实验四 数据包捕获和分析

实验 4-1 Wireshark 的使用

一、实验目的

1. 认识 WireShark 在网络中的作用。
2. 熟练使用 WireShark 捕获网络数据包。
3. 利用 WireShark 对数据包作分析。

二、实验设备

连网的计算机， windows 操作系统，WireShark。

二、实验步骤

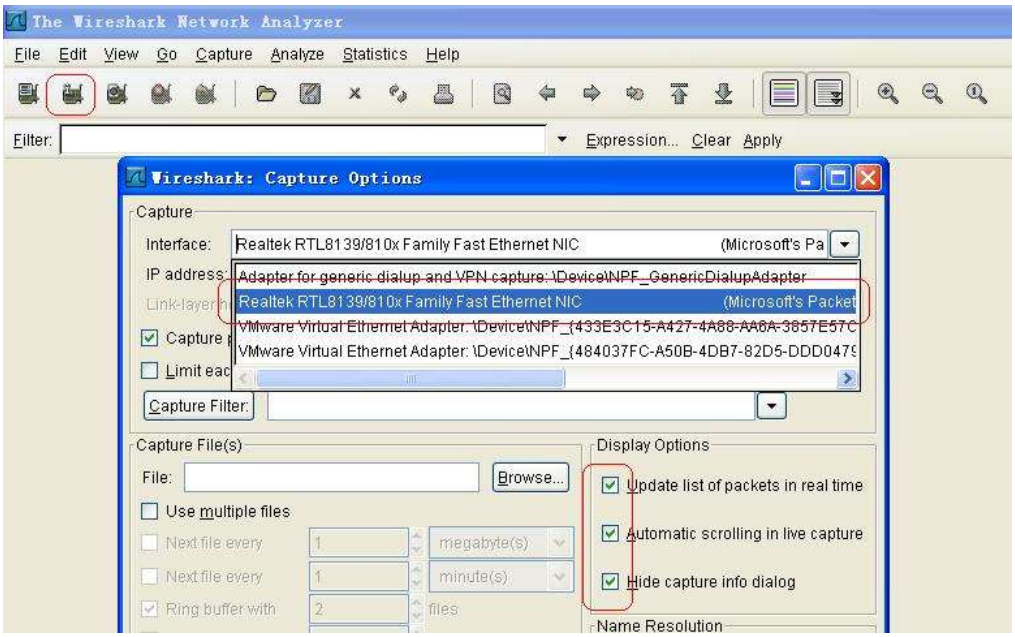
1. WireShark 的安装

Wireshark 的前身叫做 Ethereal(2006.06 因为商标问题改名)，是一种开放原代码软件。Wireshark 支持了多种操作系统，在 Windows、UNIX、等下都有相对应的版本。由此软件可以抓取数据封包，进一步分析封包内的摘要及详细信息。一般常用在网络故障排除、监听异常封包、软件封包问题检测等地方。Wireshark 的方便强大之处，在于其支持的 Protocol 多且完整，。此外，在接口使用上，Wireshark 图形化的接口相当容易上手，丰富的过滤语言，可以判别出封包的种类，是一套整合度完整的软件。

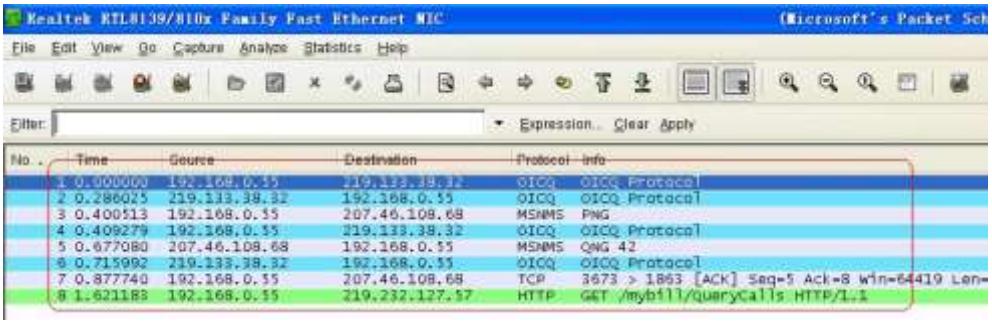
点击可执行程序 Wireshark，安装软件。

2. WireShark 的使用

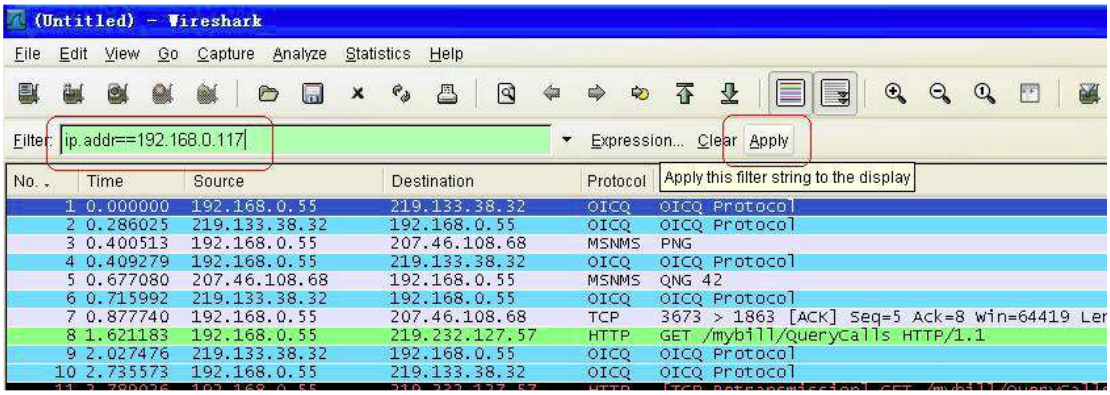
打开WireShark，如图所示：



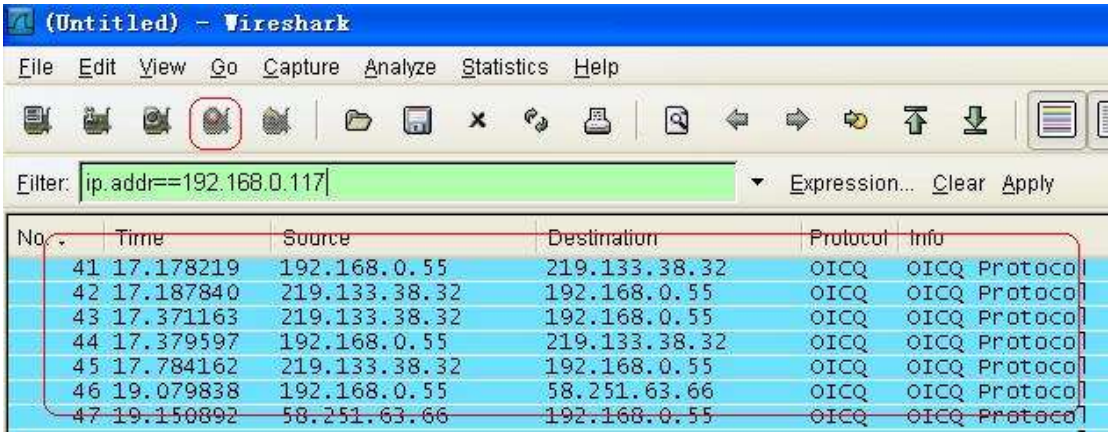
选择 PC上的物理网卡，即目前电脑所使用的网卡，然后在红线所圈处把选项勾上后点击 start；正确的选择网卡后，会有数据包出现，如下图所示：



