广州大学学生实验报告

**开课学院及实验室：****计算机科学与工程实验室518 2019年11月13日**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **学院** | 计算机科学与教育软件学院 | **年级/专业/班** | 软件 171 | **姓名** | 谢金宏 | **学号** | 1706300001 |
| **实验课程名称** | 计算机网络实验 | | | | | **成绩** |  |
| **实验项目名称** | 使用网络协议分析器捕捉和分析协议数据包 | | | | | **指导老师** | 唐琳 |

## 实验目的

1. 熟悉一种网络协议分析器（Wireshark或Ethereal，后者为前者的前身）的使用。
2. 验证各种协议数据包的格式。
3. 学会捕捉并分析各种数据包。

## 实验环境

1. 安装有TCP/IP协议的Windows计算机。
2. 安装有Wireshark或Ethereal网络协议

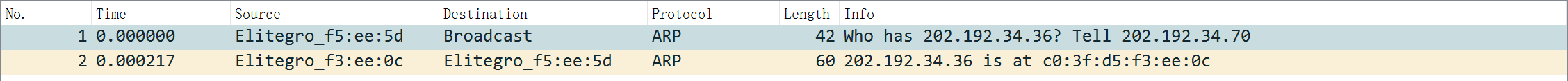
## 实验内容

1. 安装网络协议分析器。
2. 捕捉数据包，验证数据帧、IP数据报、TCP数据段的报文格式。
3. 捕捉并分析ARP报文。
4. 捕捉ping过程中的ICMP报文， 分析结果各参数的意义。
5. 捕捉tracert过程中的ICMP报文，分析跟踪的路由器IP是哪个接口的。
6. 捕捉并分析TCP三次握手建立连接的过程。
7. 捕捉整个FTP工作过程的协议包。对协议包进行分析说明。
   1. 地址解析ARP协议执行过程
   2. FTP控制连接建立过程
   3. FTP 用户登录身份验证过程
   4. FTP 数据连接建立过程
   5. FTP数据传输过程
   6. FTP连接释放过程（包括数据连接和控制连接）
8. 捕捉及研究WWW应用的协议报文，回答以下问题：
   1. 当访问某个网页时，从应用层到网络层，用到了哪些协议？
   2. 对于用户请求的百度主页（www.baidu.com），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？
   3. 两个存放在同一个服务器中的截然不同的Web页（例如， http://www.gzhu.edu.cn/index.jsp和http://www.gzhu.edu.cn/cn/research/index.jsp可以在同一个持久的连接上发送吗？
   4. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？
   5. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif图像和两个远地.gif图像，那么需要建立几次TCP连接和有几个UDP过程？

## 实验步骤、记录和结果

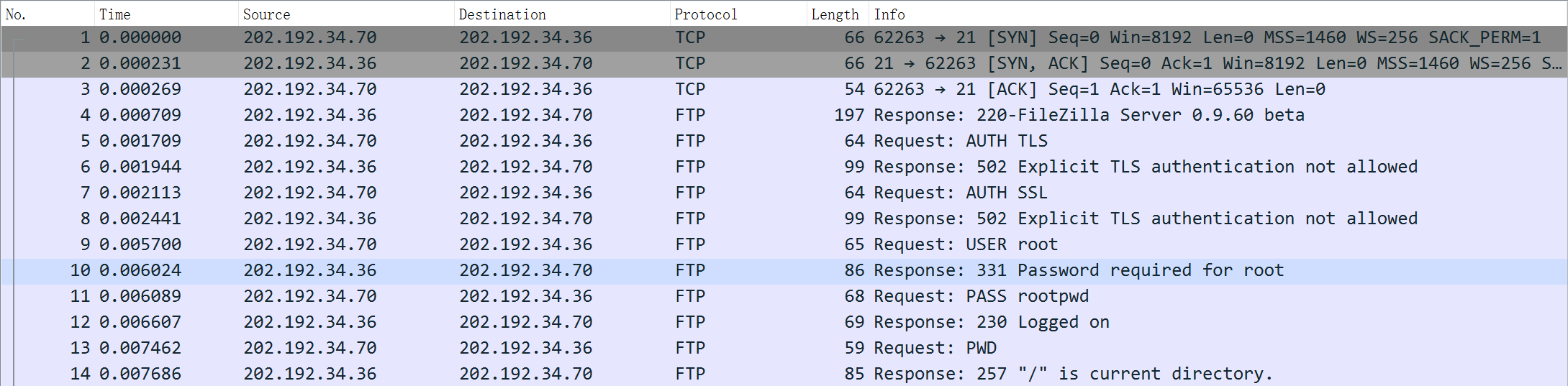
实验中FTP服务端的IP地址为202.192.34.70，FTP客户端的IP地址为202.192.34.36。捕捉FTP工作过程的协议包：

