# 中国矿业大学计算机学院

# 2019 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 李春阳 学 号 10193657

专业班级 信息安全 2019-1 班

学 院 计算机科学与技术学院

任课教师 姜秀柱

| | | | | |
|---|---|---|---|---|
| **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：02

项目名称：协议报文分析

实验内容：

（1） 拓扑结构探测：给出实验用机所在机房的局域网以及接入校园网的拓扑结构；

（2） 测试互联网接入路径：运用 tracert 命令测试本机到互联网的接入路径；

（3） 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；

（4） 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） 通过拓扑结构探测，懂得跨网连接的概念，以及跨网连接必须的设备；

（2） 通过 tracert 命令应用，给出校园网连接互联网的接入网结构；

（3） 运用抓包工具，实时抓包，记录包状态变化；

（4） 给出不同应用情境下的不同层次数据包的分析结果。

（5） 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（选做）。

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。

实验步骤

3.2.1 拓扑结构探测

给出实验用机所在机房的局域网以及接入校园网的拓扑结构；

3.2.2 测试互联网接入路径

运用 tracert 命令测试本机到互联网的接入路径；

3.2.3 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；

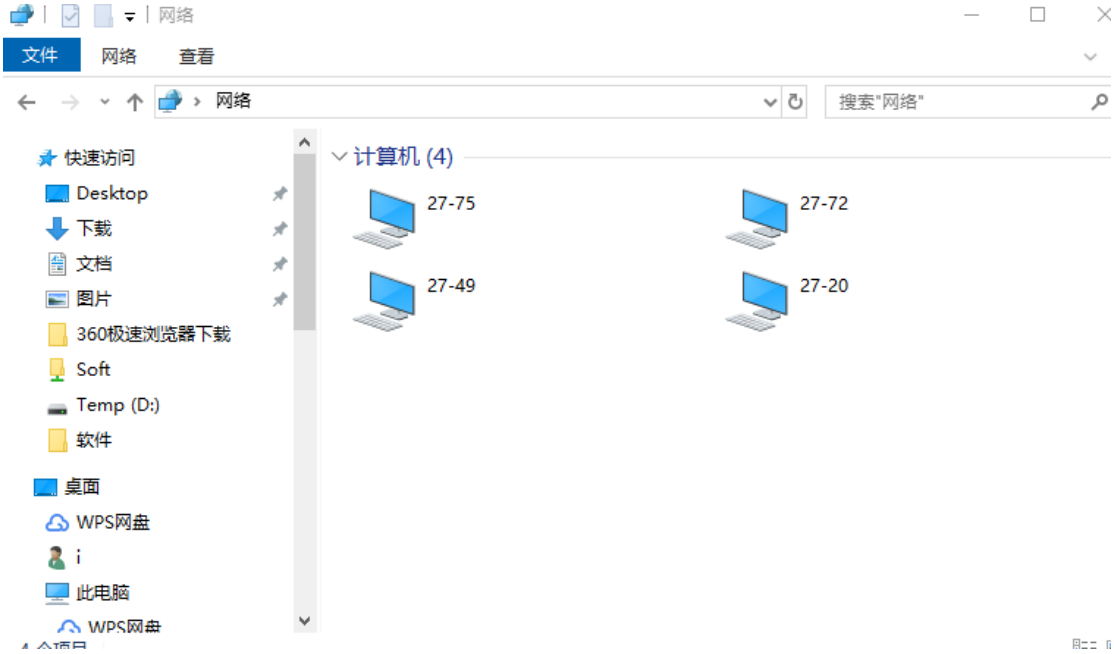
3.2.4 包分析

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）。

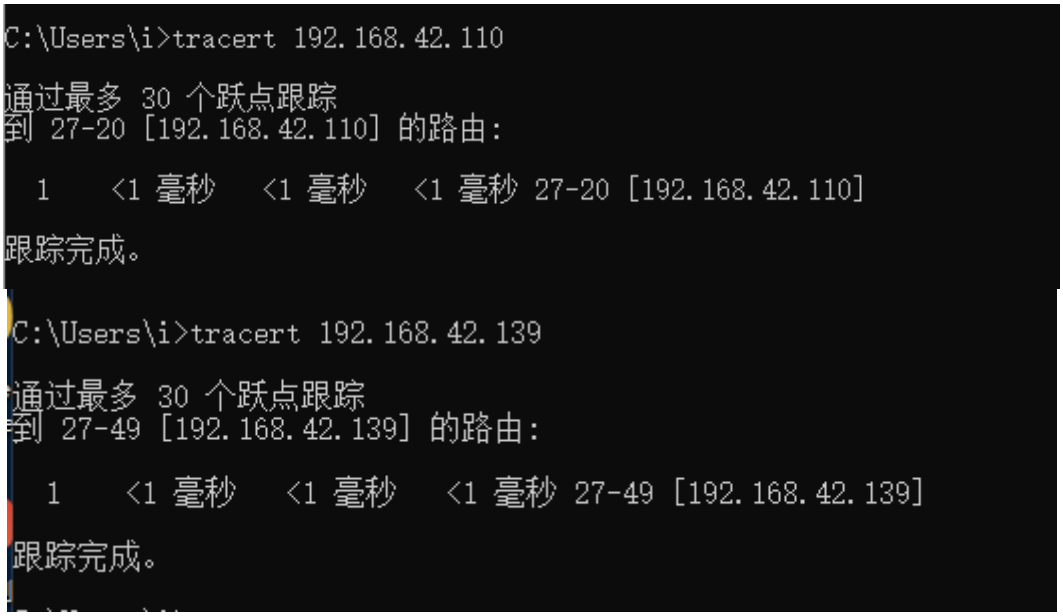
**实验报告内容：**

# 1 拓扑结构探测

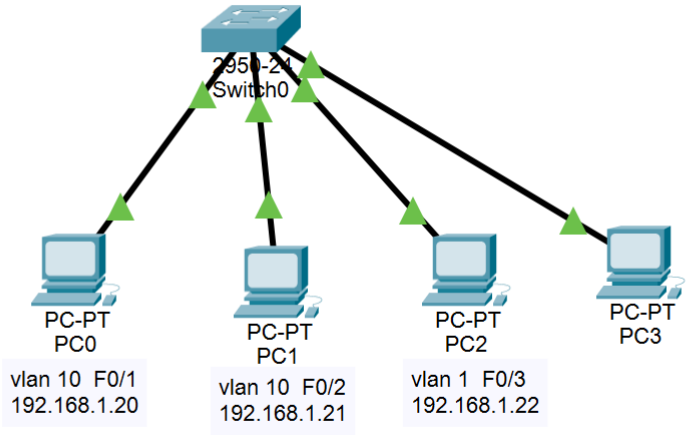
步骤一：进入计算机桌面，打开资源管理器，展开左侧“网络”。 从展开的网络目录树中，看到处在同一个网络内的相邻的主机数及其主机名，记录下同网的的这些主机。



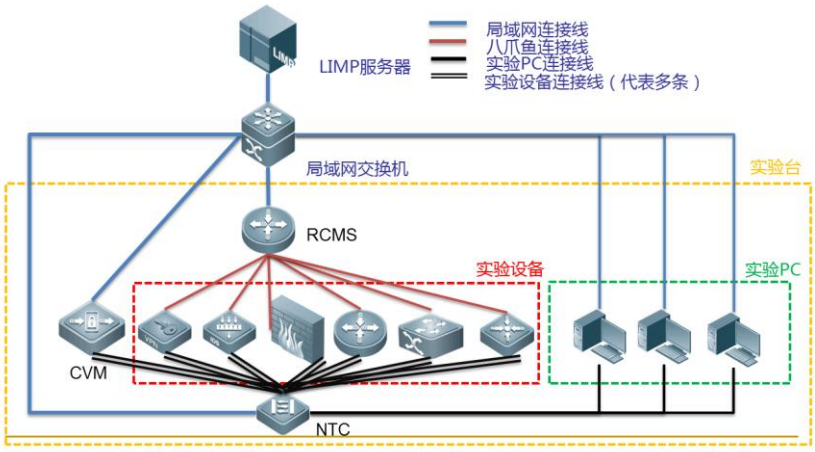

步骤二：使用快捷键 Win+R 打开运行，输入 cmd 打开命令提示符。用 tracert 命令，探测到达任一相邻主机的中间节点。记下通往所探测节点的中间节点数，给出本机到达探测主机的路径。对不同主机，重复此步，可给出本网内主机的拓扑结构。