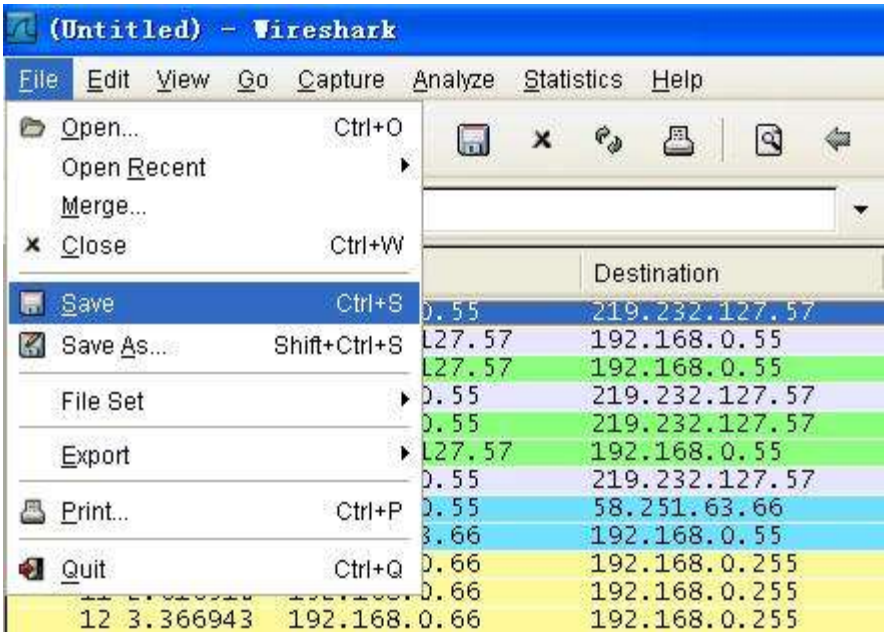
填写IP地址，实行包过滤。格式为：ip.addr＝＝设备的 ip地址。填写完成后，点击 APPLY 应用。然后点开始，就有相应ip地址的数据包出现。