1. 地址解析ARP协议执行过程



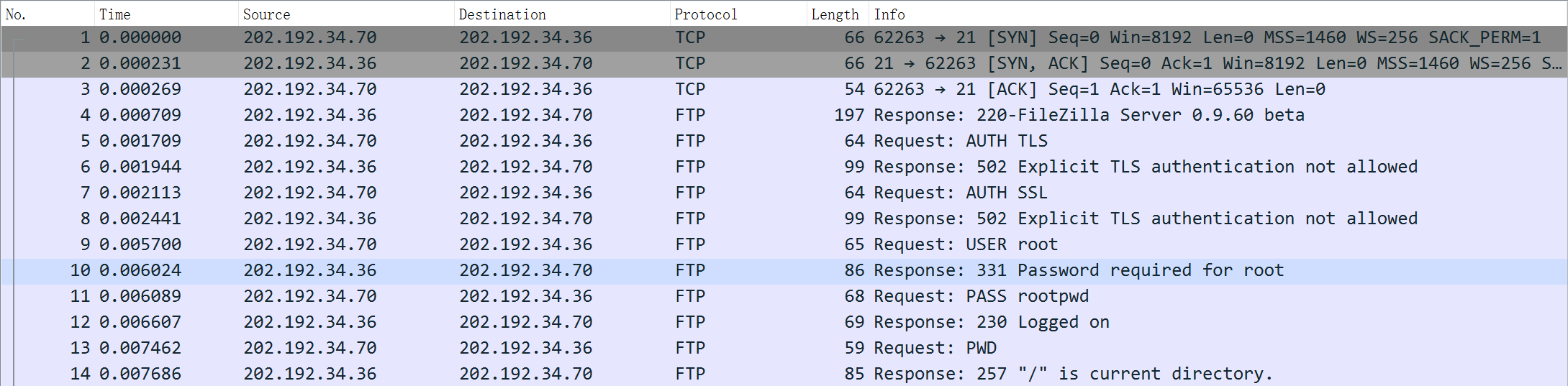
图中可见202.192.34.70正在询问FTP服务器的202.192.34.36的MAC地址。