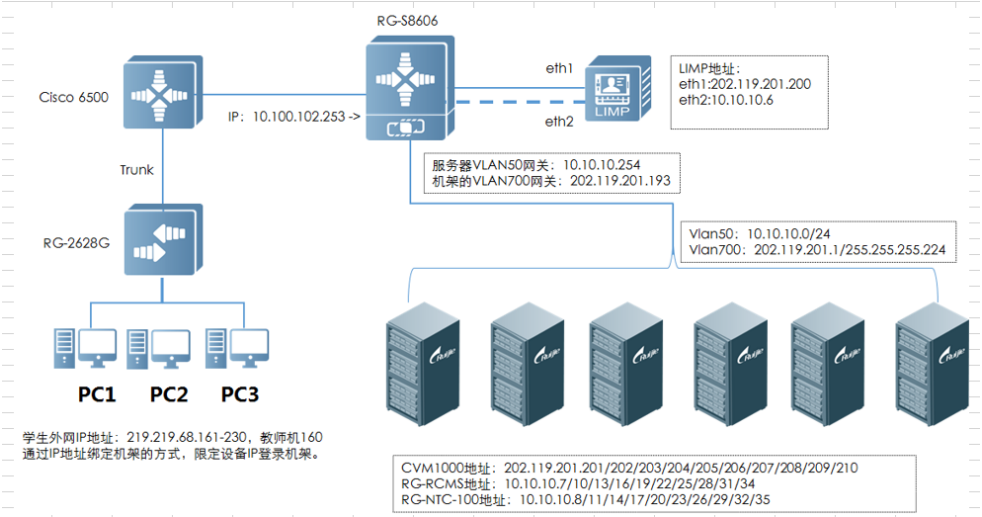



用 tracert 命令，探测到达任一相邻主机的中间节点，观察发现中间节点数均为 1。故下图为拓扑图。




- 中国矿业大学 锐捷网络实验室典型拓扑



# 2 实验用机接入校园网的拓扑结构：

## 2.1 测试校园网接入路径

进入 cmd ，用 tracert 命令，探测访问校园网 Web 服务器、DNS 服务器的路径，记录下从本机到达两个不同服务器的前面共同路径，即为本机接入校园网的路径。

```
C:\Users\lenovo>tracert www.cumt.edu.cn

通过最多 30 个跃点跟踪
到 www.cumt.edu.cn [202.119.200.206] 的路由:

  1     *       26 ms     *     10.3.255.254
  2     *        *        *     请求超时。
  3     *        *       6 ms   10.2.6.1
  4     7 ms     6 ms     5 ms   172.35.1.2
  5     *        *        *     请求超时。
  6     3 ms     2 ms     3 ms   202.119.200.206

跟踪完成。

C:\Users\lenovo>tracert DNS.cumt.edu.cn

通过最多 30 个跃点跟踪
到 DNS.cumt.edu.cn [202.119.200.10] 的路由:

  1     1 ms     1 ms     1 ms   10.3.255.254
  2     *       16 ms     3 ms   10.2.4.2
  3     6 ms     7 ms     4 ms   10.2.6.1
  4    10 ms    15 ms    20 ms   172.35.1.2
  5     *        *        *     请求超时。
  6     7 ms     4 ms     3 ms   dns.cumt.edu.cn [202.119.200.10]

跟踪完成。
```

## 2.2.测试互联网接入路径

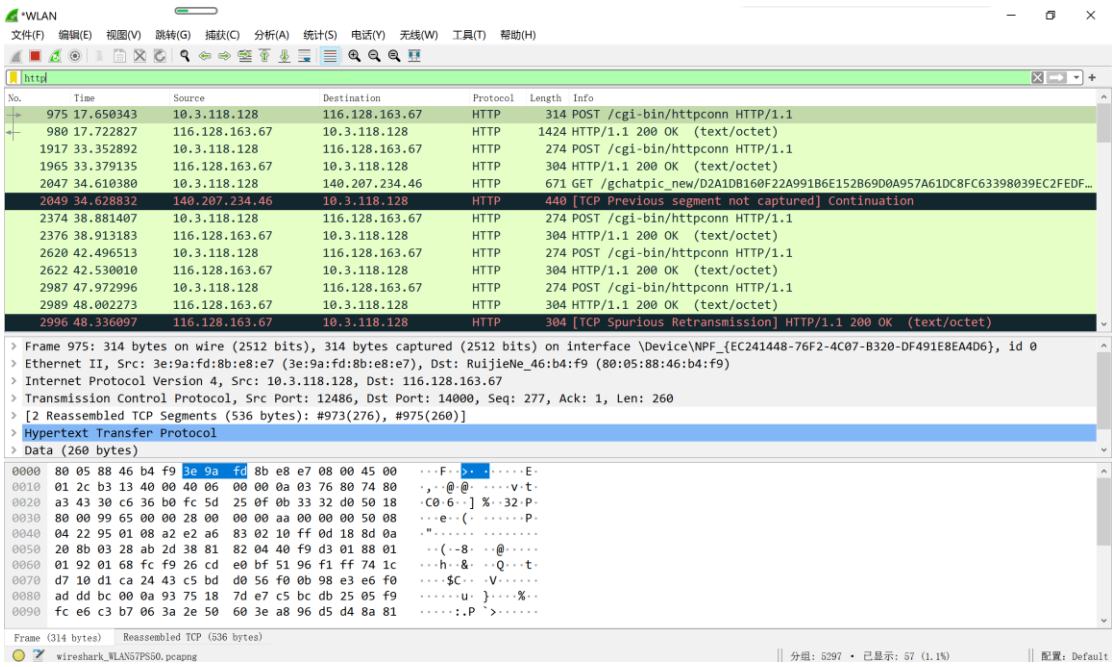
步骤四：进入 cmd ， 用 tracert 命令，反复探测到达互联网门户网站的中间节点，记录下这些节点，尤其记住前面几个节点。从而给出本机接入互联网的入网路径。

```
C:\Users\lenovo>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [112.80.248.75] 的路由:

  1     5 ms     4 ms    11 ms  10.3.255.254
  2     *        9 ms     5 ms  10.2.1.1
  3    14 ms     8 ms     9 ms  112.85.229.157
  4     7 ms     7 ms     5 ms  112.85.230.46
  5    16 ms    15 ms    15 ms  112.85.230.137
  6    21 ms    19 ms    18 ms  122.96.66.102
  7    23 ms    22 ms    20 ms  112.86.192.146
  8     *        *        *     请求超时。
  9    28 ms    22 ms    27 ms  112.80.248.75

跟踪完成。
```