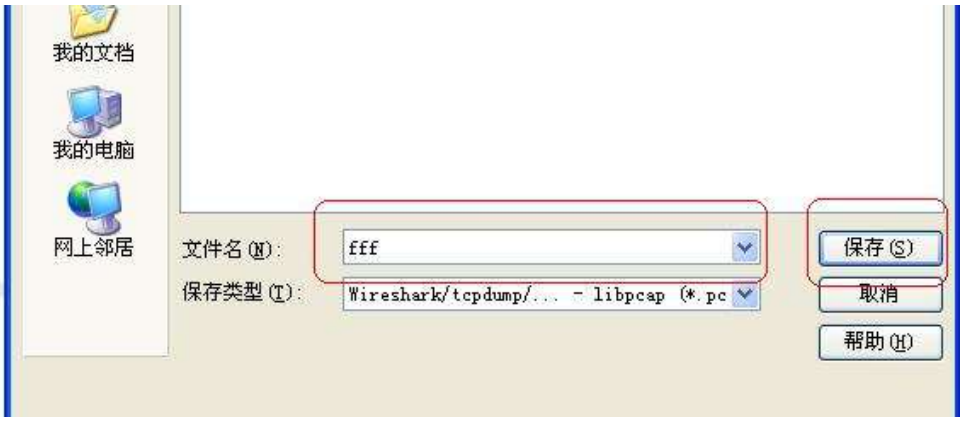
点击停止抓包（图中小红圈中的按钮）



保存所抓的数据包

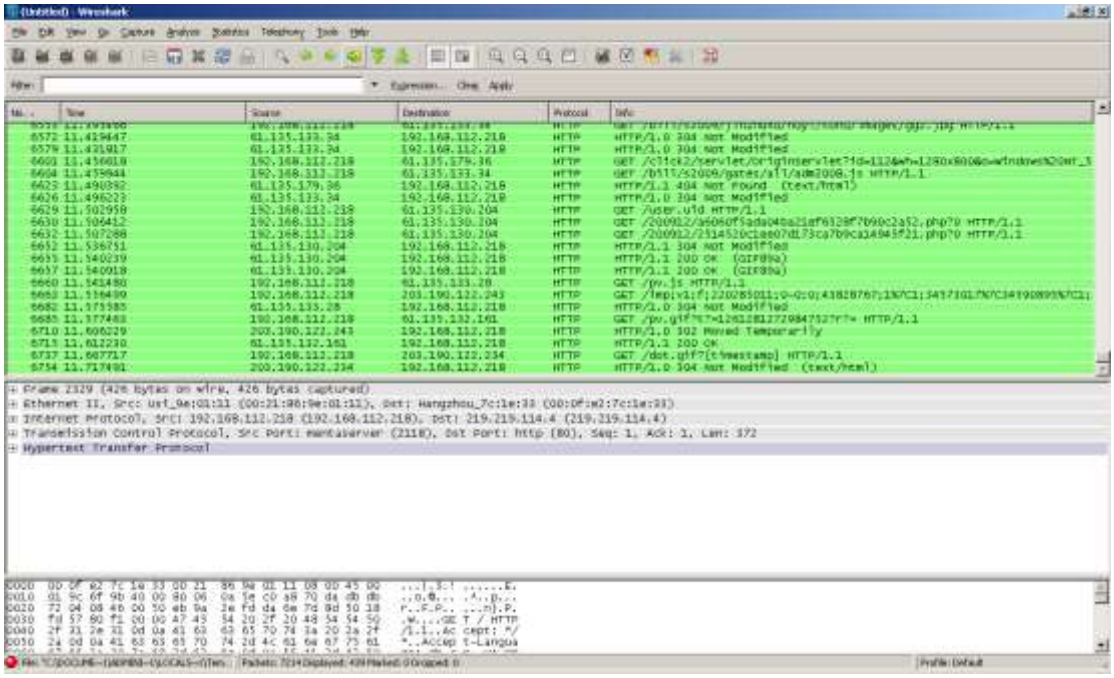


点击 FILE 中的 SAVE， 添加文件名，选择保存的地点，点击保存，最后退出抓包软件。

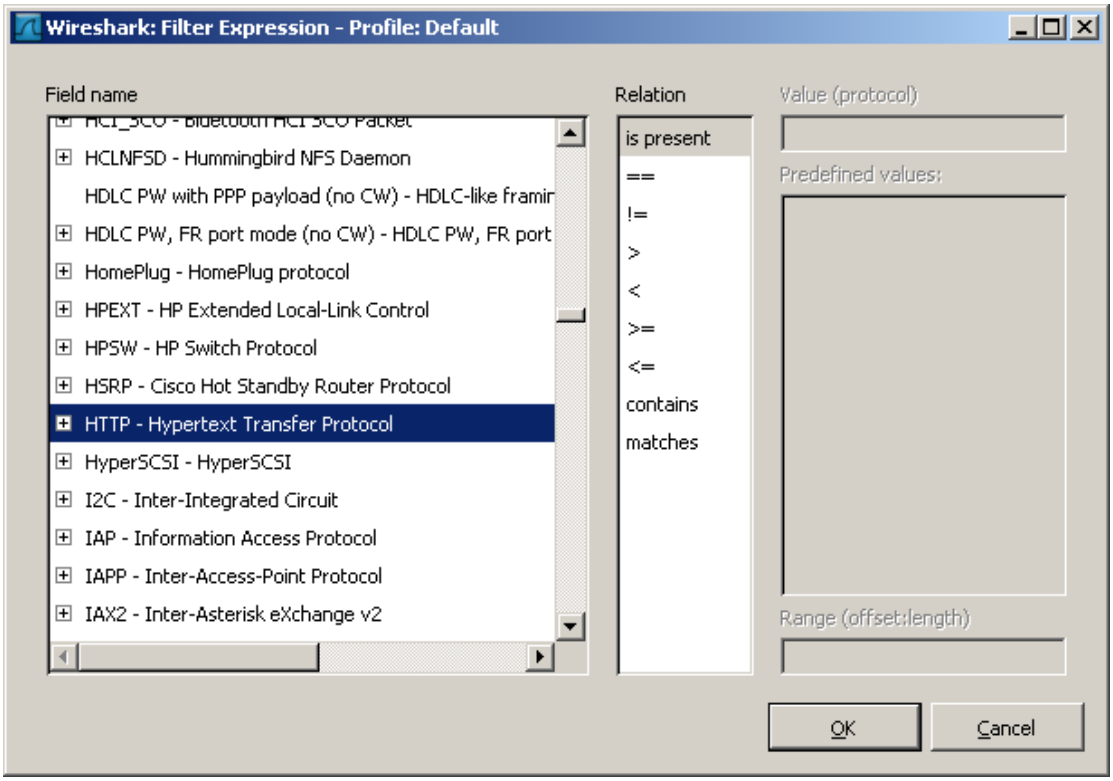


3. 捕获数据包过滤

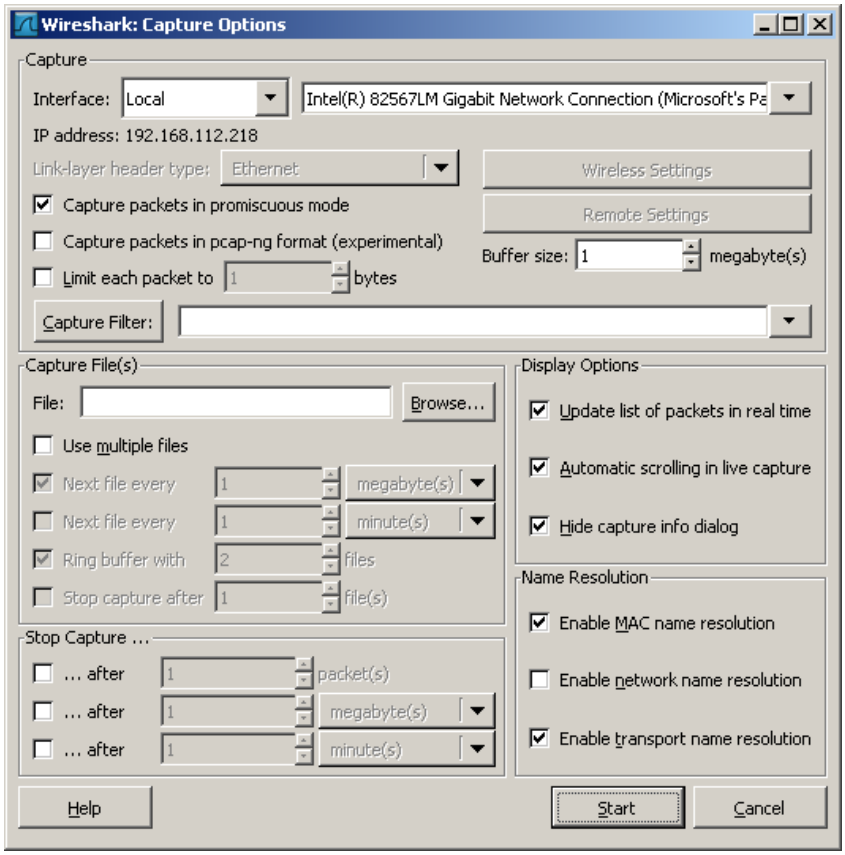
先捕获网络数据包。停止之后接口上的数据包将不再增加，由于数据包太多太杂，这时候可以利用 Display Filter 功能过滤呈现的内容，如下图点击 Expression 挑选过滤语法。



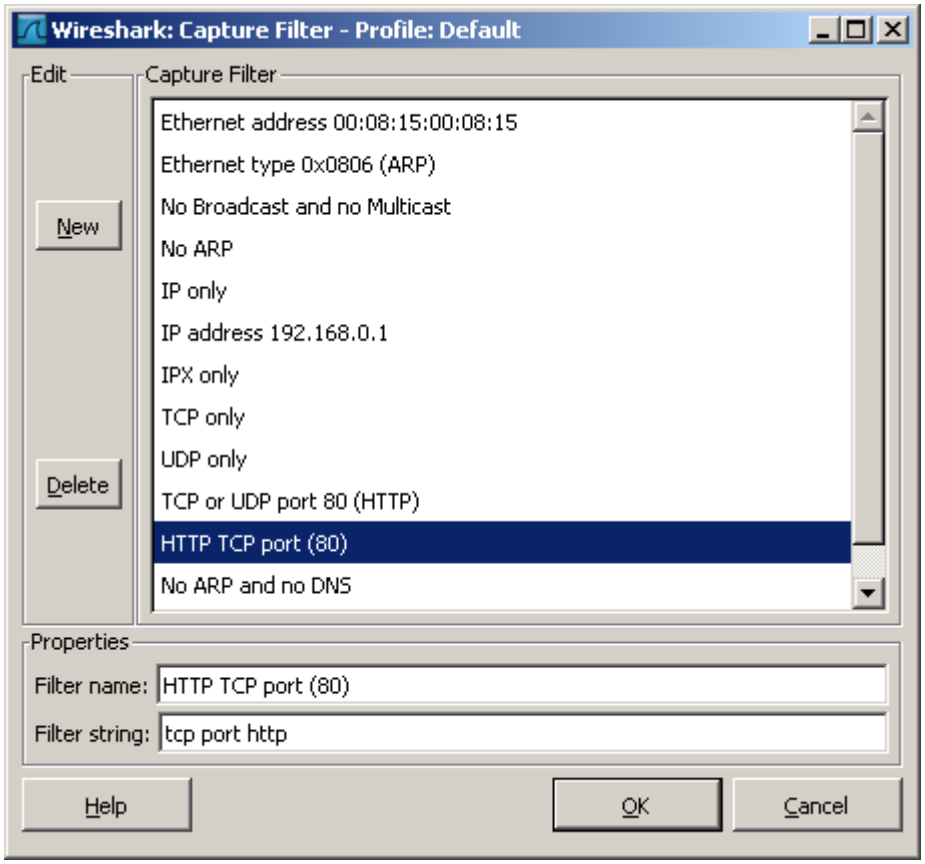
因为我们只是要筛选出 Http 协议的流量，找到 Http 字样如下，直接按 OK。点击 apply，实现过滤。



也可以通过下图的方式，过滤捕获的数据包。



点击 Capture Filter：


Wireshark: Capture Filter - Profile: Default
Edit
Capture Filter
New
Delete
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
No Broadcast and no Multicast
No ARP
IP only
IP address 192.168.0.1
IPX only
TCP only
UDP only
TCP or UDP port 80 (HTTP)
HTTP TCP port (80)
No ARP and no DNS
Properties
Filter name:
HTTP TCP port (80)
Filter string:
tcp port http
Help
OK
Cancel

实验 4-2 Ethernet 帧结构分析实验

一、实验目的

1. 学习 Ethereal/Wireshark网络协议分析器的操作，掌握捕获和分析网络数据包的方法。
2. 通过捕获数据包观察和了解 Ethernet帧的结构。