1. FTP控制连接建立过程



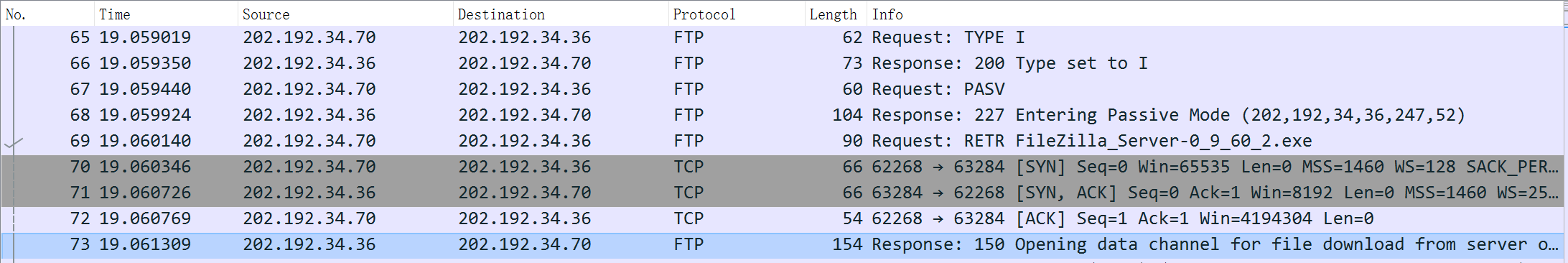
上图中可见TCP三次握手过程，以及控制连接建立过程。

1. FTP 用户登录身份验证过程



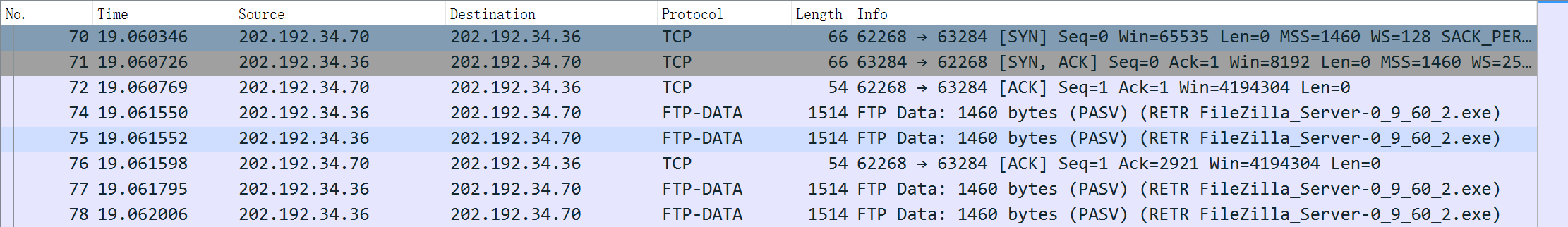
上图为TCP三次握手过程和FTP用户登录身份验证过程。

1. FTP 数据连接建立过程

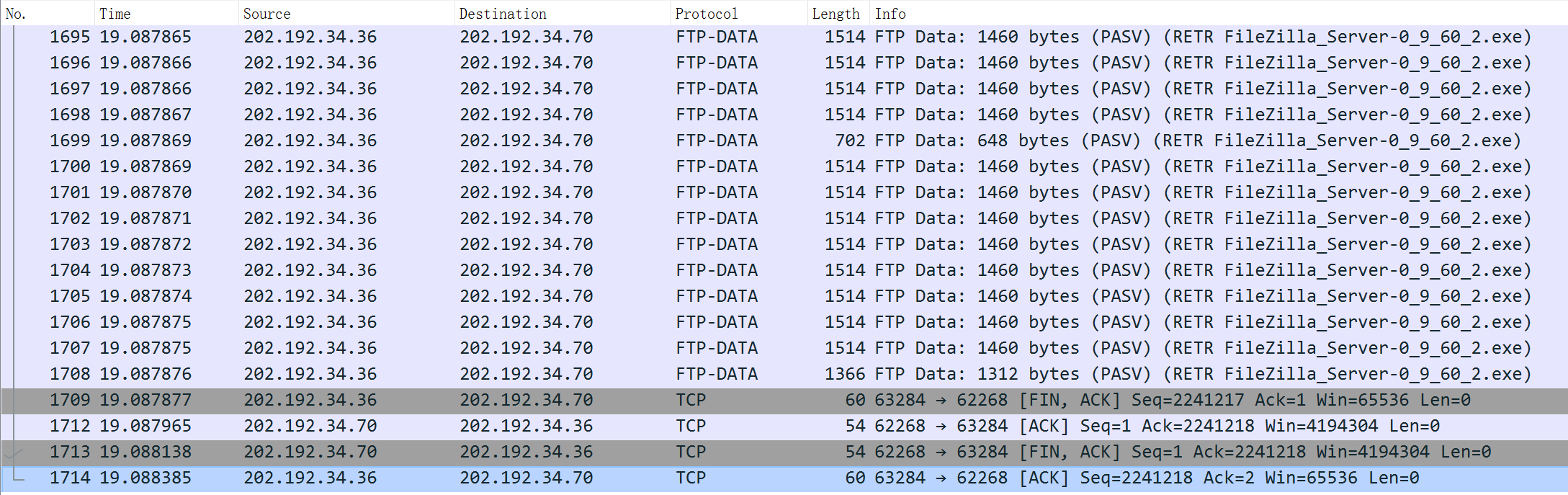


上图为FTP进入二进制被动模式并建立数据连接的过程。

1. FTP数据传输过程



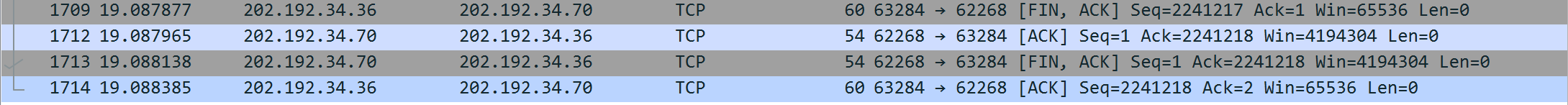
……



上图为从服务器上下载某个大文件时的FTP过程。

1. FTP连接释放过程（包括数据连接和控制连接）

下图为数据连接释放过程：



下图为控制连接释放过程：



## 实验分析

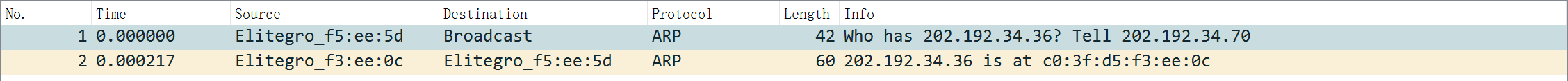
1. 捕捉整个FTP工作过程的协议包，并分析FTP协议。



图 1 工作在被动模式下的FTP

FTP协议的工作过程大致可划分为地址解析ARP过程（不总是需要进行）、控制连接建立过程、控制指令传输过程、用户身份认证过程、数据链接建立过程、数据传输过程和数据连接释放过程以及控制连接释放过程。逐过程分析如下（不考虑异常过程）：