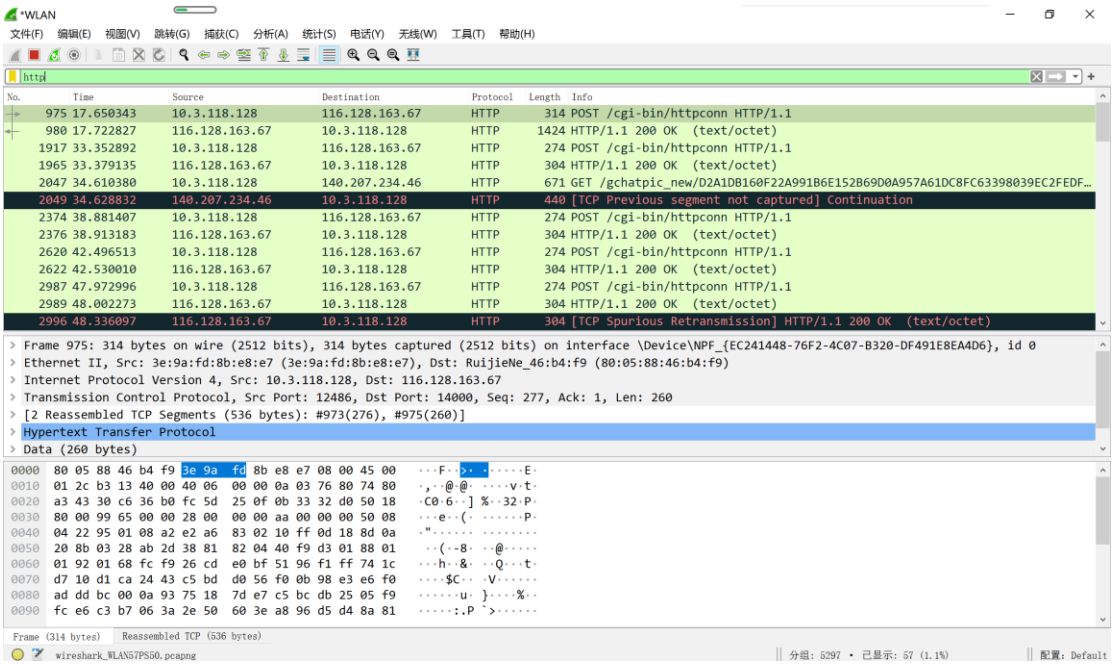
# 3.抓包过程

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

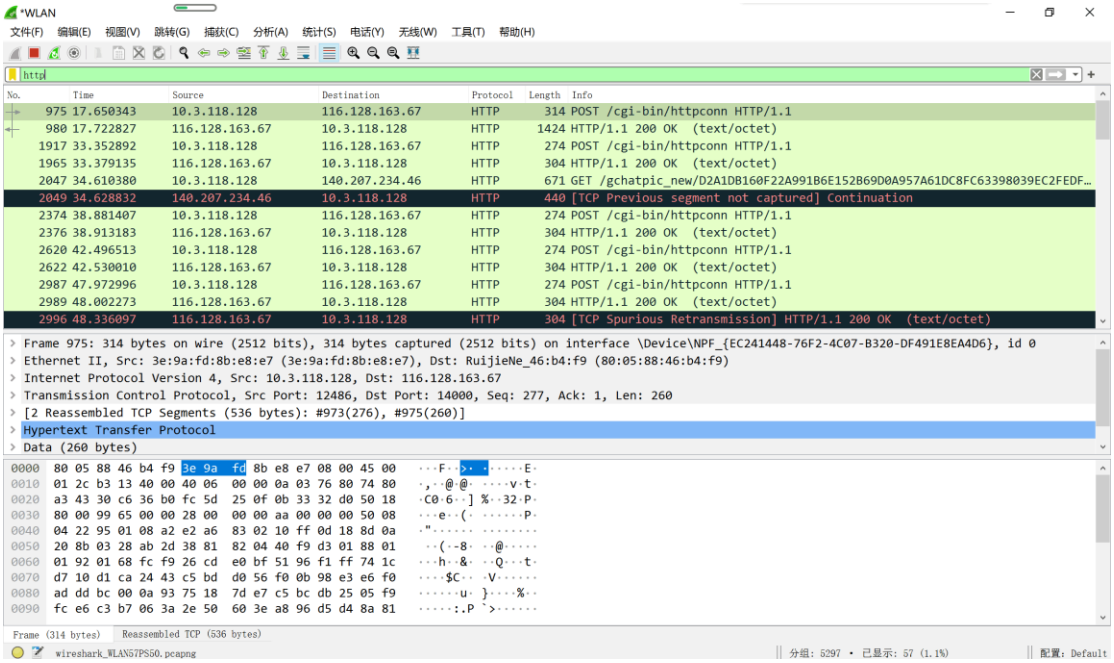
## 3.1.http 协议



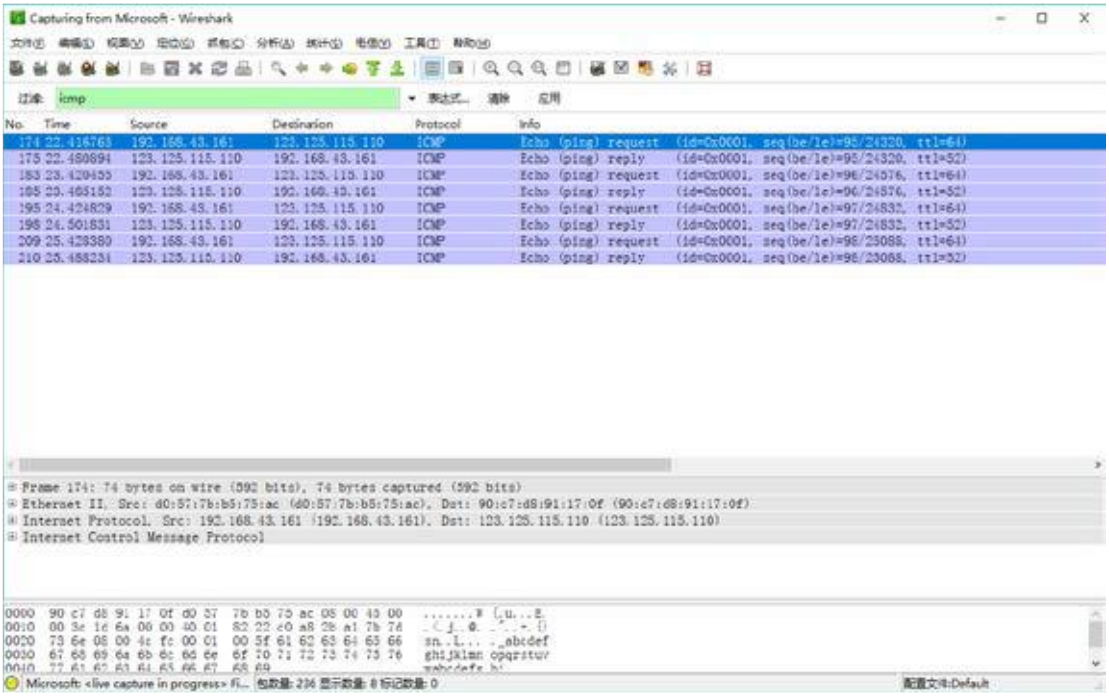
## 3.2.UDP 协议



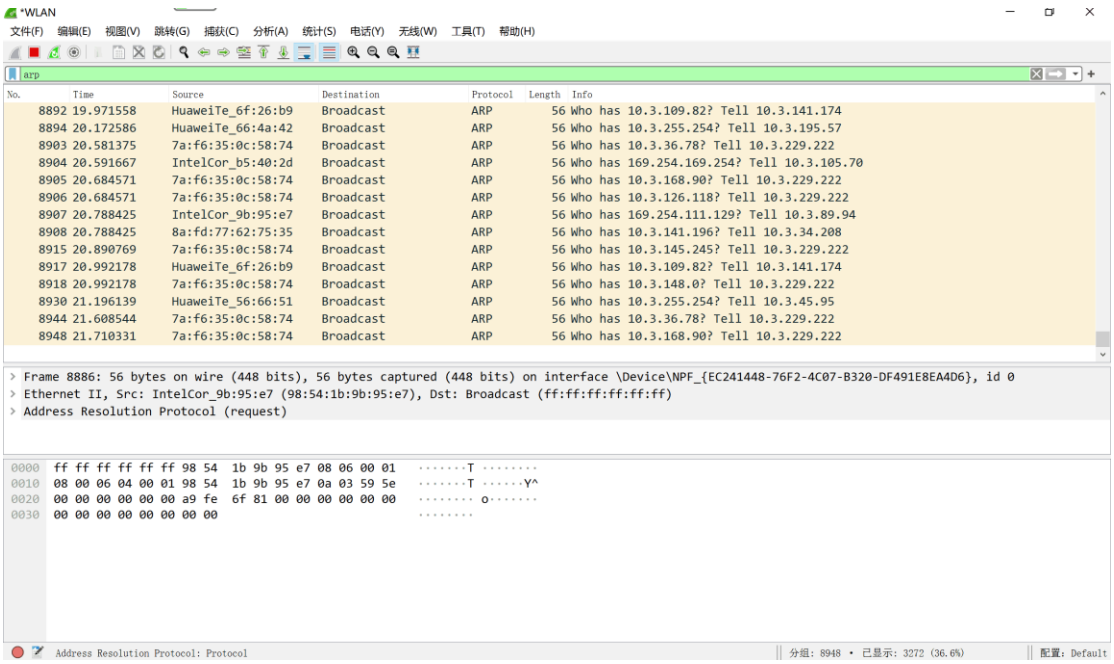