二、实验设备

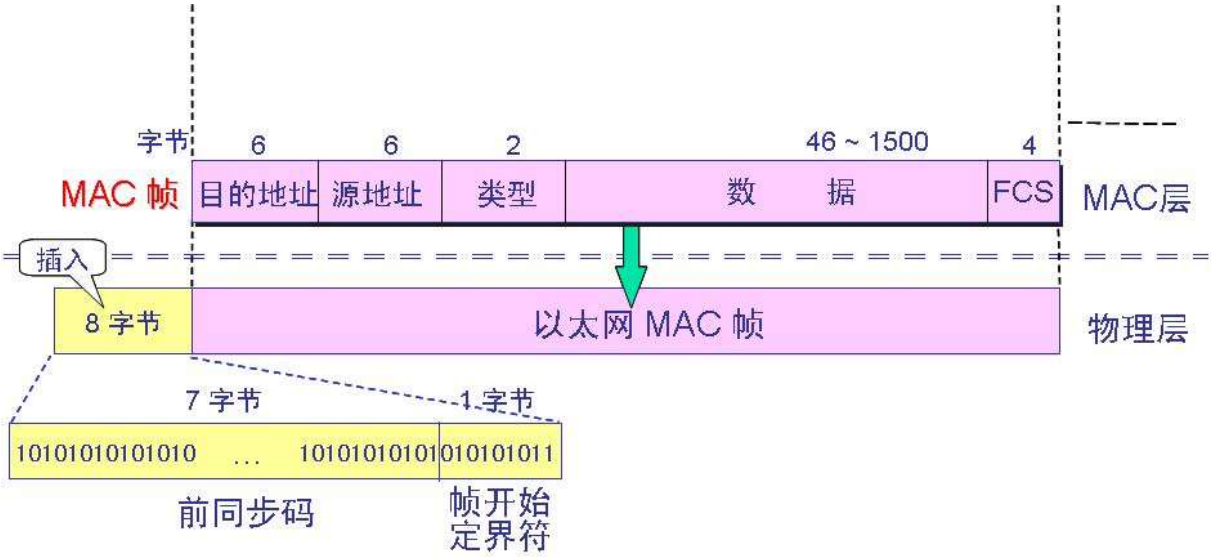
连网的计算机， windows 操作系统，WireShark。

三、实验原理

Ethernet 帧结构

Ethernet 是目前应用最广的局域网，因此学习 Ethernet 技术对深入掌握局域网知识是非常重要的。对 Ethernet 帧结构的观察和分析有利于理解和掌握 Ethernet 的工作原理。在 IEEE802.3 标准中将 Ethernet 帧结构设定为：

前同步码 (7 字节) 、帧前定界符 (1 字节)、目的地址(6 字节)、源地址 (6 字节)、类型(2 字节)、数据 (44-1500 字节)、帧校验字段 FCS (4 字节)。



各部分含义为：

前同步码：用来保证接收电路在帧的目的地址字段到来之前达到正常状态。

帧前定界符：可视为前导码的延续。前导码和帧前定界符主要起到接收同步的作用，这 8 个字节接收后不需要保留，也不计入帧头长度。

目的地址和源地址：分别表示数据帧的接收结点和发送结点的 MAC 地址。

类型：用 2 个字节表示上一层使用的是什么协议,以便将收到的 MAC 帧交给上一层的这个协议。

数据字段：为帧的数据字段，当数据少于 46 字节时用任意字符将数据字段的长度填充到 46 字节，填充部分不计入长度字段值中。

帧校验字段：采用 32 位 CRC 来校验目的地址、源地址、类型、数据等字段。

四、实验步骤

1．启动 Ethereal/Wireshark 软件。

2．在“Capture”菜单中选择“Options”菜单选项，在 Options 设置窗口中把捕获参数设置为非混杂模式。

3．点击“Start”按钮开始捕获数据包。

4．打开

IE 浏览器浏览某网站的主页，待页面完全显示完后点击“Stop”按钮，关闭浏览器。

5．选中被捕获的一个数据包，在详细信息窗口中逐层观察各协议层的详细信息。

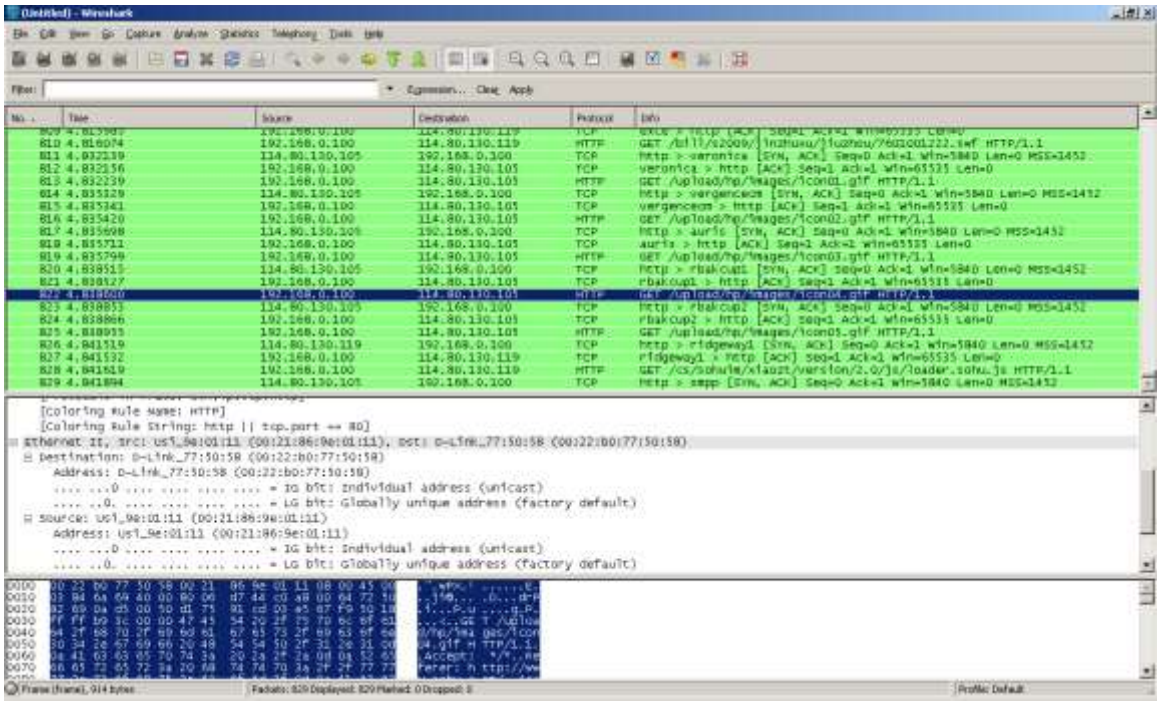
6．分析 Ethernet 帧中的结构以及各项信息的含义。

7．选择“File”菜单中的“Save”保存捕获信息。

8．选择“File”菜单中的“Save as”将捕获信息保存为其他文件格式。

9．熟悉 Wireshark 软件的其他功能。

10．实验结果参考



五、实验总结

通过实验掌握数据包捕获的方法，了解 Ethernet 帧的结构。在实验报告中需要回答以下问题：

1. 挑选捕获的一个数据包，写出该数据包中 Ethernet 帧的结构以及各项信息的含义。
2. 捕获数据包的封装协议层次依次有哪些，为什么。
3. 源 MAC 地址和目的 MAC 地址分别指什么计算机的物理地址？

实验 4-3 IP 数据报结构及分析实验

一、实验目的

1．观察和了解 IP 数据报的结构。

2．学习 IP 数据报的分片和重组。

二、实验内容

1．在 Windows 环境下，使用 Wireshark 捕获 IP 数据报。

2．观察和分析 IP 数据报的结构、分片信息。

三、实验原理

IP 协议一种无连接的、点对点的数据报传送协议，它位于网络层，且能将来自底层的不同物理网络帧统一为 IP 数据报提供给传输层使用，因此 IP 协议使得各种异构物理网络的互联变得容易。

(1) IP 数据报结构

IP 数据报的结构如图所示，分为报头和数据两个部分。

报头格式有：

版本 ：占 4bit，表示所使用的 IP 协议的版本号。

首部长度：占 4 bit，可表示的最大数值是 15 个单位(一个单位为 4 字节)，因此 IP 的首部长度的最大值是 60 字节。

服务类型：长度为 8 位，其中包括 4 位的服务类型子域和 3 位优先级组成（1 位为保留位）。服务类型用于指示路由器如何处理该数据报，即延迟(delay)、可靠性(reliability)、通信量(throughput)与成本(cost)；优先级共分为 8 级，数值越高登记越高。