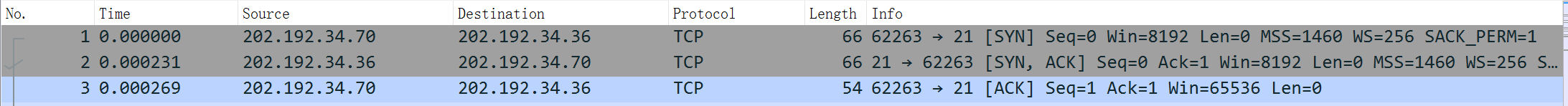
* 1. 地址解析ARP协议执行过程



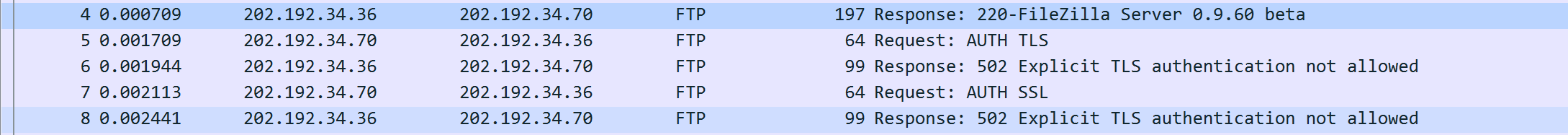
图示为FTP客户端202.192.34.36使用ARP查询同一网段下的FTP服务器202.192.34.36的MAC地址。在捕获的第1分组中，ARP查询报文被封装在IP数据包中，在同网段中进行广播。在捕获的第2分组中，服务器端202.192.34.36将自己的MAC地址以IP单播的方式告知客户端。这样，客户端获知了服务器端的MAC地址，（服务器端也可通过ARP获知客户端的地址，）两者可以通过IP数据报进行网络层通信了。

* 1. FTP控制连接建立过程

FTP控制连接建立在运输层协议TCP之上。要建立控制连接，首先要建立TCP连接。在完成a过程后，服务器和客户端已经能进行网络层通信里，接来需要进行TCP三次握手，建立TCP连接。

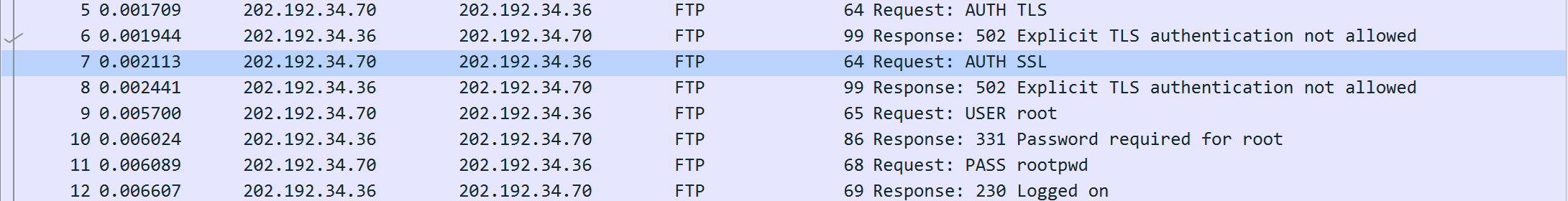


图示为TCP三次握手过程。在捕获的第1分组中，客户端向服务器发送自己随机挑选的报文段序号0，并置SYN比特，表示请求建立TCP连接。在第2分组中，服务器向客户端回应自己挑选的序号0，并置SYN比特，将ACK设为1，表示已经确认了客户端发送的序号为0的报文段。在第3分组中，客户端向服务器发送序号为1的报文段，置ACK为1，表示确认收到服务器端序号为0的报文段。这时，TCP连接已经建立了。



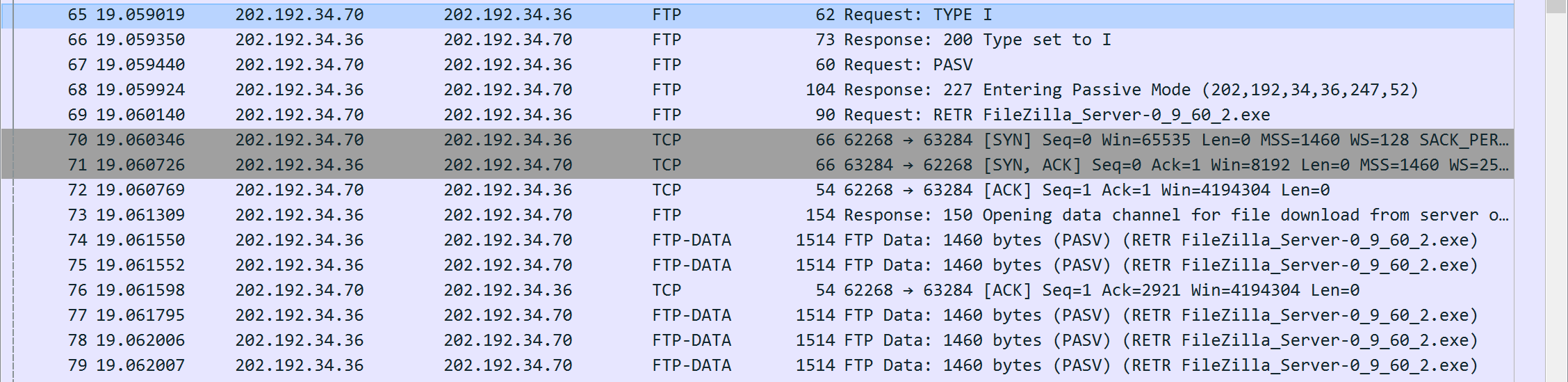
如图所示，TCP连接建立后，服务器向客户端发送FTP报文，报告服务器使用的软件版本号。（这是欢迎消息。）FTP连接建立。