## 3.3.TCP 协议



## 3.4.ICMP 协议



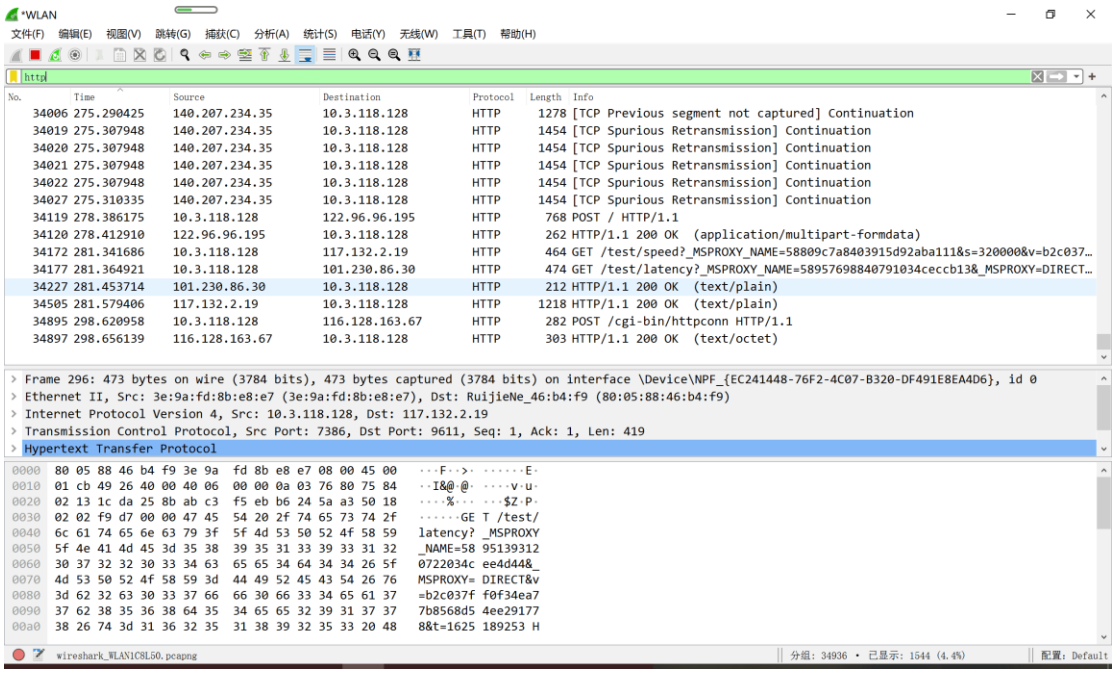

## 3.5.ARP 协议



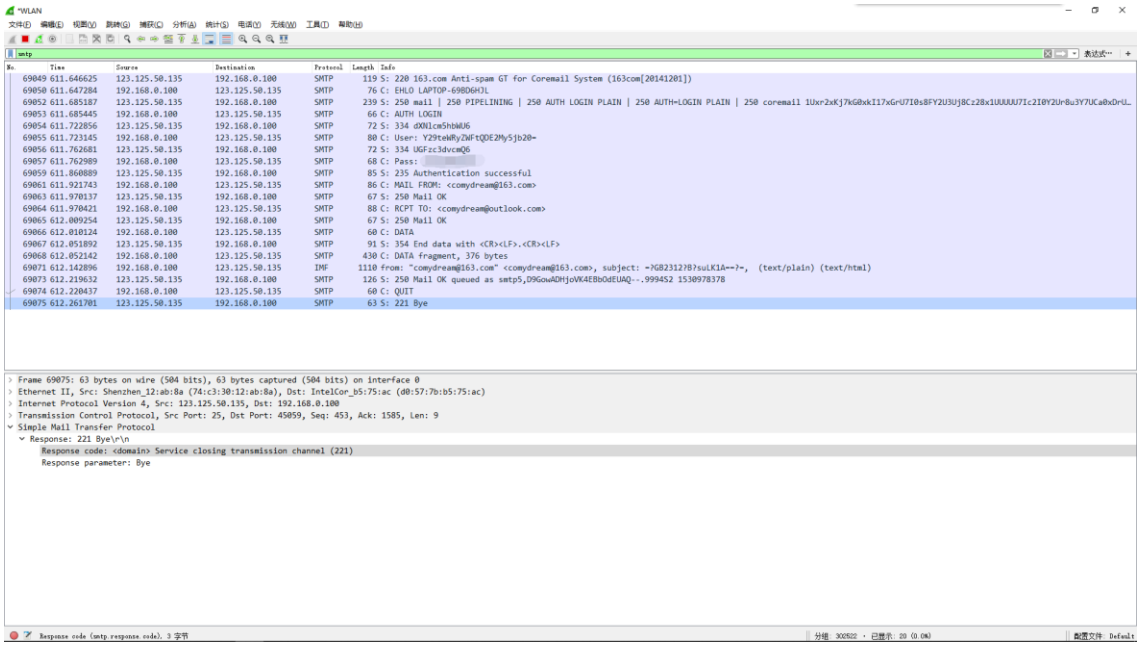

# 4.解析数据包

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。

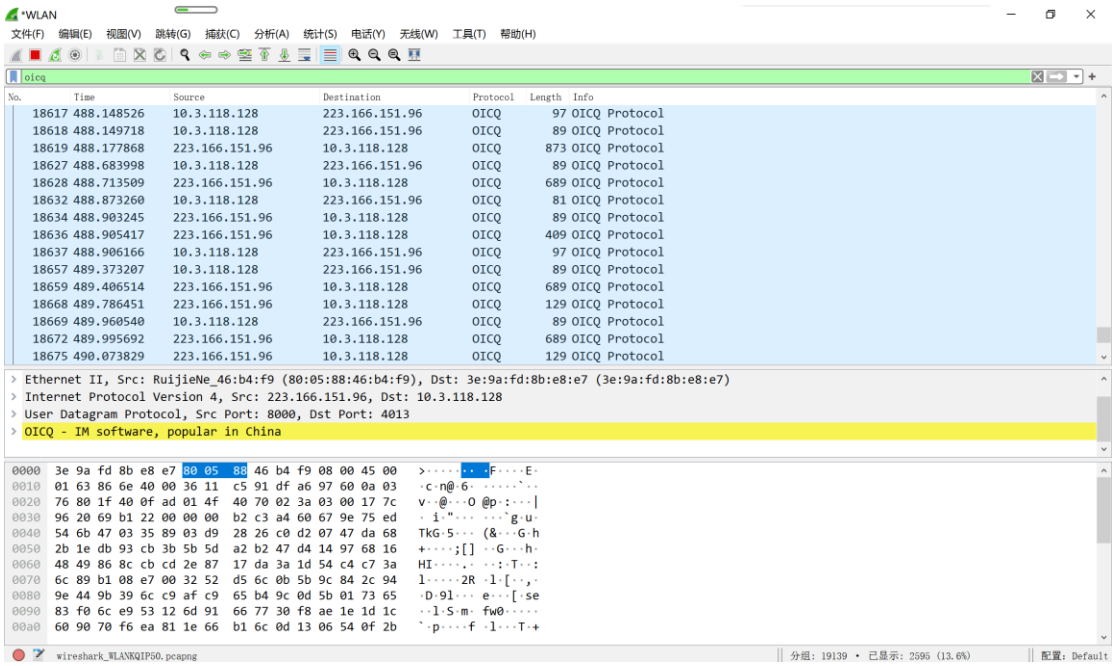
## 4.1.WWW 服务数据包:



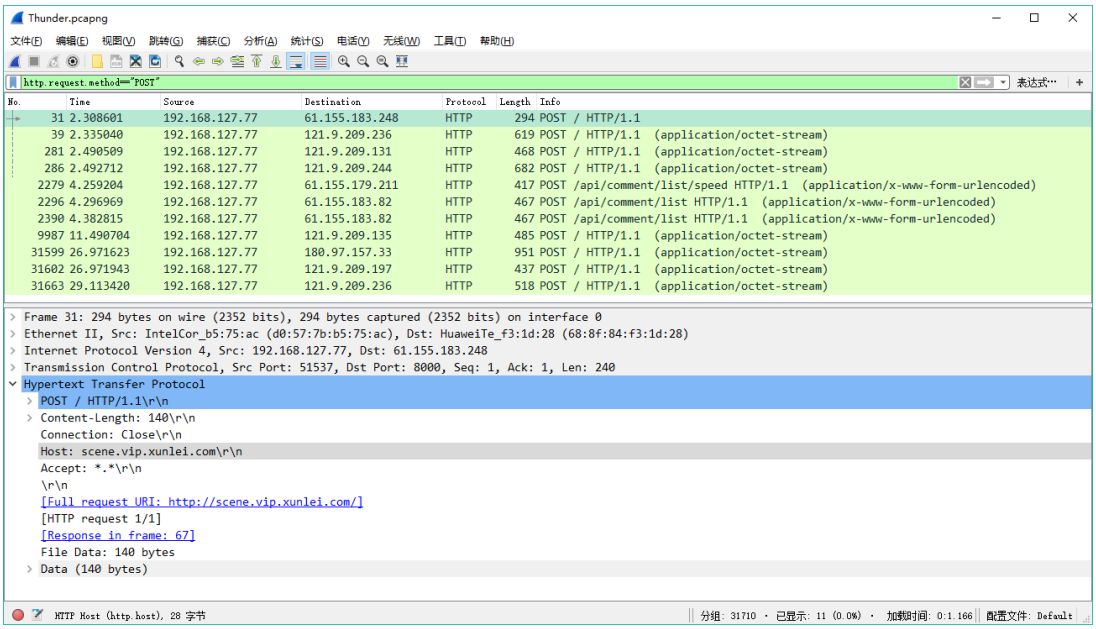

## 4.2.Email 服务数据包



## 4.3.QQ 通信数据包:

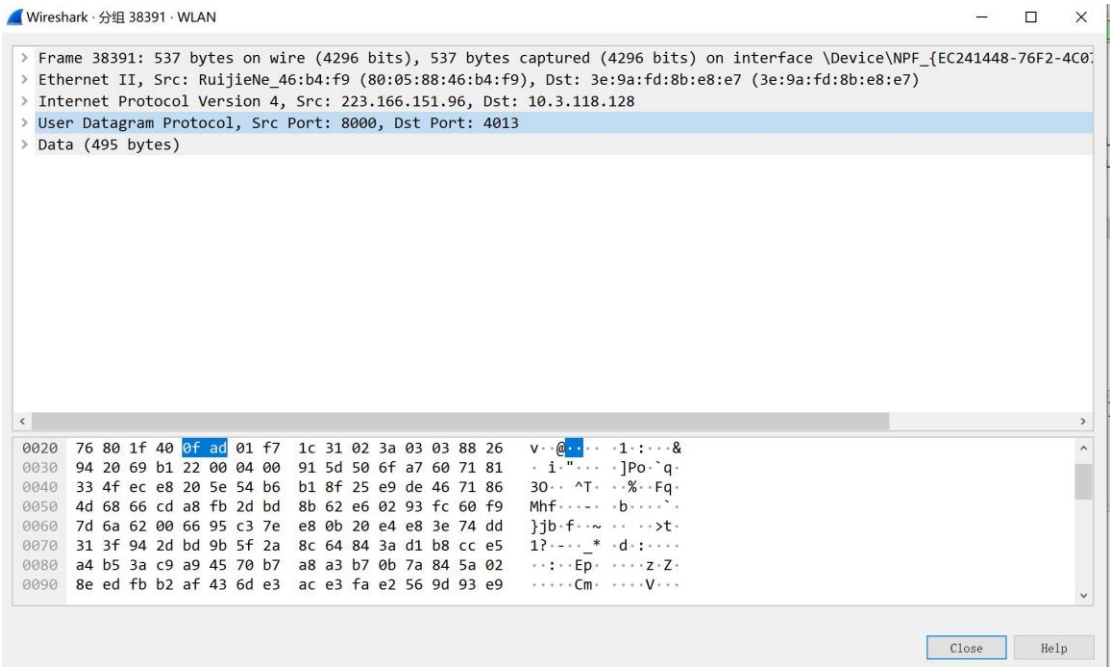



## 4.4. 迅雷文件下载服务数据包

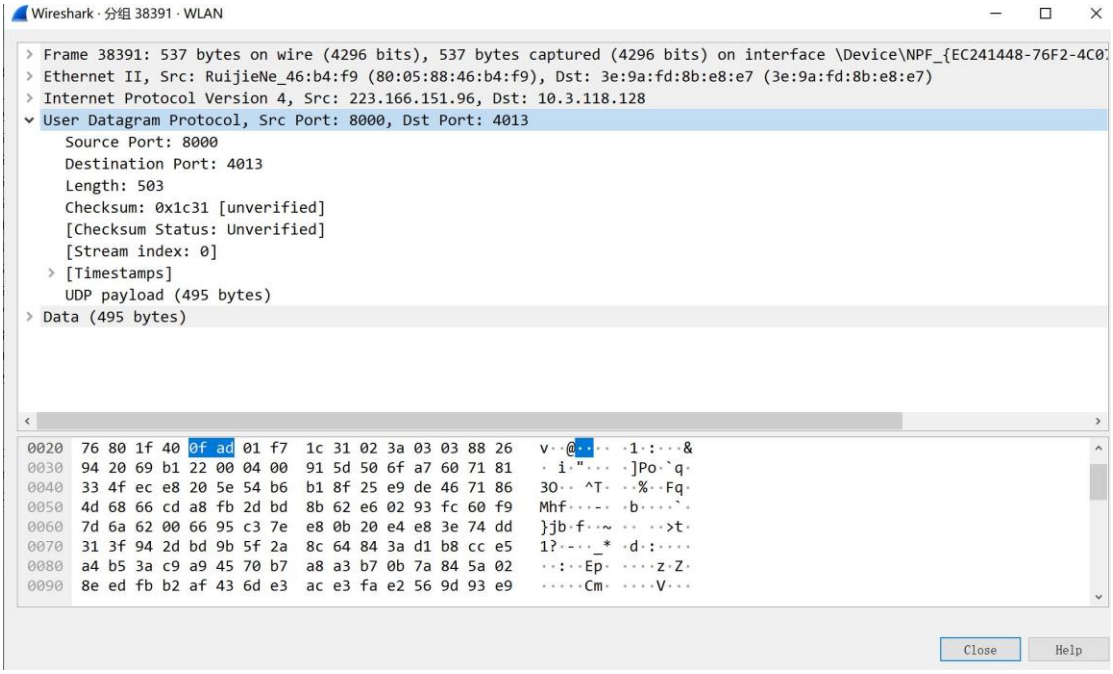


# 5.包分析

## 5.1UDP 数据包详细分析

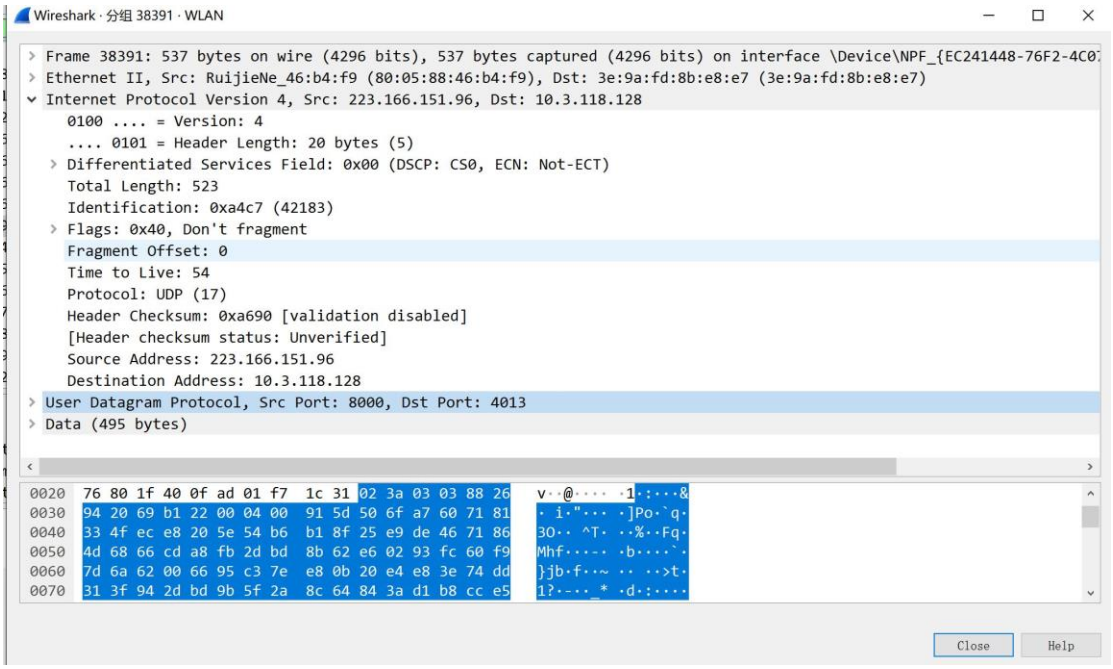



### 5.1.1.UDP 层



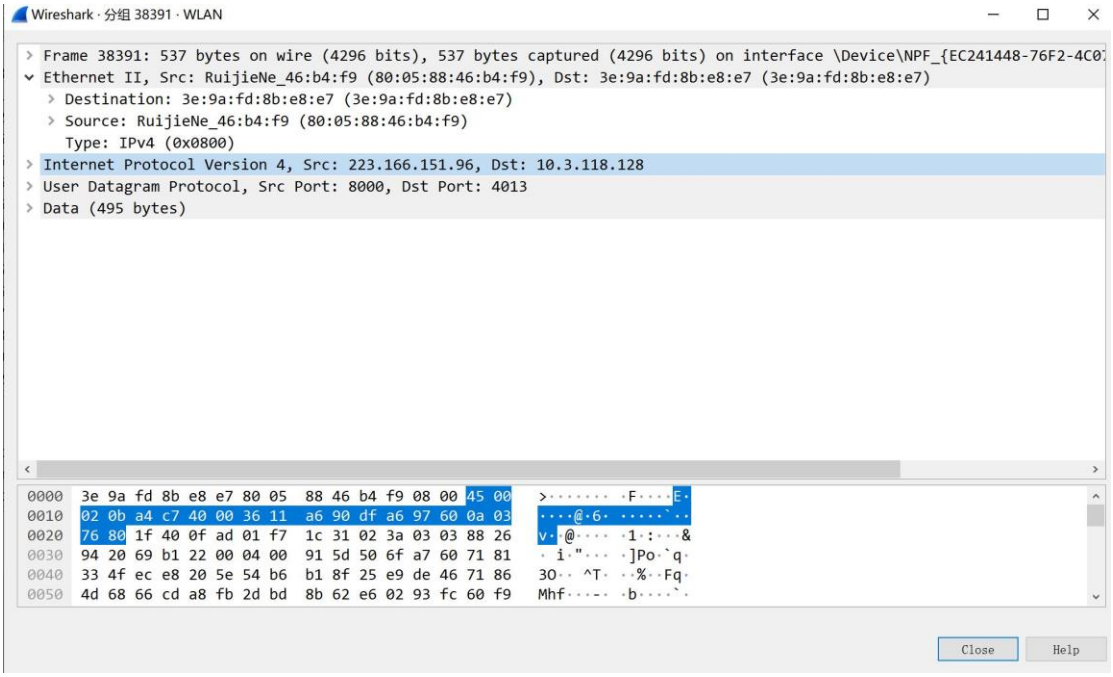

从 UDP 的报文格式可以得到 UDP 的首部信息，源端口为 8000，目的端口为 4013，UDP 长度为 503，检验和为 0x1c31

### 5.1.2.IP 层



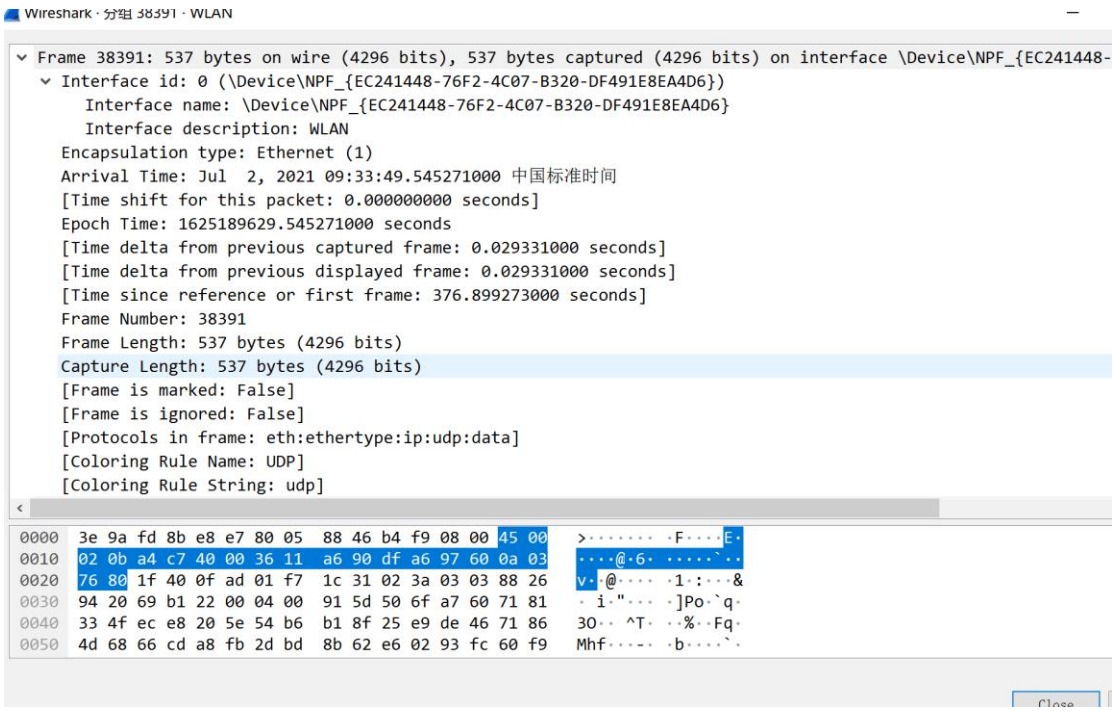

分析出他的首部信息，首部长为 20 字节，还有标识位 42183，5 位没有设置的标志位以及总长度偏移量，TTL 为 54，协议字段 17，代表了上层使用 UDP，下面就是源 IP 为 223.166.151.96，目的 IP 为 10.3.118.128

