计算机科学与工程学院实验报告（首页）

课程名称 计算机网络 班级 17 软 2

实验名称 网络层、数据链路层数据包分析 指导教师 李慧

姓名 陈庆辉 学号 1714080902201 日期 2020 年 5 月 22 日

一、实验目的

1. 分析并熟悉数据链路层中以太网封装的格式；
2. 分析并熟悉网络层中 IP 数据报首部格式。
3. 熟悉 UDP 用户数据报首部格式，并掌握计算验证首部检验和的步骤；
4. 熟悉 TCP 报文段首部格式以及三次握手过程。

二、实验设备与环境

win10，Wireshark

三、实验内容及结果

1. 实验内容

使用 Wireshark 软件捕获任意 UDP 数据报并分析数据链路层中以太网封装的格式；

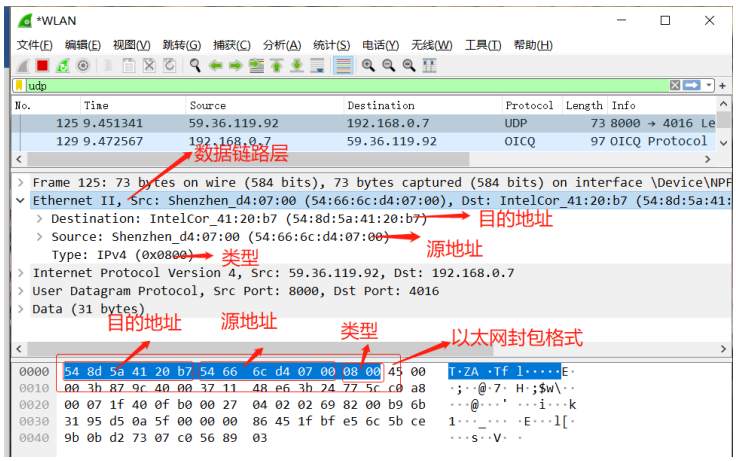
使用 Wireshark 软件捕获任意 UDP 数据报并分析网络层中 IP 数据报的首部格式；

使用 Wireshark 软件分析 UDP 用户数据报首部格式，并通过计算验证 UDP 首部检验和。

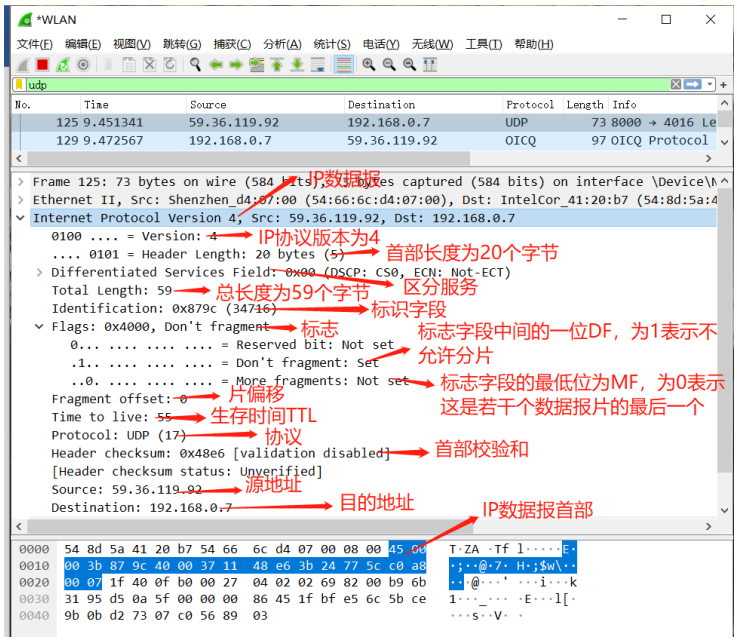
使用 Wireshark 软件分析 TCP 报文段首部格式，并通过捕获 FTP://172.17.21.223 与客户机的通信数据分析 TCP 连接的三次握手过程，找出其中 SYN、ACK 等标志位，seq，ack 字段的信息。