* 1. FTP 用户登录身份验证过程



FTP连接建立后，用户当前处于匿名身份，需要进行用户名和密码验证以切换身份。如图所示，客户端先后使用Auth TLS和Auth SSL指令请求服务器加密FTP连接，但都被服务器拒绝。（实验时禁用了TLS和SSL设置，因为这样会使得网络协议分析器难以解密FTP报文。）于是客户端继续使用明文连接，先后使用USER和PASS指令，向服务器发送用户名和密码。服务器验证密码通过后接受了用户的登录请求。

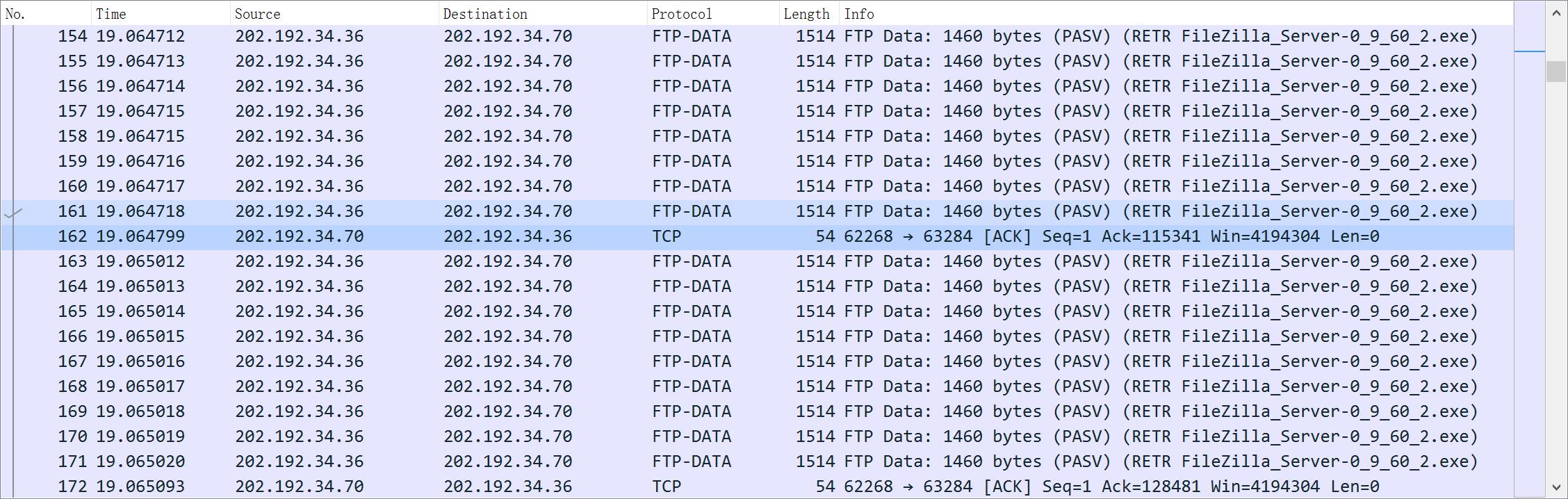
* 1. FTP 数据连接建立过程



实验时，FTP工作在被动模式。如图所示，客户端先使用Type I指令，将数据连接设置为二进制传输模式，接着使用PASV指令，指示服务器进入被动状态。最后使用RETR指令，表示从服务器中下载某文件。PASV响应报文中，服务器向客户端说明自己在63284端口（63284=247\*256+52）接收下一个FTP数据连接。于是客户端与服务器在服务器的63284端口进行TCP三次握手，TCP连接建立，FTP数据连接即相应地建立。

