太网，数据链路层。源Mac地址为58:fb:84:5a:4f:ab；目标Mac地址为80:05:88:46:b4:f9。



**图3-3-13**

C. 第三行，IPV4协议，是网络层；源IP地址为10.3.188.131,目标IP地址为216.58.200.46，首部长度为20字节，总长度是52字节；

D. 第四行，TCP协议，是传输层；源端口(61709)，目标端口(443)，其中序号seq是0号，确认号ack是0号，窗口大小是17520，这应该算是tcp的第一次握手，表示客户端第一次建立连接。检验和是0x513d,紧急指针Urgent pointer置0 。

**实验体会：**

首先，学会了使用wireshark网络抓包工具，并且学会分析抓包内容。其次，对于计算机网络分层的理解也更加深刻。从最底层的物理层，当然wireshark只能从高一层的数据链路层的数据帧开始，然后到Mac硬件地址，网络层的IP数据包，运输层的TCP包，应用层的数据包。