**实验报告**

姓名： 林炬乙 学号： 3180103721

课程名称： [数据通信与计算机网络](https://courses.zju.edu.cn/course/28804/content#/) 任课老师：

实验名称： 网络数据监测与分析 实验日期： 2021/4/13

# 1 实验目的和要求

（分点简要说明本次实验需要进行的工作和最终的目的）

利用wireshark学习网络数据检测和分析

# 2 实验原理

翻译自官网: Wireshark是世界上使用最广泛的网络协议分析器。 它使您可以从微观角度查看网络中发生的事情，并且是许多商业和非营利性企业，政府机构和教育机构的事实上（通常是法律上）的标准。

Wireshark具有丰富的功能集，其中包括：深入检查数百种协议，并始终添加更多内容实时捕获和离线分析标准三窗格数据包浏览器.

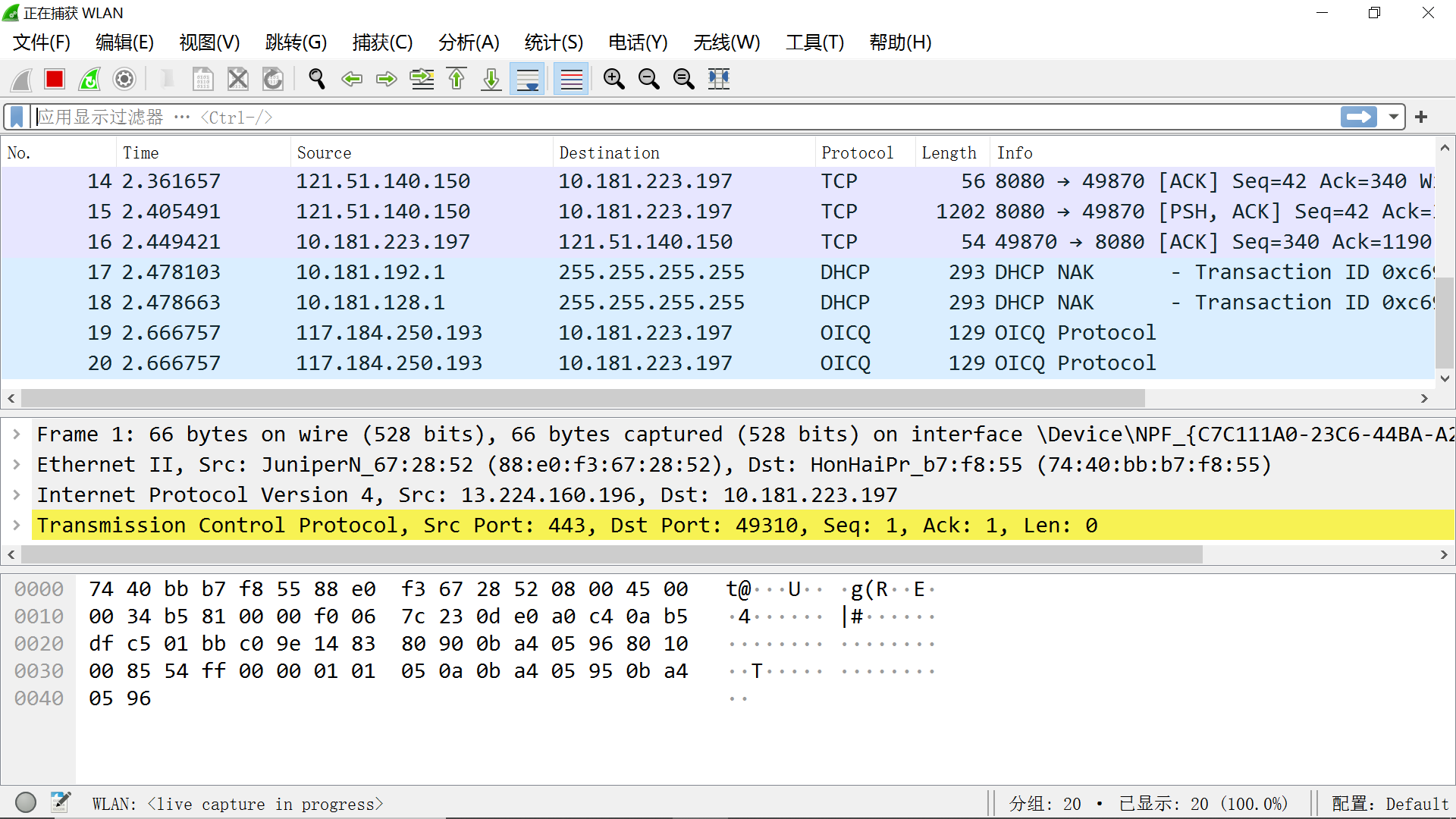
多平台：可在Windows，Linux，macOS，Solaris， FreeBSD，NetBSD等许多捕获的网络数据可以通过GUI或TTY模式的TShark实用程序进行浏览

业界最强大的显示过滤器丰富的VoIP分析读取/写入许多不同的捕获文件格式.