### 5.1.3.数据链路层




上层 IP 类型为 IPv4，源 MAC 地址: 80:05:88:46:b4:f9 目的 MAC 地址 3e:9a:fd:8b:e8:e7

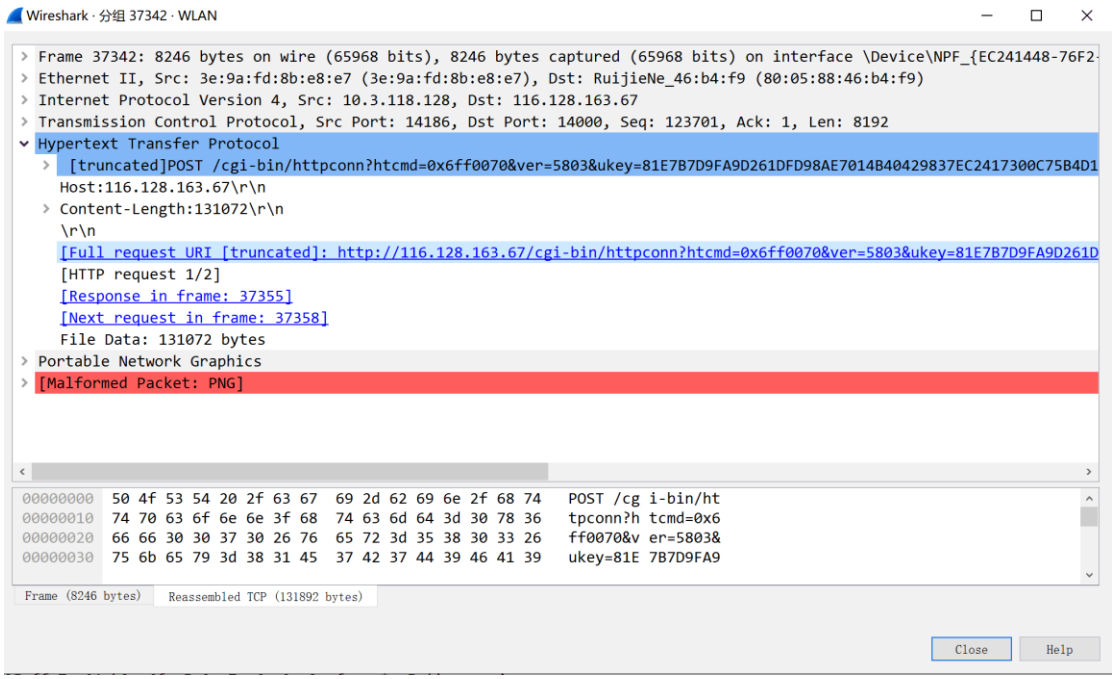
### 5.1.4.物理层

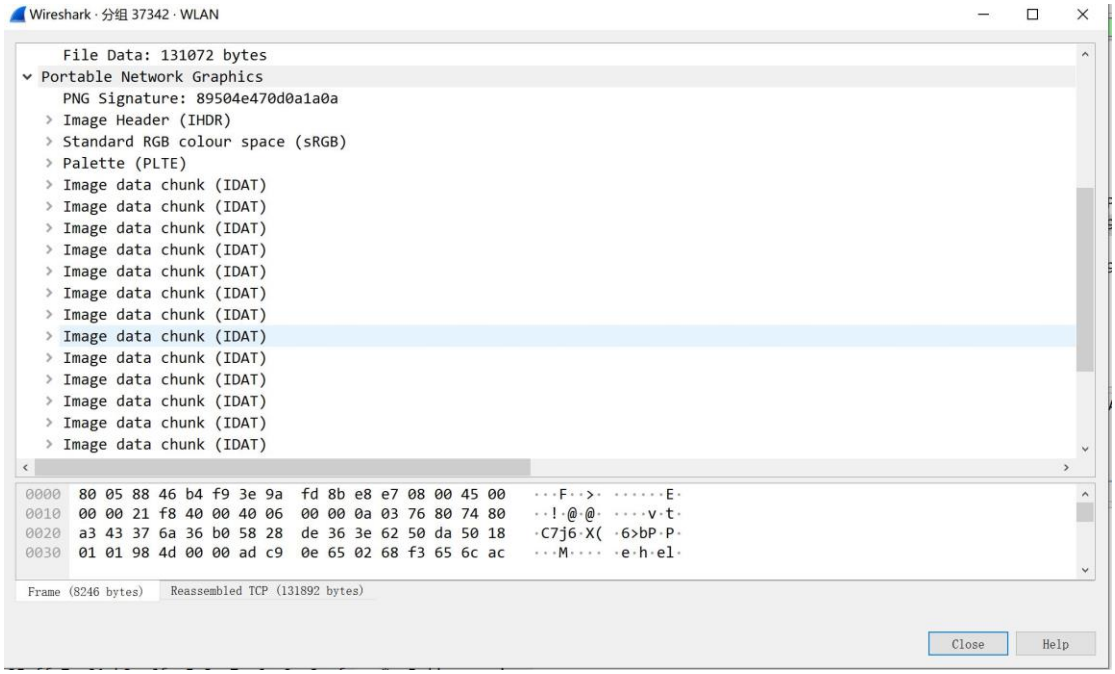



接口 id 为 0 捕获日期为： Jul 2,2021 09:33:49，帧序号为 38391，帧长度为 537 字节，捕获了 537 字节，帧内封装的协议层次结构：eth:ethertype:ip:udp:data

## 5.2.HTTP 数据包详细分析

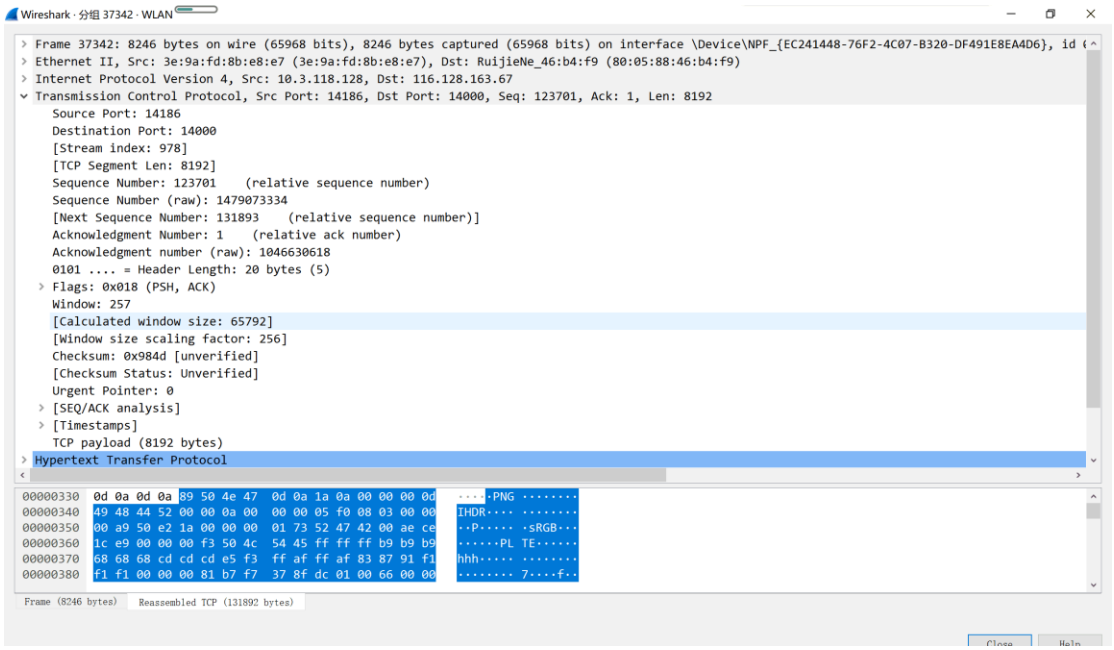
### 5.2.1.传输层





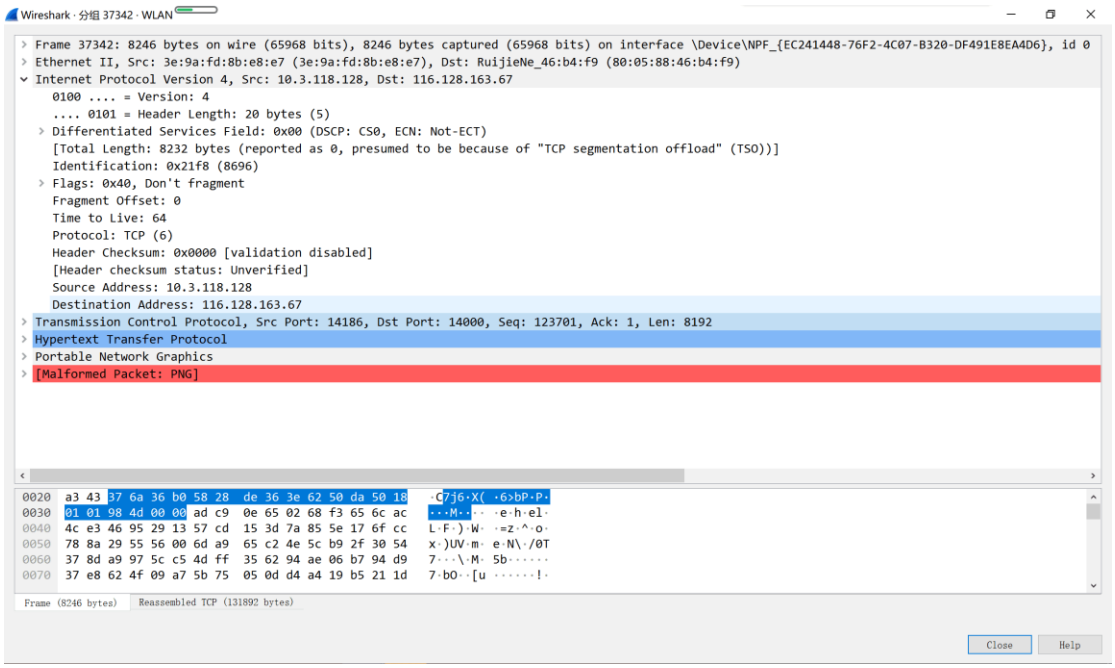

这一次应用层以 http 报文显示，里面传递的东西很明确，通过 GET 方式访问网站资源，访问的主机名为 suggestion.baidu.com,还有其他的一些浏览器相关的信息等等

## 5.2.2.TCP 层




可以看出 TCP 首部信息，我们也可以从另一个方面推出 http 协议使用的运输层协议是 TCP，源端口为 14186，目的端口为 14000，还有它的序号 131892 以及确认信号，还可以看到标志位 Flags：0x018，窗口大小:256，首部长度为 20，检验和是 0x8fd9，紧急指针 Urgent pointer 置 0