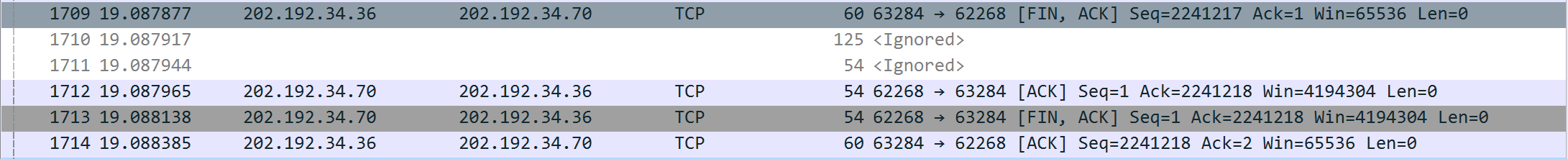
注意此时客户端并非与服务器端的20端口建立数据连接，而是进入FTP被动模式，与服务器端的动态端口进行连接。这里的被动是指服务器进入被动状态，等待客户端连接自己的动态端口，而不是通过20端口主动连接客户端的动态端口。

* 1. FTP数据传输过程

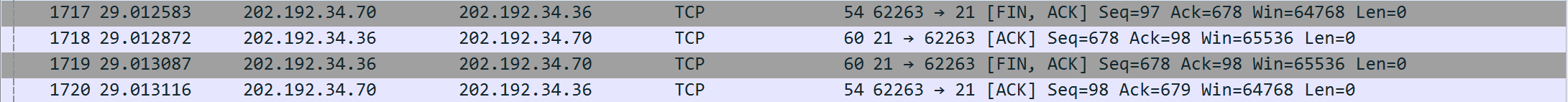


如图所示，FTP数据传输过程中，FTP数据连接中，低层次的TCP需要发送携带ACK字段的确认报文段，确认客户端已经正确地从服务器端接收到了数据。

* 1. FTP连接释放过程（包括数据连接和控制连接）



如图所示，在数据传输完毕后，数据连接进行关闭连接的四次挥手。服务器主动关闭连接，先是服务器发送FIN，客户端确认；然后是客户端发送FIN，服务器确认。



如图所示，客户端主动向服务器传送指示关闭FTP连接的QUIT指令后，控制连接的TCP进行关闭连接的四次挥手。客户端主动关闭连接，客户端向服务器发送FIN，服务器确认；然后服务器向客户端FIN，客户端确认。报文段顺序恰好与数据连接相反。