总长度：总长度指首部和数据之和的长度，单位为字节。总长度字段为 16bit,因此数据报的最大长度为 65 535 字节。

标识：占 16 bit，它是一个计数器，用来产生数据报的标识。

生存时间：表示数据报在互联网络的传输过程中可以经过的最多的路由器跳步数。

首部校验和：用于保证数据报头部的数据完整性。

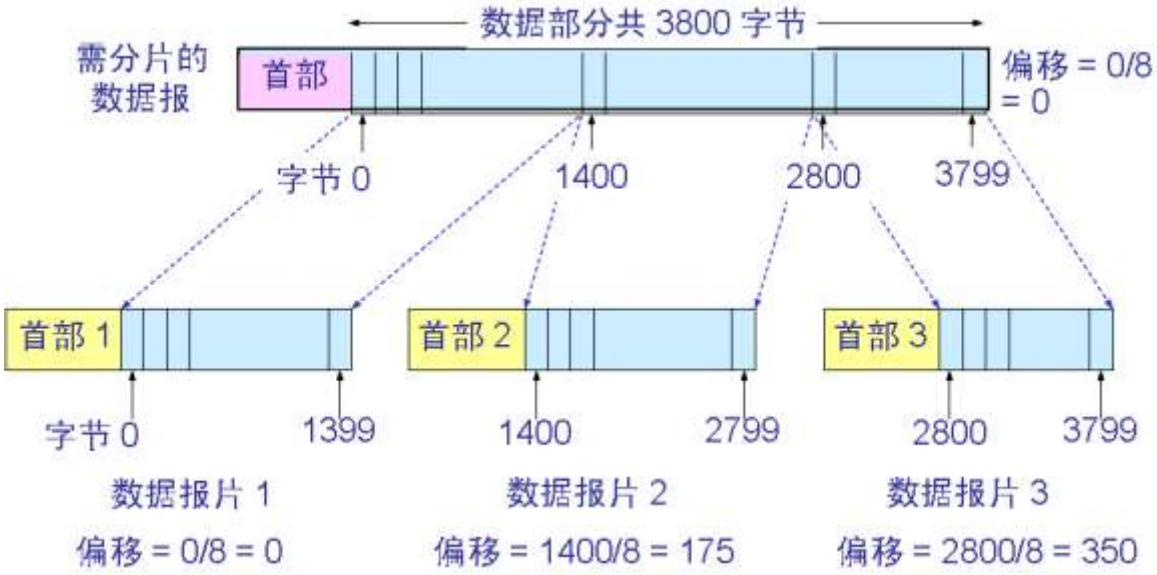
源地址和目的地址：分别表示发送和接收数据报的机器的 IP 地址。

可选字段：用于控制与测试的目的。

填充域：如果 IP 头部的长度不是 32 位的整数倍，就需要填充域来凑齐。

(2)IP 数据报的分片与重组

由于 IP 下面的不同物理网络规定了各自数据帧的最大字节长度（Ethernet 的最大传输单元 MTU 为 1500 字节），所以 IP 协议必须将大于这些最大传输单元的 IP 数据报分片，才能通过物理网络传输 IP 数据报。当分片的 IP 数据报到达目的地的网络层时，又由 IP 协议将分片数据报组装为一个完整的 IP 数据报，提供给传输层的协议使用。



IP 数据报分片示意如图。在 IP 数据报的报头中，与一个数据报的分片、组装相关的域有标识域、标志域与片偏移域。

标识（identification）：为一个数据报的所有片分配一个标识 ID 值，成为片识别的标记，它占 2 个字节，最多可以分配 65535 个 ID 值。

标志（flags）：占 3 位，最高位为 0，中间位 DF 为 1 时，表示接收结点不能对数据报分片。最低位 MF 为 1 表示接收的分片不是最后的一个分片；为 0 时表示接收的是最后一个分片。

片偏移域（fragment offset）：是以 8 字节为单位来计数的，表示该分片在整个数据报中的相对位置。

四、实验步骤

1．启动 Wireshark 软件。

2．在“Capture”菜单中选择“Options”菜单选项，在 Options 设置窗口中把捕获参数设置为非混杂模式。

3．点击“Start”按钮开始捕获数据包。

4．在开始菜单中点击“运行”，输入“ping 202.102.75.163”命令（注意 ping 命令中的 IP 地址应是实际实验网络中存在的一个 IP 地址），ping 命令执行完后，点击“Stop”按钮停止捕获。

5．选中被捕获的一个 ICMP 协议数据包，在详细信息窗口中观察并记录 IP 数据报的详细信息。

6．分析 IP 数据报的结构以及各项信息的含义。

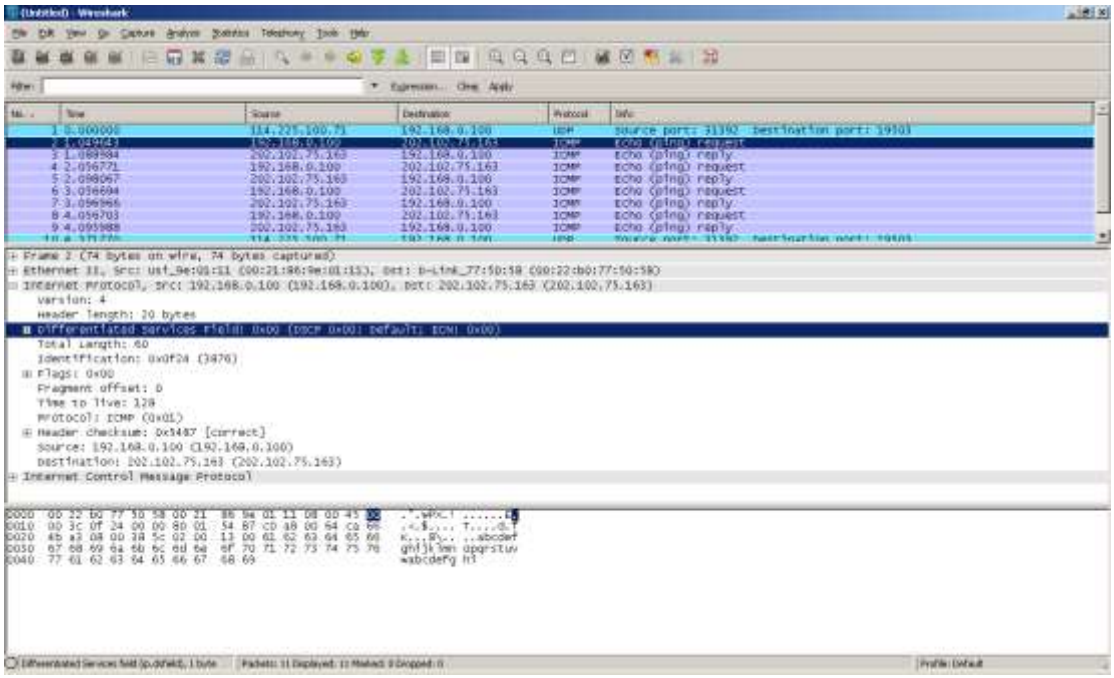
7．在“Capture”菜单中选择“Start”菜单选项，重新开始捕获数据包。此时，在开始菜单的“运行”窗口中，输入“ping －l 4000 202.102.75.163”命令，ping 命令执行完后，点击“Stop”按钮停止捕获。