# 3 实验内容

（分点阐述实验步骤）

1. 捕获wlan, 观察所有网络包.

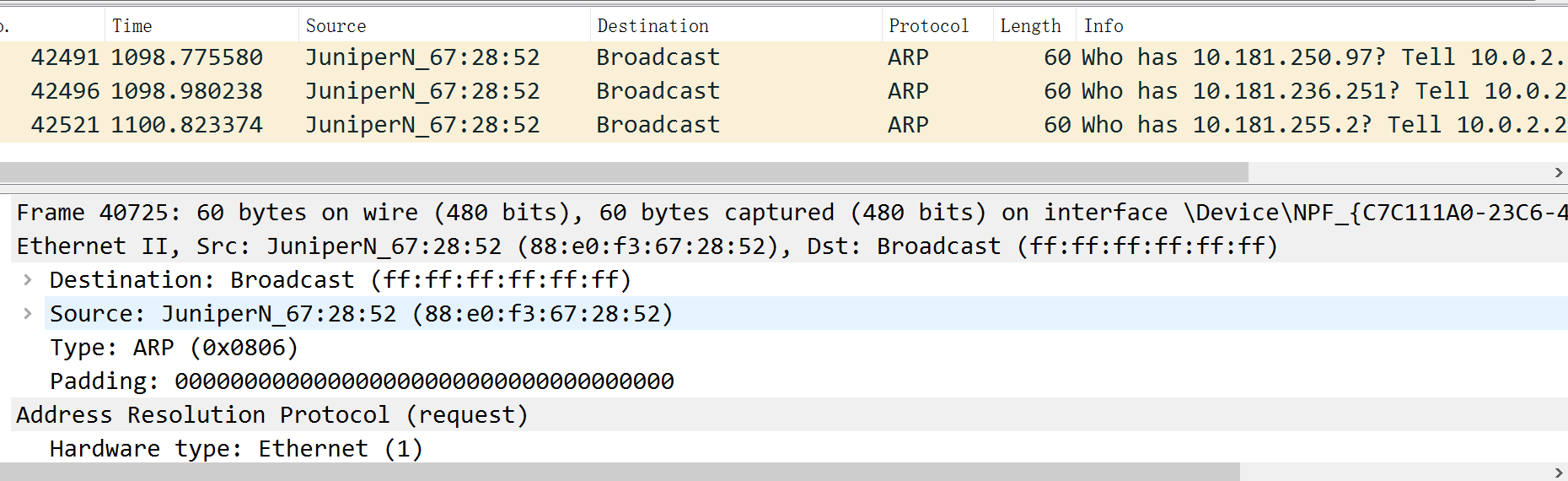


中间是详细信息, Frame：「物理层」数据帧情况。Ethernet：「数据链路层」以太网头部信息。

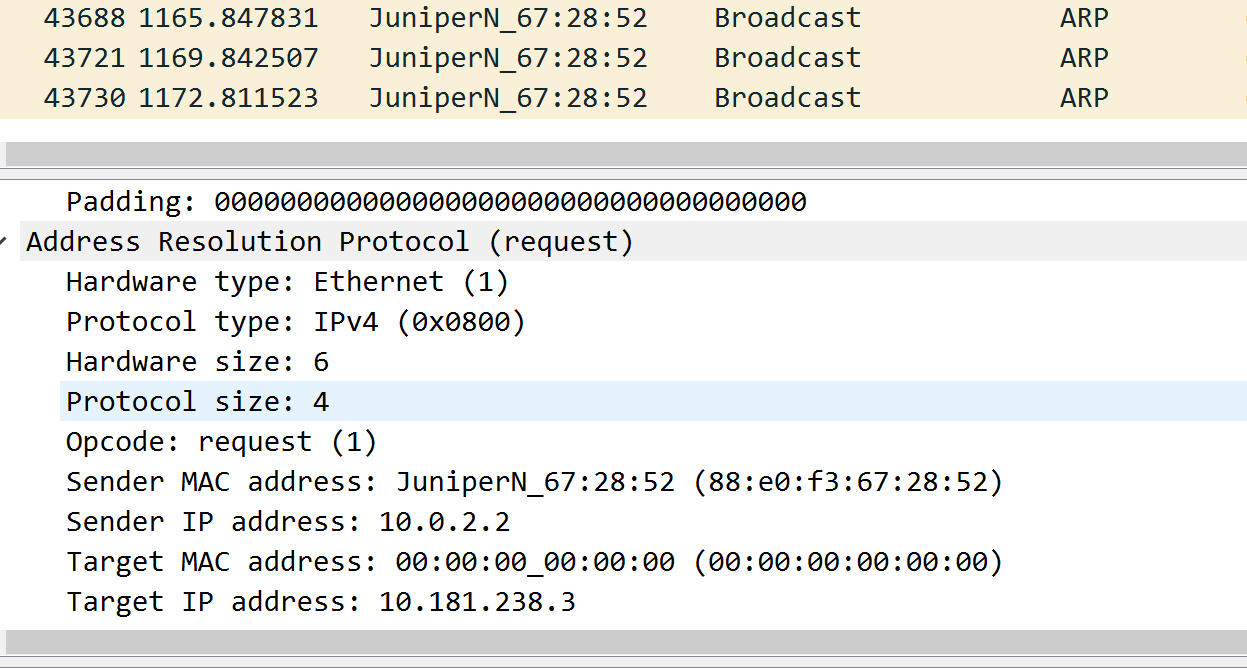
Internet Protocol Version 4：「网络层」数据包头部信息, IP用了IPV4. Transmission Control Protocol：「传输层」数据段头部信息。可以看到TCP层的端口号以及seq1 确认号ack1,

可以发现，一些行文字的底色不同。不同报文采用不同的颜色来区分。

我们来抓取数据链路层ARP地址解析协议.