1. 捕捉及研究WWW应用的协议报文，回答以下问题：
   1. 当访问某个网页时，从应用层到网络层，用到了哪些协议？

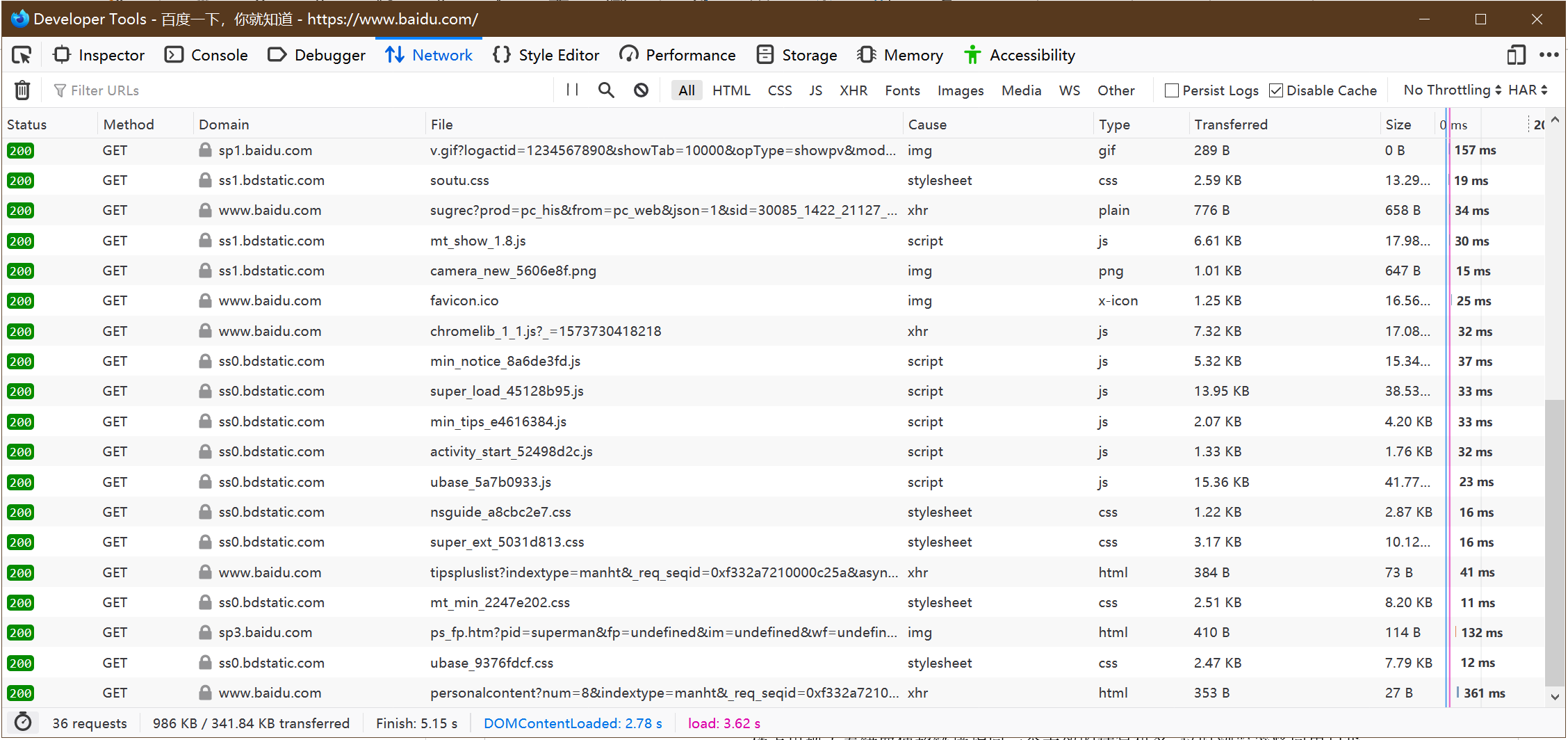
应用层：域名解析协议DNS、超文本传输协议HTTP/HTTPS。

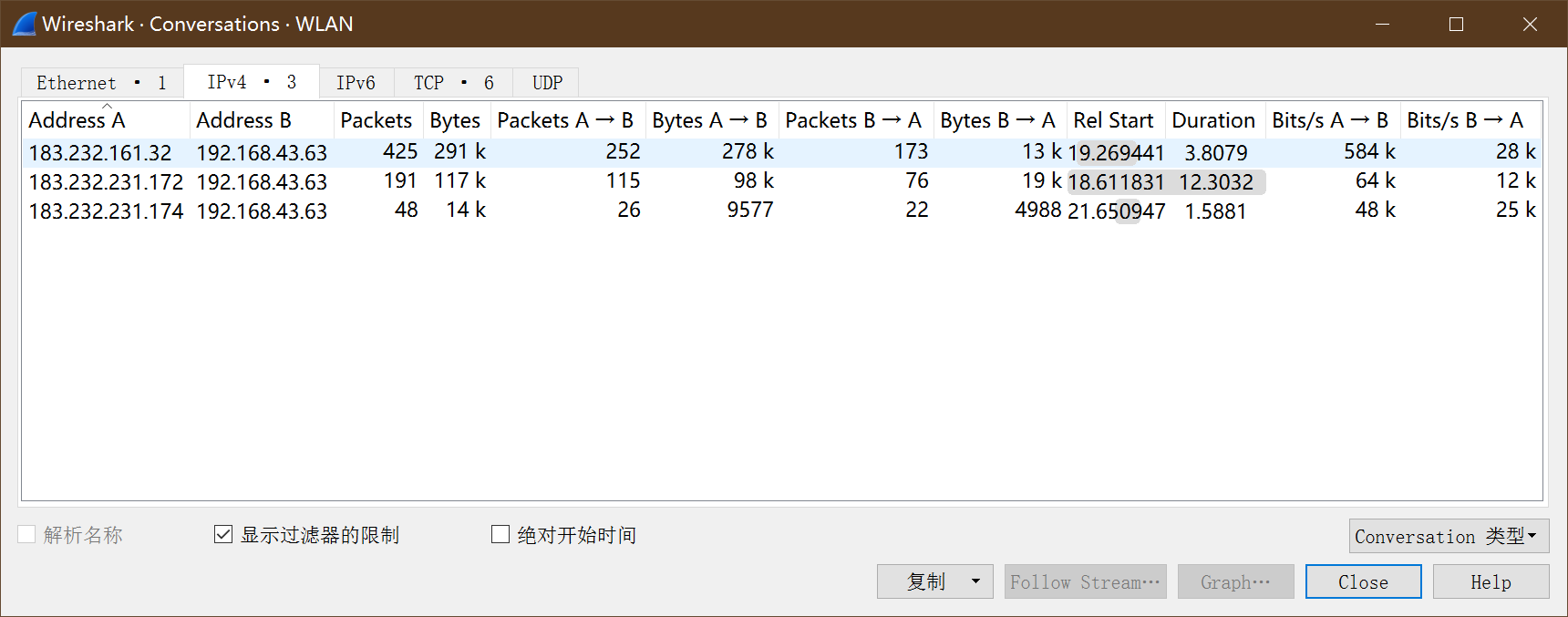
运输层：用户数据报协议UDP、传输控制协议TCP。

网络层：网际协议IP、地址解析协议ARP、网际控制报文协议ICMP。

* 1. 对于用户请求的百度主页（www.baidu.com），客户端将接收到几个应答报文？具体是哪几个？假设从本地主机到该页面的往返时间是RTT，那么从请求该主页开始到浏览器上出现完整页面，一共经过多长时间？