8．在详细信息窗口中观察 ICMP 协议数据包，并记录 IP 数据报分片的详细信息。

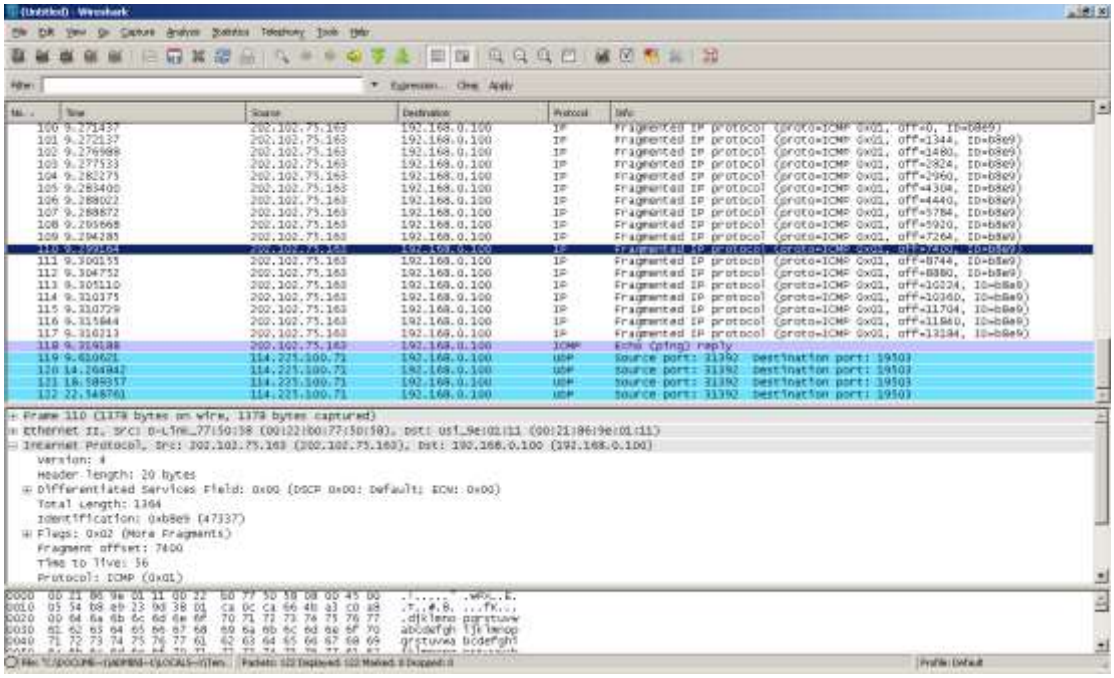
9．分析 IP 数据报是如何分片的。

10．实验结果参考

未分片 IP 数据包：



分片 IP 数据包：



五、实验总结

通过实验了解和掌握 IP 数据报的结构及分片、组装方法。在实验报告中需要回答以下问题：

1. 挑选捕获的一个未分片数据包，写出该数据包的结构以及各项信息的含义。
2. 挑选捕获的一个分片数据包，写出该数据包中的结构以及各项信息的含义。
3. 根据实验数据，说明 IP 数据报的结构及分片、组装方法。
4. 当 ping 一个网络中不存在的机器时，会捕获到什么样的数据包？
5. 在捕获“ping －l 4000 202.102.75.163”命令的数据包中，为什么会将发送的一个 IP 数据报分片，一共分为几个分片。