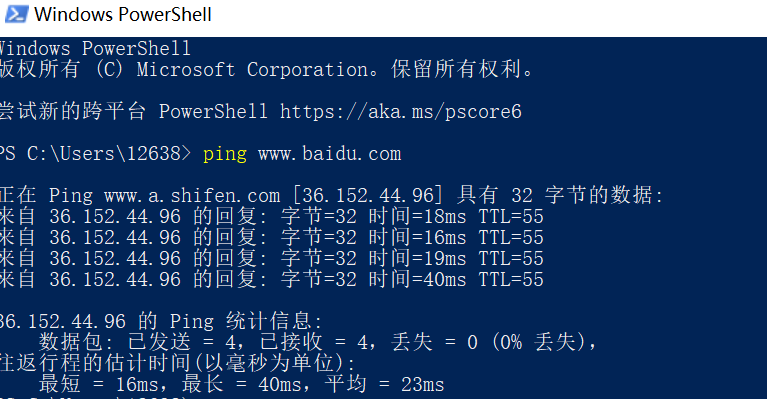
我们可以看到以太网的arp请求, 目的端, 发送端

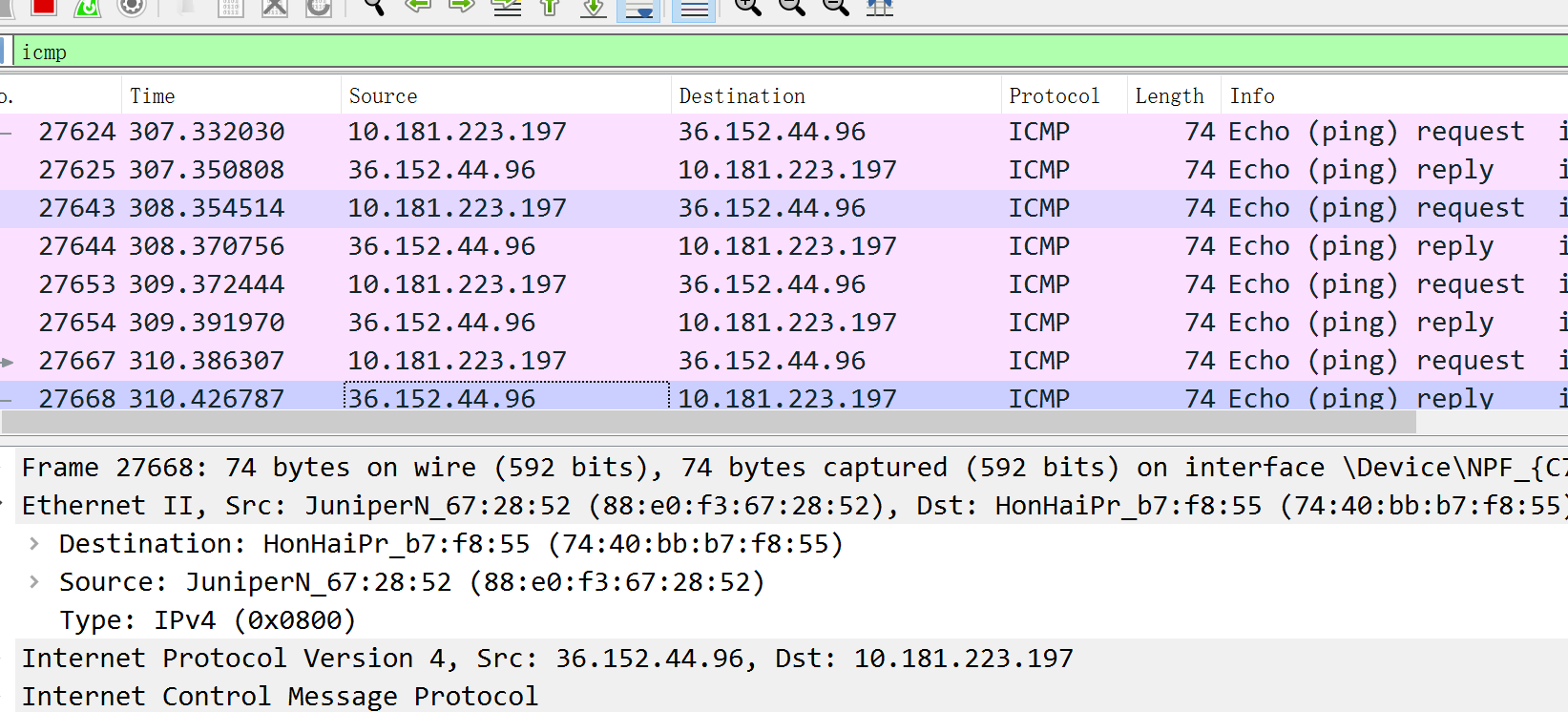


可以看到操作类型, 1代表请求2代表响应, 他是一个广播, 所以mac地址为全0 .就是发送给所有ip地址. 想知道target ip地址对应的硬件地址, target ip地址收到了之后就会响应,把自己的硬件地址发送过去.