如图是一次实验的实验数据记录：





在图示的一次实验中，客户端收到了来自www.baidu.com（183.232.231.172），ss0.bdstatic.com（183.232.161.32），ss1.bdstatic.com（183.232.161.32），sp1.baidu.com（183.232.231.174），sp3.baidu.com（183.232.231.174）的共计664个TCP报文段，共收到来自各个域名的36个HTTP报文。

报文段RTT与请求主页到浏览器上出先完整页面的时间，在理论上与传输报文段的数量有关，约等于RTT乘以传输报文的数量。

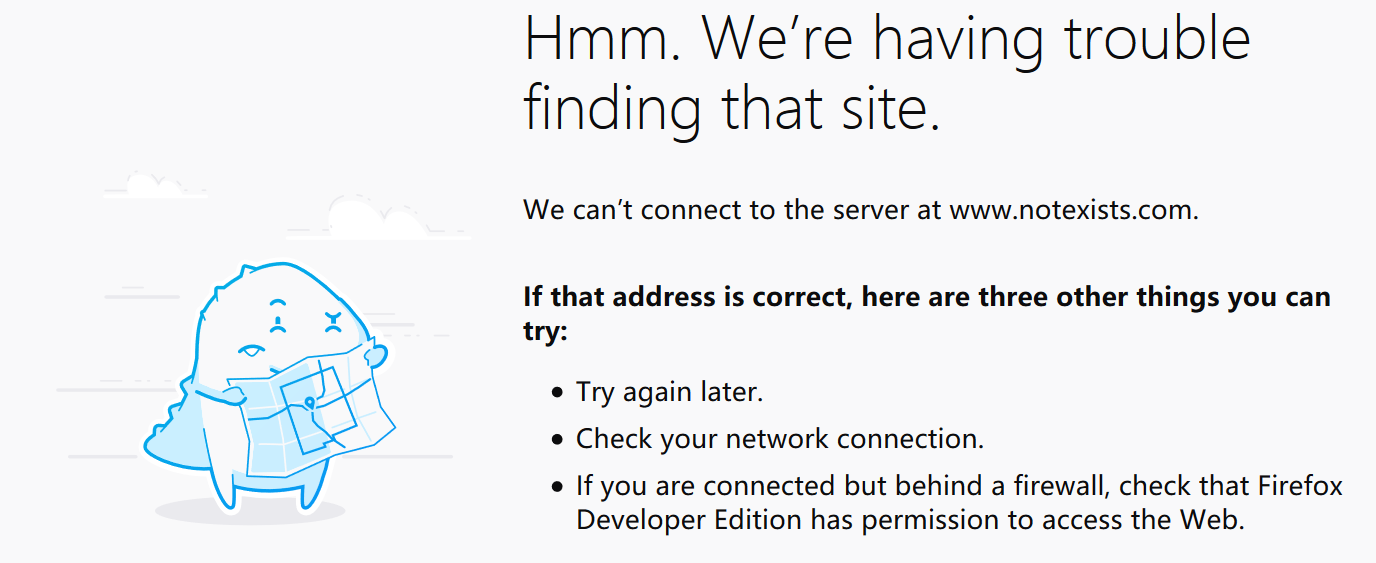
在图示的一次实验中，加载并显示完整页面的时间是5.15秒。

* 1. 两个存放在同一个服务器中的截然不同的Web页（例如， http://www.gzhu.edu.cn/index.jsp和http://www.gzhu.edu.cn/cn/research/index.jsp可以在同一个持久的连接上发送吗？

一般可以在同一个持久连接上发送，具体取决于HTTP服务器的设置。对于HTTP/1.0用户端可以使用“Connection: Keep-Alive”首部请求持久连接。对于HTTP/1.1，持久连接是默认开启的。

* 1. 假定一个超链接从一个万维网文档链接到另一个万维网文档，由于万维网文档上出现了差错而使超链接指向一个无效的计算机名，这时浏览器将向用户报告什么？

浏览器报告“无法找到服务器”。



* 1. 当点击一个万维网文档时，若该文档除了有文本外，还有一个本地.gif图像和两个远地.gif图像，那么需要建立几次TCP连接和有几个UDP过程？

DNS查询，取决于远地文档和图像的域名数量，可能产生1~3个UDP过程，与域名的数量相当。

本地连接不需要建立TCP连接或UDP连接。文本和两个图像，视乎于是否在同一个域名以及网页服务器的相关设定，可能在1~3个TCP连接中传输。

## 实验建议

请更新2015网络实验指导书中的Ethereal软件为Wireshark。在2006年，Ethereal因商标问题重命名为Wireshark。名为Ethereal的软件不再维护，已经很难用于现代硬件。相比于Ethereal，Wireshark提供的功能夜更加丰富。