实验 4-4　TCP 协议分析实验

一、实验目的

1．观察和了解 TCP 报文段的结构。

2．学习和理解 TCP 传输的连接和释放过程。

二、实验内容

1．在 Windows 环境下，使用 Wireshark 捕获 TCP 协议传输的数据包。

2．观察和分析 TCP 报文段的结构。

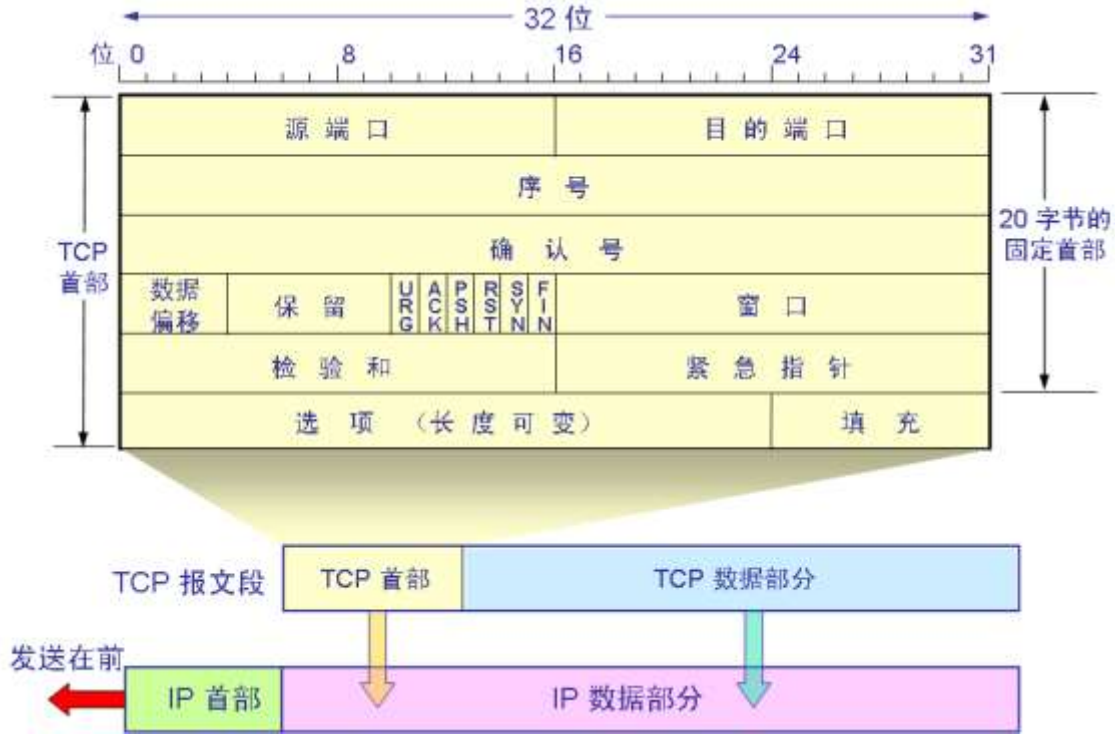
3．观察和分析 TCP 传输的连接和释放过程

三、实验原理

TCP 是 TCP/IP 体系中面向连接的运输层协议，它提供全双工的和可靠交付的服务。

1. TCP 报文段的结构

一个 TCP 报文段分为首部和数据两个部分。首部信息体现了 TCP 的全部功能，长度为 20 至 60 字节，固定部分为 20 字节，其结构如图所示：



首部结构如下所示：

源端口号与目的端口号：分别表示发送和接收该报文段的端口号。

序号：为每一个发送的字节编的序号。

确认号：表示接收端希望接收到的下一个报文段的第 1 个字节的序号。

数据偏移：占 4bit，且以 4 字节为一个单位来计算报文头部的长度。

保留：占 6bit，留做今后使用，目前置为 0。

控制域：包括 URG、ACK、PSH、RST、SYN、FIN 6 个不同的控制，用于 TCP 的流量控制，连接建立和释放、数据传送方式的控制。

窗口：用于控制对方发送的数据量，表示接收端接收能力的大小。

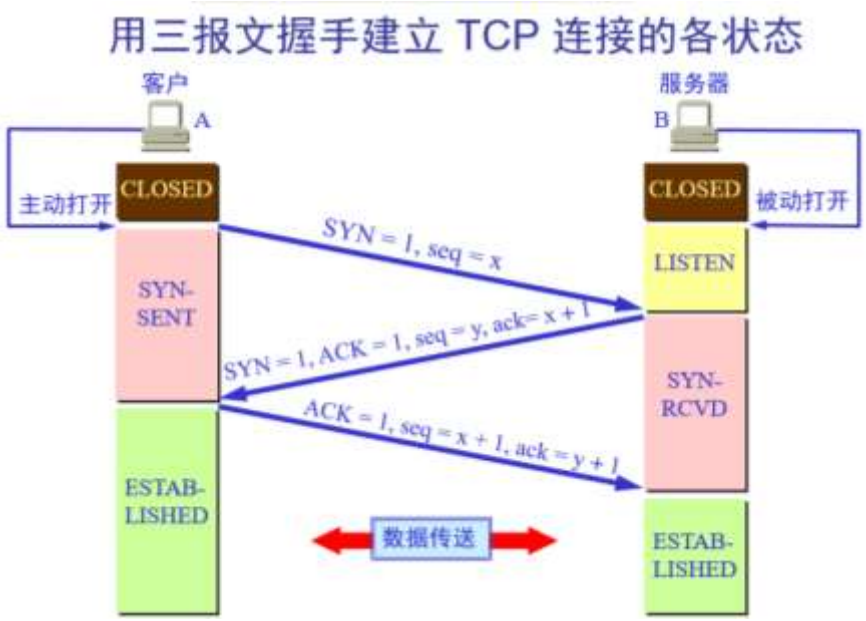
紧急指针：当紧急标志 URG=1 时有效，表示该报文中有紧急数据。

校验和：用于检验报文数据是否出错。

选项：包括选项结束、无操作、最大报文段长度、窗口因子以及时间戳。当没有使用选项时，TCP 首部长度是 20 字节。

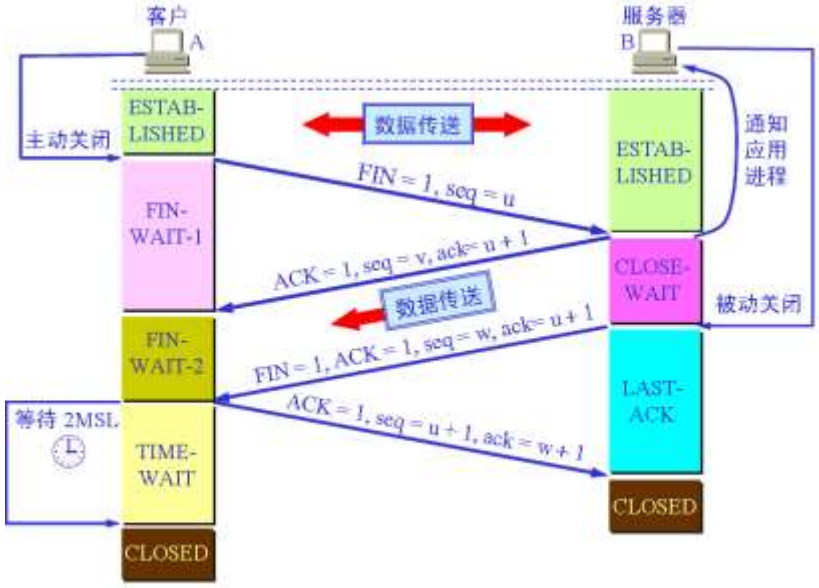
2. TCP 建立连接

TCP 在进行传输之前必须在客户进程与服务器进程之间使用 3 次握手的方式建立一条传输连接，只有当连接建立之后，通信的两个进程才可以在该连接之上发送和接收数据。TCP 建立连接的过程如图所示 。



3. TCP 释放连接

当客户进程与服务器进程之间的数据传送结束时，需要释放传输连接，由其中一方提出释放连接请求（请求报文中的终止比特 FIN 被置为 1），经过双方的 4 次交谈之后，才能释放已建立的连接。其过程如图所示。



四、实验步骤

1．启动 Wireshark 软件。

2．在“Capture”菜单中选择“Options”菜单选项，在 Options 设置窗口中把捕获参数设置

为非混杂模式。

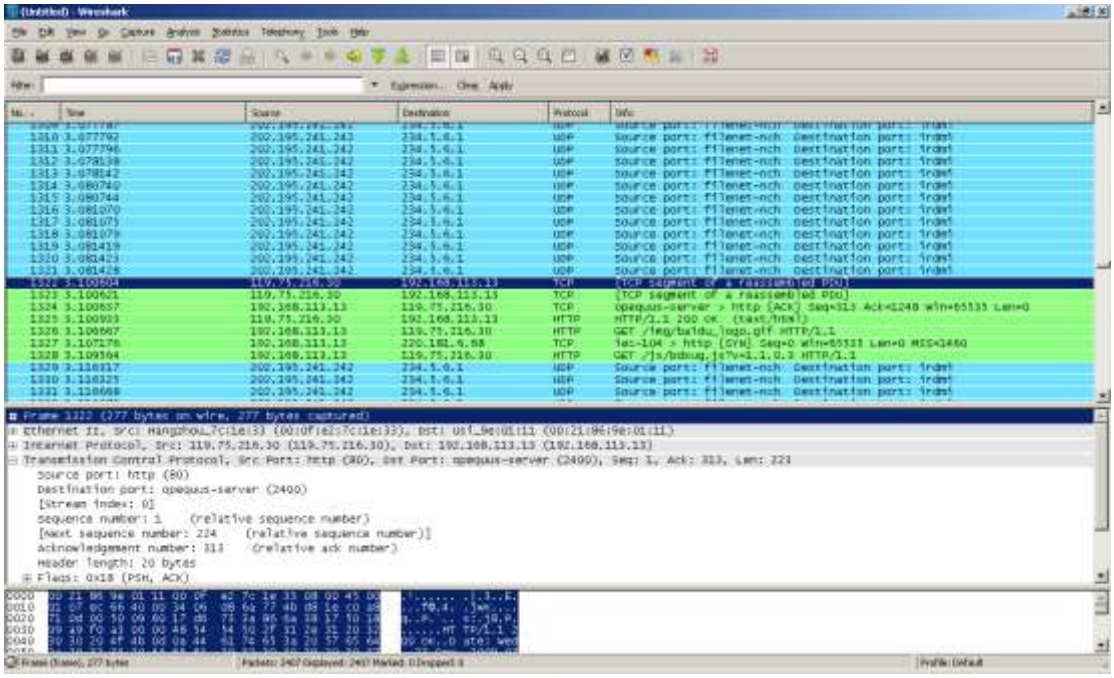
3．点击“Start”按钮开始捕获数据包。

4．在 IE 浏览器的地址兰输入“www.baidu.com”浏览该网站的主页，待主页信息显示完毕后，点击“Stop”按钮停止捕获。

5．观察和分析 TCP 报文段的结构以及各项信息的含义。

6．分析 TCP 建立连接、传送数据和释放连接的过程。

实验结果参考：



五、实验总结

通过实验可以使学生了解 TCP 报文段的结构和 TCP 建立连接和释放连接的过程。在实验报告中需要回答以下问题：

1．根据实验数据，说明 TCP 报文段的结构以及各项信息的含义。

2．根据实验数据，说明 TCP 建立连接和释放连接的过程。

3．为什么 TCP 要经过 3 次握手来建立连接？如果只进行前 2 次握手来建立连接行不行，为什么？

4．TCP 数据传送完时为什么要释放连接，为什么释放连接还要进行 4 次握手？

实验 4-5 HTTP 协议分析实验

一、实验目的

1．观察和了解 HTTP 的操作过程

二、实验内容

1．在 Windows 环境下，捕获浏览 www.baidu.com 网站主页。

2．分析 HTTP 协议的工作过程以及相关数据包的信息。

三、实验原理

1． HTTP 协议

HTTP 协议用于超文本文件的传输。当浏览网站获得一个网页时需要经历以下过程：

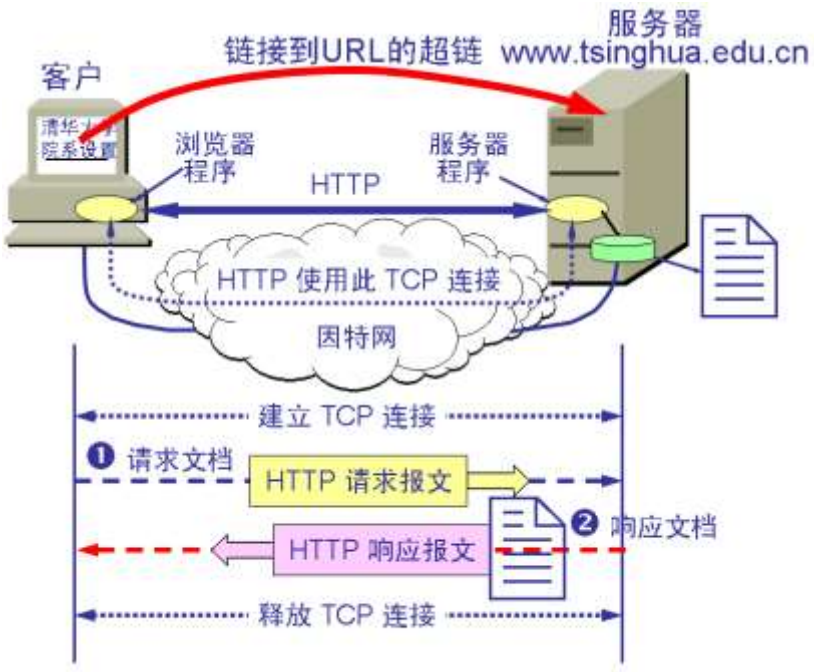
第 1 步用户输入链接地址，浏览器向本地域名服务器发送，获取所输连接地址的计算机的 IP 地址。