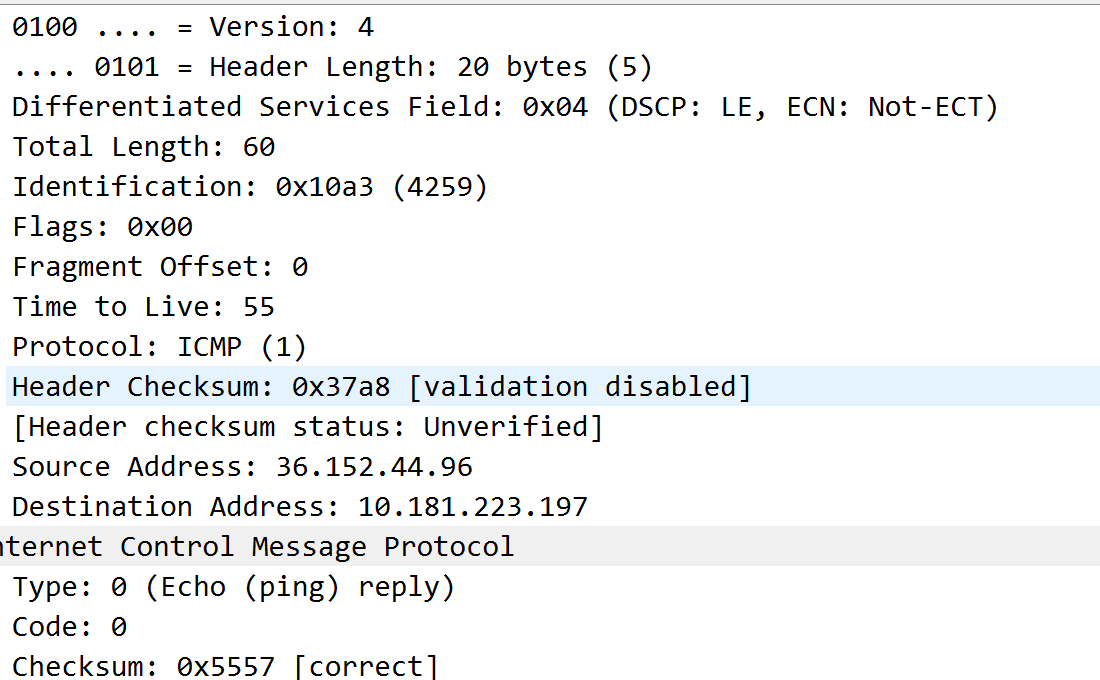
IP协议

* Icmp是网络层的一个协议, 传递控制消息.



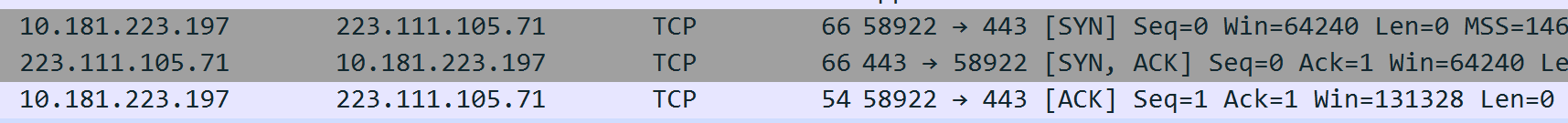


在 Wireshark 中，我们可以看到一共抓取了 8 个数据包，与命令行显示的数量一致，分别为双方的请求与应答。

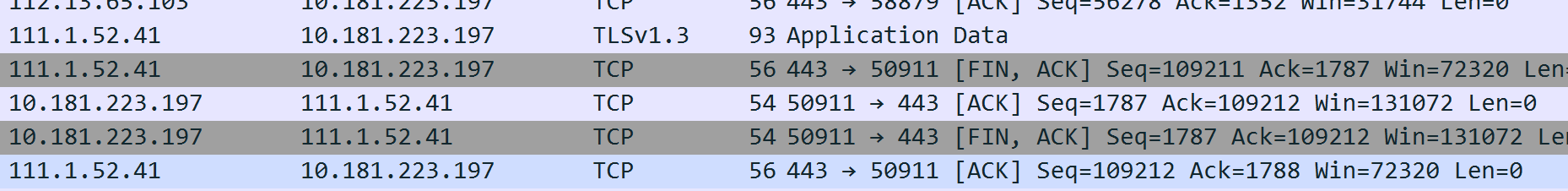