2. 分析

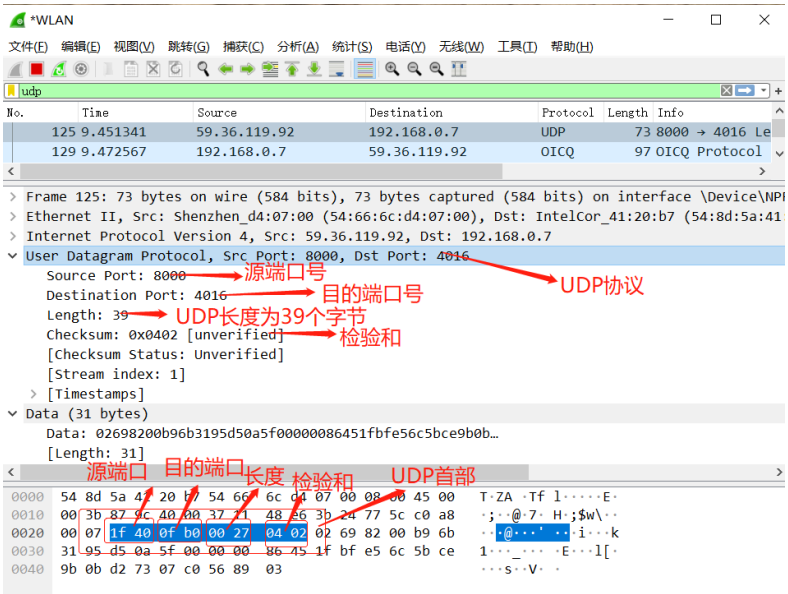
利用 wireshark 进行抓包，找到任意 UDP 数据报，对于数据链路层以太网封装的格式分析如下：