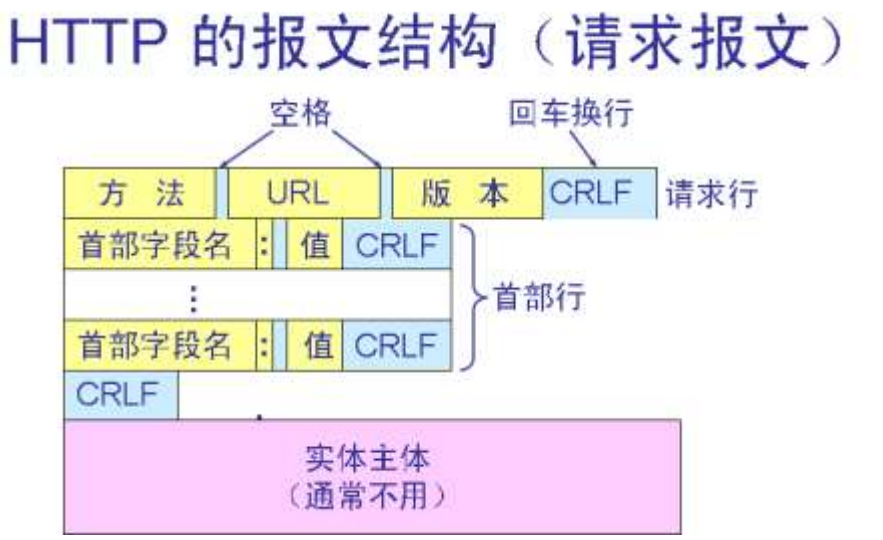
第 2 步 获得 IP 地址后，浏览器申请与服务器进程建立连接， 一般是 TCP 连接。如果服务器准备就绪，则连接成功。

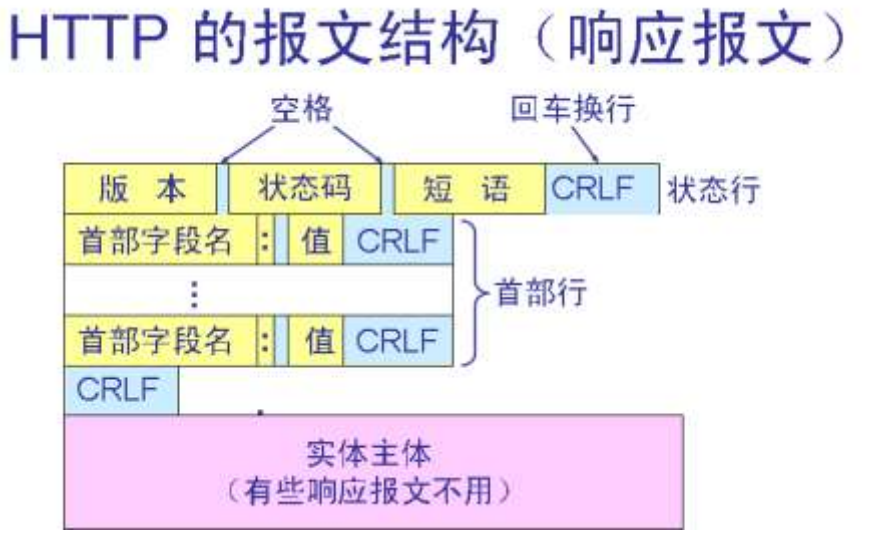
第 3 步 浏览器运行 HTTP，发出请求，并申明要获取的文档名和合法的文档格式。 含有所需文档的服务器通过发送 HTTP 应答响应。

第4步 含有所需文档的服务器通过发送HTTP应答响应客户的HTTP请求，并按要求的文档格式将所请求的文档传送给浏览器。

第 5 步 用户浏览文档。若无新的请求，一定时间后服务器 关闭 TCP 连接。







四、实验步骤

1．启动 Wireshark 软件。

2．在“Capture”菜单中选择“ Options”菜单选项，在 Options 设置窗口中把捕获参数设置为非混杂模式。

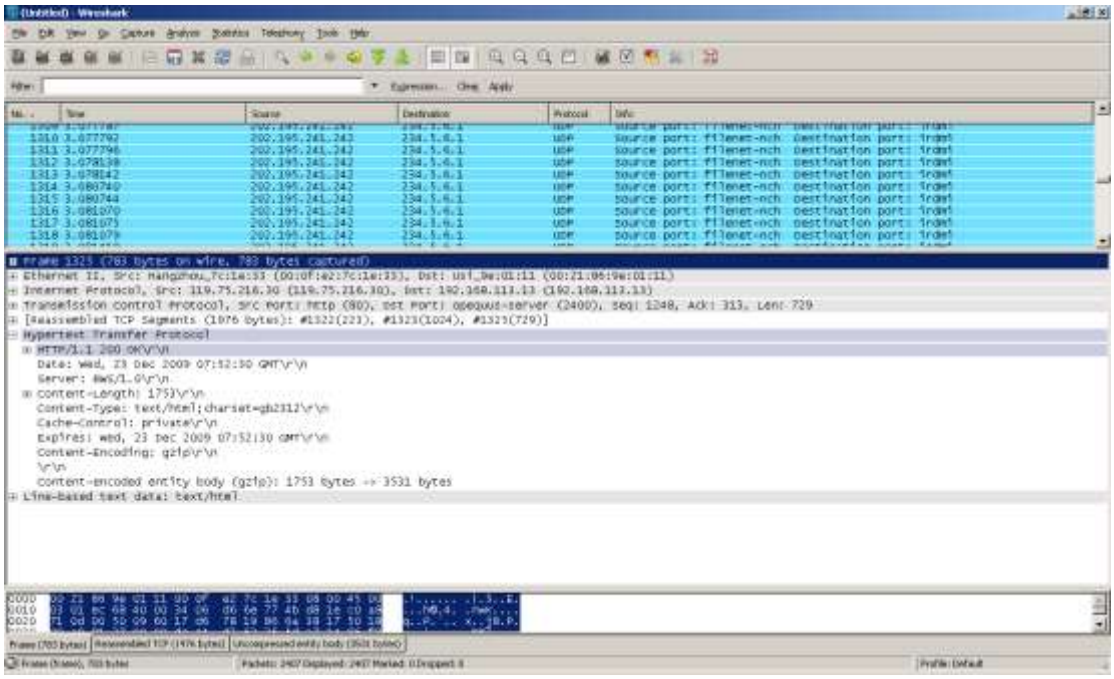
3．点击“Start”按钮开始捕获数据包。

4. 打开 IE 浏览器，在地址栏中输入“www.baidu.com”，待全部信息显示完毕后点击 “Stop”按钮停止捕获。

5．保存或记录捕获的数据包。

6．分析 HTTP 协议。

7．实验结果参考。



五、实验总结

通过实验了解 HTTP 的工作过程。在实验报告中需要回答以下问题：

1．根据实验数据，分析 HTTP 的操作过程以及各项信息的含义。

2．如何观察访问网站时，客户机与服务器之间传送的 cookie 信息。