看到ip 版本号, ip首部长度20bytes, 首部载荷总长度60字节,ttl 为55和命令行一致, 请求 0 代表应答.

三次握手



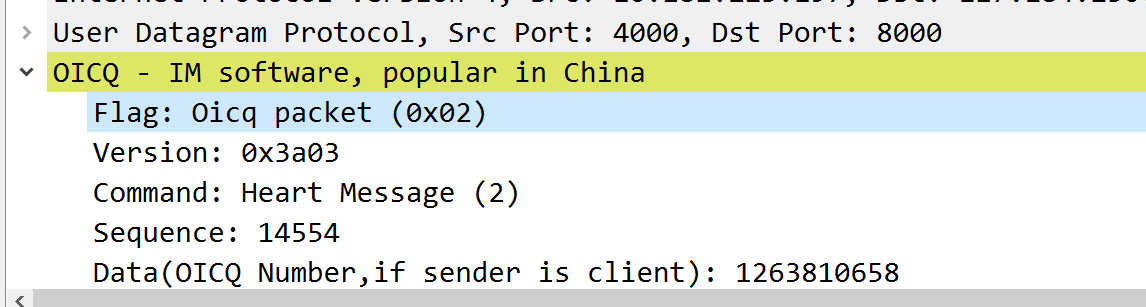
三次握手,客户端发送一个 TCP，标志位为 SYN，序列号为 0，客户端请求建立连接。服务器发回确认包，标志位为 SYN，ACK。客户端再次发送确认包，SYN 标志位为 0，ACK 标志位为 1，将服务器发来的 ACK 序号字段加 1，放在确定字段中发送给对方。