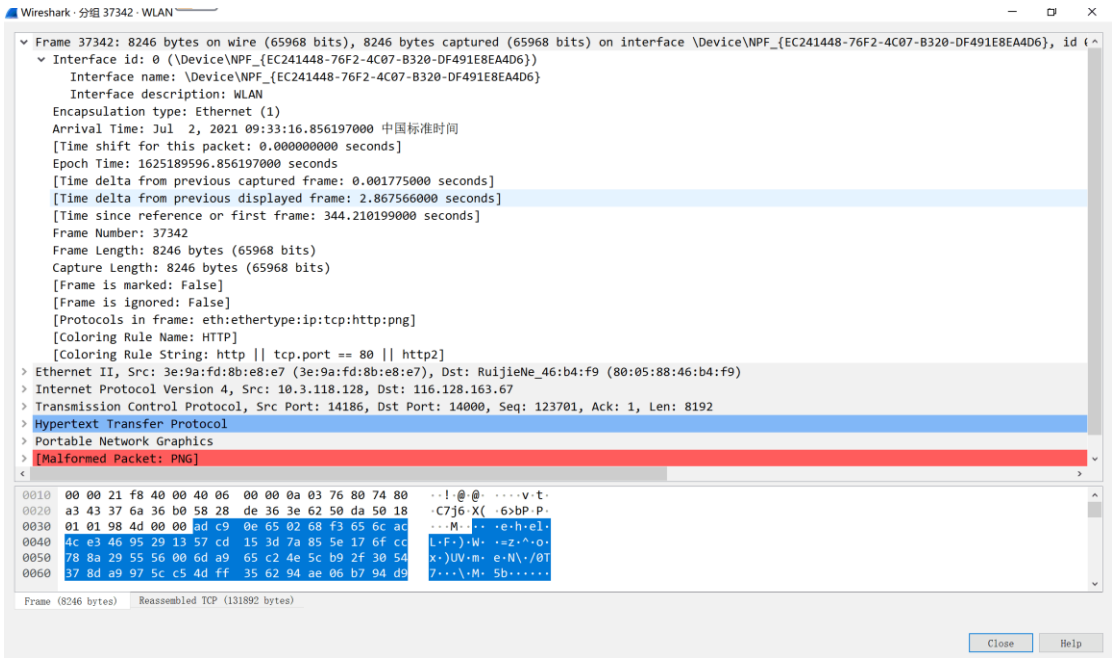
## 5.2.3.IP 层




IP 层的内容，可以清楚分析出他的首部信息，版本号为 4，首部长为 20 字节，还有标识 8696，

TTL 为 64，协议字段 6，代表了上层使用 TCP，下面就是源 IP 为 10.3.118.128，目的 IP 为 116.128.163.67

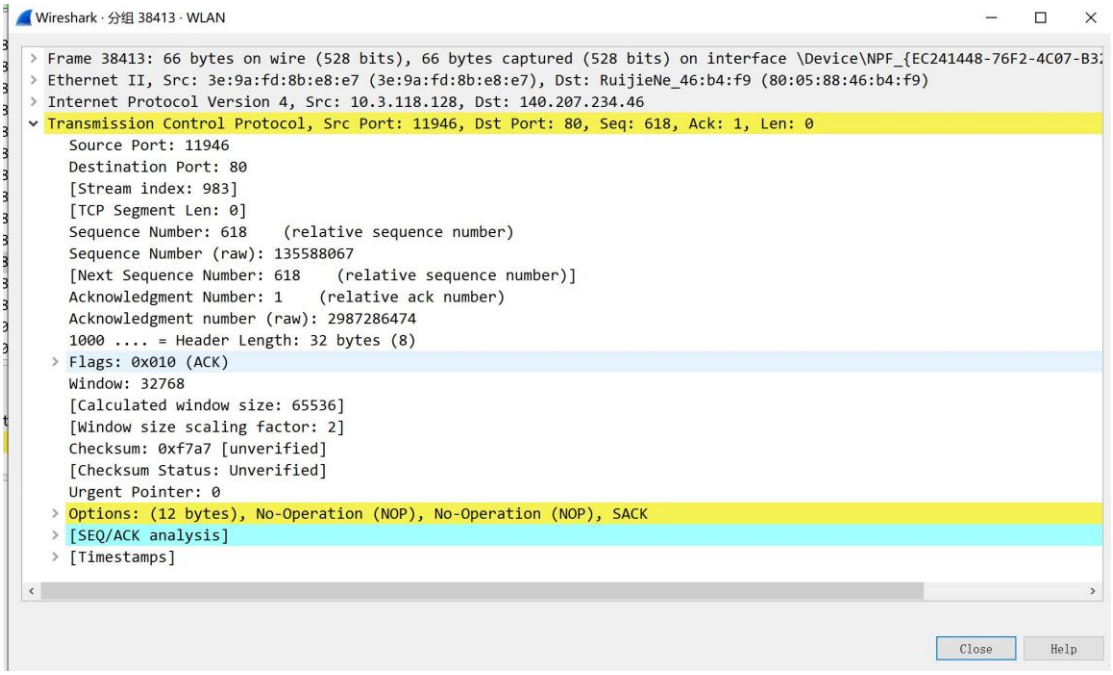
## 5.2.4.数据链路层




上层 IP 类型为 IPv4，源 MAC 地址: 3e:9a:fd:8b:e8:e7,目的 MAC 地址 80:05:88:46:b4:f9

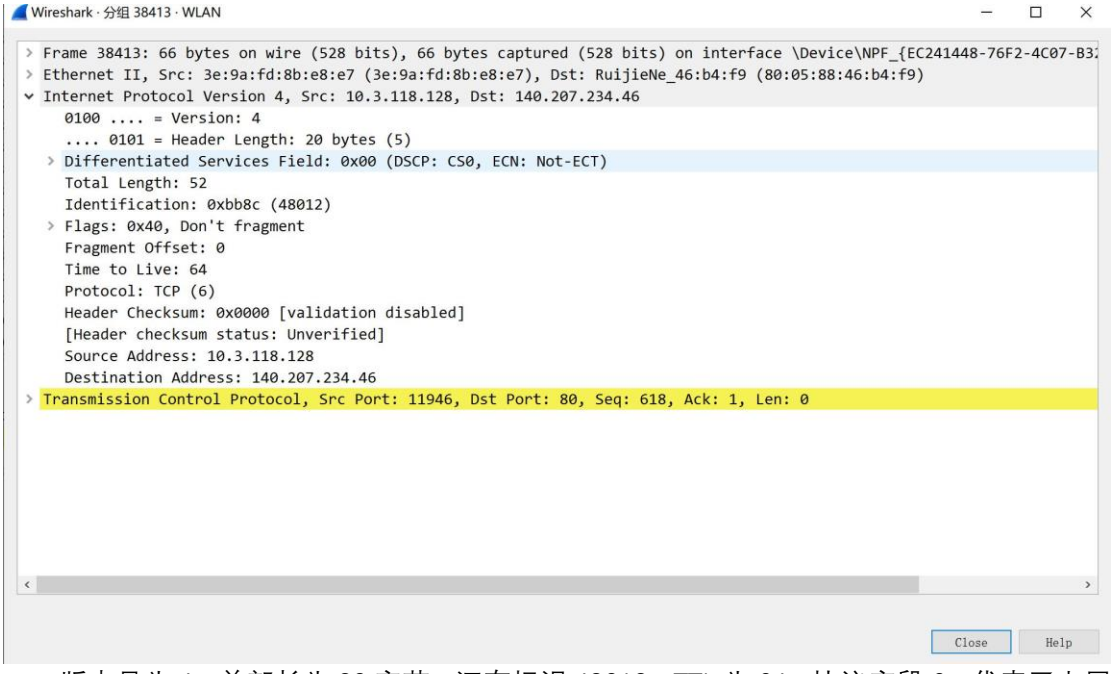
## 5.3.TCP 数据包详细分析

### 5.3.1.TCP 层



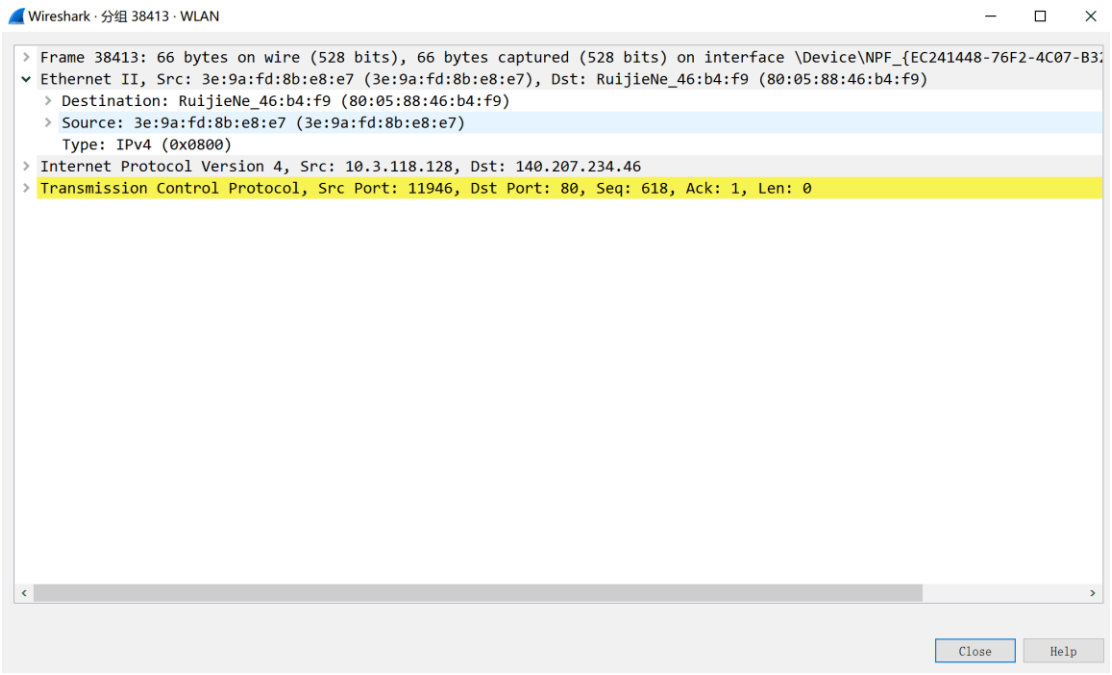

源端口为 11946，目的端口为 80，还有它的序号 0 以及确认信号 618，还可以看到标志位 Flags：0x010，窗口大小:65536，首部长度为 32，检验和是 0x1577，紧急指针 Urgent pointer 置 0