利用 wireshark 进行抓包，找到任意 UDP 数据报，对于网络层 IP 数据报的首部格式分析如下：



使用 Wireshark 进行抓包，找到任意 UDP 数据报，分析如下：



蓝色选中部分正好 8 个字节，分别对应上 UDP 首部的解释。剩下的为数据部分。

检验和为 0402，计算验证 UDP 首部和过程如下：

3b24（伪首部：源 IP 地址的前 2 个字节）

+775c（伪首部：源 IP 地址的后 2 个字节）

=b280

+c0a8（伪首部：目的 IP 地址的前 2 个字节）

=17328 → 7329 （进位）

+0007（伪首部：目的 IP 地址的后 2 个字节）

=7330

+0011（伪首部：固定部分）

=7341

+0027（伪首部：UDP 长度）

=7368

+1f40（UDP 用户数据报源端口号）

=92a8

+0fb0（UDP 用户数据报目的端口号）

=a258

+0027（UDP 长度）

=a27f

+0000（检验和，计算前填入全 0）

+0269 → UDP 报文的数据部分

=a4e8

+8200 →UDP 报文的数据部分

=126e8 → 26e9

+ ……（UDP 报文的数据部分）

+0300

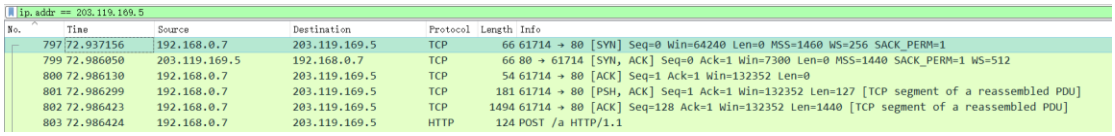
=fbfd → 和

求反码：

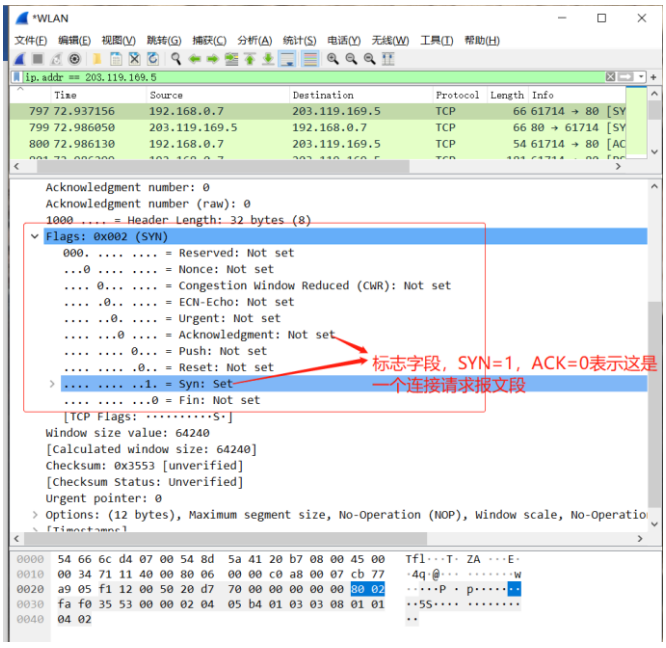
ffff-fbfd=0402 → 计算结果与所示的一致，验证正确。

使用 Wireshark 进行抓包，找到任意 TCP 报文段，分析如下：

无法访问 FTP://172.17.21.223，故捕获其他地址的三次握手过程进行分析：



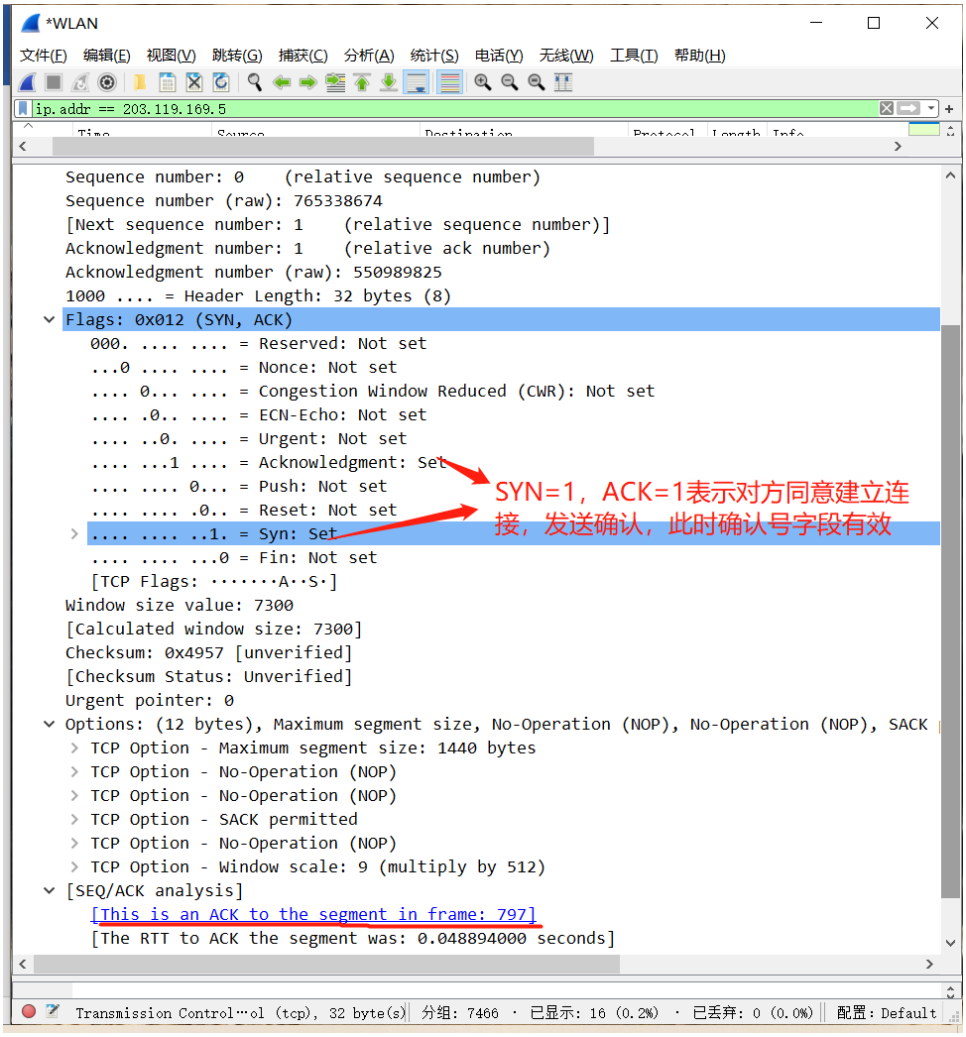
第一次握手：