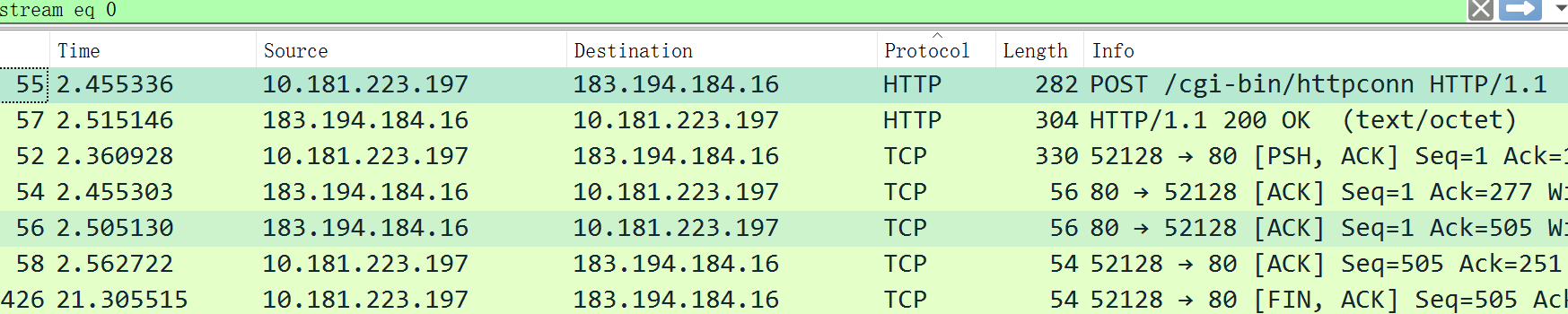
四次挥手, 客户端发送结束包fin,ack标志位为1, 服务器发送ack, 服务器完成最后的发送后, 发送包, fin =1, ack=1, 然后客户端返回ack= 1. 443是https 端口.

我们可以发现,

QQ用的是UDP协议.



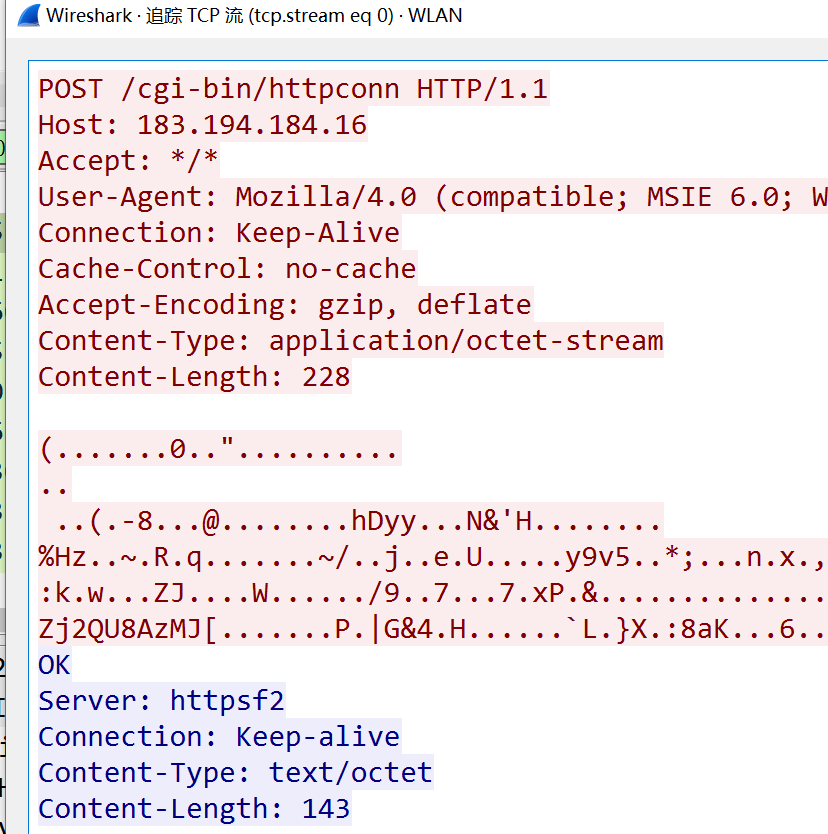
可以抓到qq的数据包. 应用层协议为OICQ



HTTP协议

可以跟踪tcp流, 请求报文, 请求方式是post, host是请求主机的名字,connection是连接方式 是keep alive, accept encoding 客户端可以接收的编码压缩格式,

下面一团乱码是响应实体.



User agent 产生请求的浏览器类型. 200返回码说明成功