### 5.3.2.IP 层



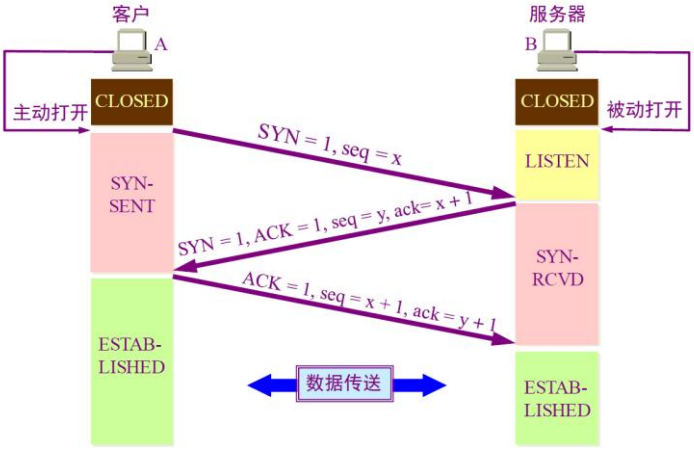

版本号为 4，首部长为 20 字节，还有标识 48012，TTL 为 64，协议字段 6，代表了上层使用 TCP，下面就是源 IP 为 10.3.118.128，目的 IP 为 140.207.234.46

### 5.3.3.数据链路层



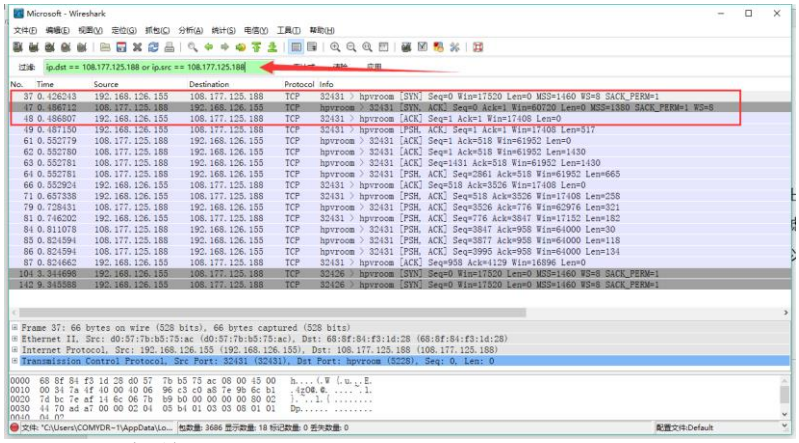

上层 IP 类型为 IPv4，源 MAC 地址: 3 e:9a:fd:8b:e8:e7,目的 MAC 地址 80:05:88:46:b4:f9

# 6.Transmission Control Protocol 连接建立三报文握手



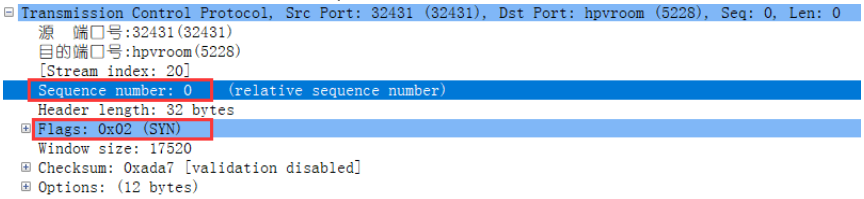

用三报文握手建立 TCP 连接示意图

打开 Wireshark，选取网卡开始抓包。先在过滤填写 tcp，表示过滤出 TCP 协议的包，任取一个，例如本机与 108.177.125.188 的连接，则在过滤填写 ip.dst == 108.177.125.188 or ip.src == 108.177.125.188，这样，就可以过滤出（本机→108.177.125.188）或（108.177.125.188→本机）的包;

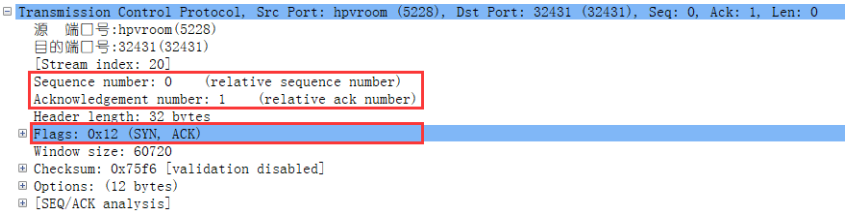


结合课程学习，可知前 3 个包为“三报文握手”，过程如下：

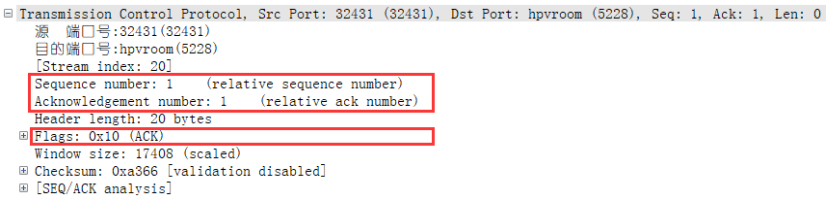
第一个 TCP 报文：客户端（本机）向服务器（108.177.125.188）发送连接请求包，标志位 SYN（同步序号）置为 1，序号 seq = x = 0；



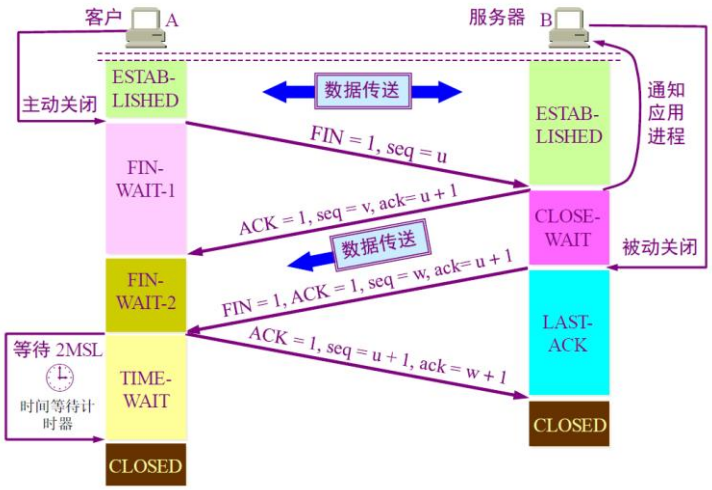

第二个 TCP 报文：服务器收到客户端发过来报文，由 SYN=1 知道客户端要求建立联机。向客户端发送一个 SYN 和 ACK 都置为 1 的 TCP 报文，设置序号 seq=y=0，将确认号 ack 设置为客户端第一个 TCP 报文的序列号加 1，即 ack = x+1 = 0+1 = 1；




第三个 TCP 报文：客户端收到服务器发来的包后检查确认号 ack 是否正确，即第一次发送的序号加 1（x + 1 = 1）以及确认标志位 ACK 是否为 1，若正确，服务器再次发送确认包，ACK 标志位为 1，SYN 标志位为 0。确认号 ack = y+1 = 0+1 = 1，序号 seq = x+1 = 1。连接建立成功，可以传送数据了；

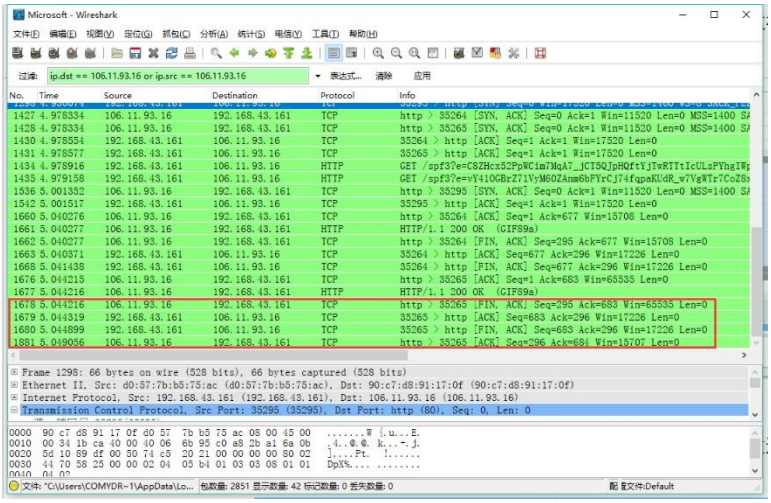


# 7.Transmission Control Protocol 连接释放四报文握手




用四报文握手释放 TCP 连接示意图

TCP 断开连接时，有四报文握手过程，如下图所示，Wireshark 截获到了四报文握手的四个数据包；




四报文握手过程如下：

- 第一个 TCP 报文：106.11.93.16 向本机发送连接释放请求，标志位 FIN 置为 1，序号 seq = u =295；
- 第二个 TCP 报文：本机收到 FIN 报文后，发回一个 ACK 报文，序号 seq = v = 683，确认号 ack =u+1=296；
- 第三个 TCP 报文：本机关闭与 106.11.93.16 的链接，发送一个 FIN，序号 seq = v =683，确认号 ack =u+1=296；
- 第四个 TCP 报文：106.11.93.16 收到本机 FIN 之后，发回 ACK，序号 seq = u+1 = 296，ack = v+1 = 684，连接释放。

**实验体会：**

通过本次实验，我对 Wireshark 软件的基本操作、过滤器填写、追踪流有了更深入的了解；对 IP、 UDP、TCP、HTTP 等协议的首部有了更好的掌握；对 TCP 协议连接建立、数据传送、连接释放过程有了直观的了解。

通过 Wireshark，结合网络上的资料，我对 TCP 协议连接建立（三报文握手）和连接释放（四报文握手）过程有了更直观的认识。在抓包过程中，我遇到了很多问题，例如包的真正到达时间不是严格和 seq 顺序一致，还和网络环境等复杂因素有关系，由此有课本上的“超时重传”、“确认丢失”、“确认迟到”等问题

Wireshark 真的是一款非常强大的抓包工具，，其功能是撷取网络封包，并尽可显示出最为详细的资料 Wireshark 使用 WinPCAP 作为接口，直与网卡进行数据报文交换。它的很多功能我在本次实验中还没有用到，在将来，我会更深入地去学习和了解这些网络分析用的工具软件，提高网络分析、网络安全的能力。