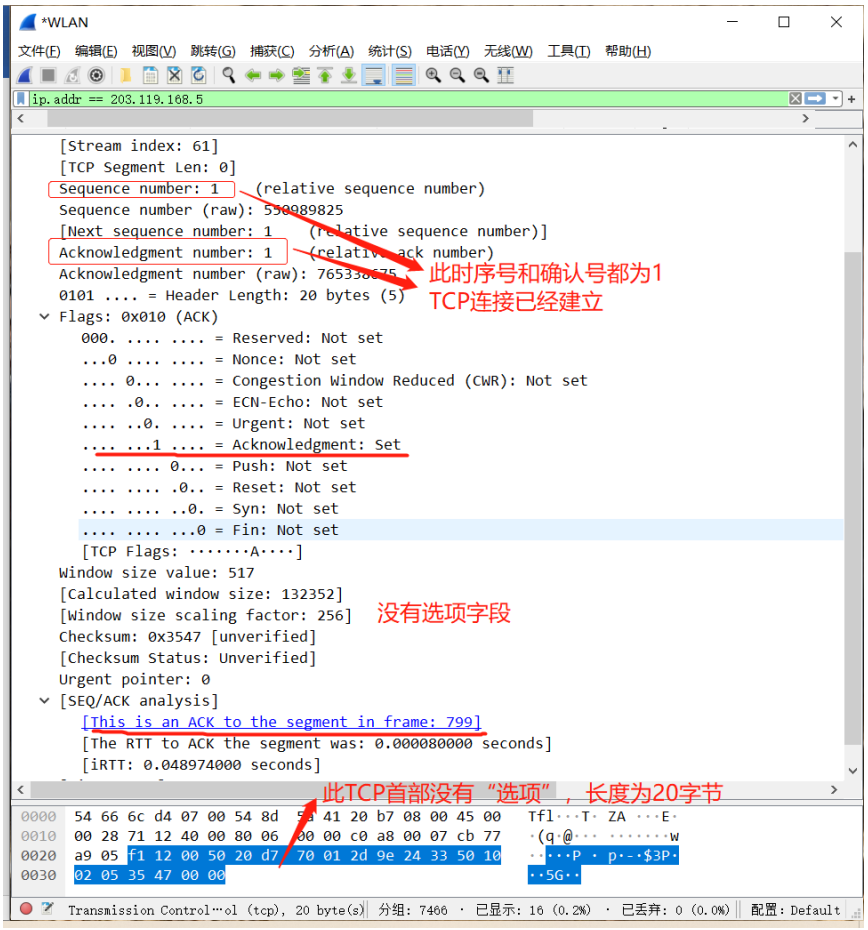
```
[Calculated window size: 64240]
Checksum: 0x3553 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operatio
  TCP Option - Maximum segment size: 1460 bytes
      Kind: Maximum Segment Size (2)
      Length: 4
      MSS Value: 1460
  TCP Option - No-Operation (NOP)
  TCP Option - Window scale: 8 (multiply by 256)
      Kind: Window Scale (3)
      Length: 3
      Shift count: 8
      [Multiplier: 256]
  TCP Option - No-Operation (NOP)
  TCP Option - No-Operation (NOP)
  TCP Option - SACK permitted
      Kind: SACK Permitted (4)
      Length: 2
  [Timestamps]
```

最大报文段长度MSS为1460个字节

第二次握手：



第三次握手：



四、结论与体会

这次实验做的时间有点长，主要是卡在了 UDP 首部检验和的计算上。该计算过程较为繁琐，一开始是采用二进制进行运算，但是算着算着就忘了算到哪里了。然后改成 16 进制进行计算，虽然好算了点，但数据部分多的话还是很容易出错的。前两次选的数据部分过长，老是有些地方漏算或者错算。最后挑了个短的来算才最终算出正确的结果。