实验 4：利用 Wireshark 进行协议分析

1120310415

王龙华

## 实验目的

熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间进行交互以 及报文交换的情况。

## 实验环境

Windows 9x/NT/2000/XP/2003  与因特网连接的计算机网络系统  Wireshark

## HTTP 分析

1. **HTTP GET/response**

**过程：**

交互启动 Web browser，然后启动 Wireshark分组嗅探器。在窗口的显示过滤说明处输入“http”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。开始 Wireshark 分组俘获。在打开的Web browser窗口中输入一下地址：http://hitgs.hit.edu.cn/news停止分组俘获。

**问题：**

你的浏览器运行的是 HTTP1.0，还是 HTTP1.1？

Request Version: HTTP/1.1

你所访问的服务 器所运行 HTTP 协议的版本号是多少？

Request Version: HTTP/1.1

你的浏览器向服务器指出它能接收何种语言版本的对象？

Accept-Language: zh-CN,zh;q=0.8\r\n（倾向于接受简体中文）

你的计算机的 IP 地址是多少？

172.17.25.248

服务器 http://hitgs.hit.edu.cn/news 的 IP 地址是多少？

219.217.227.106

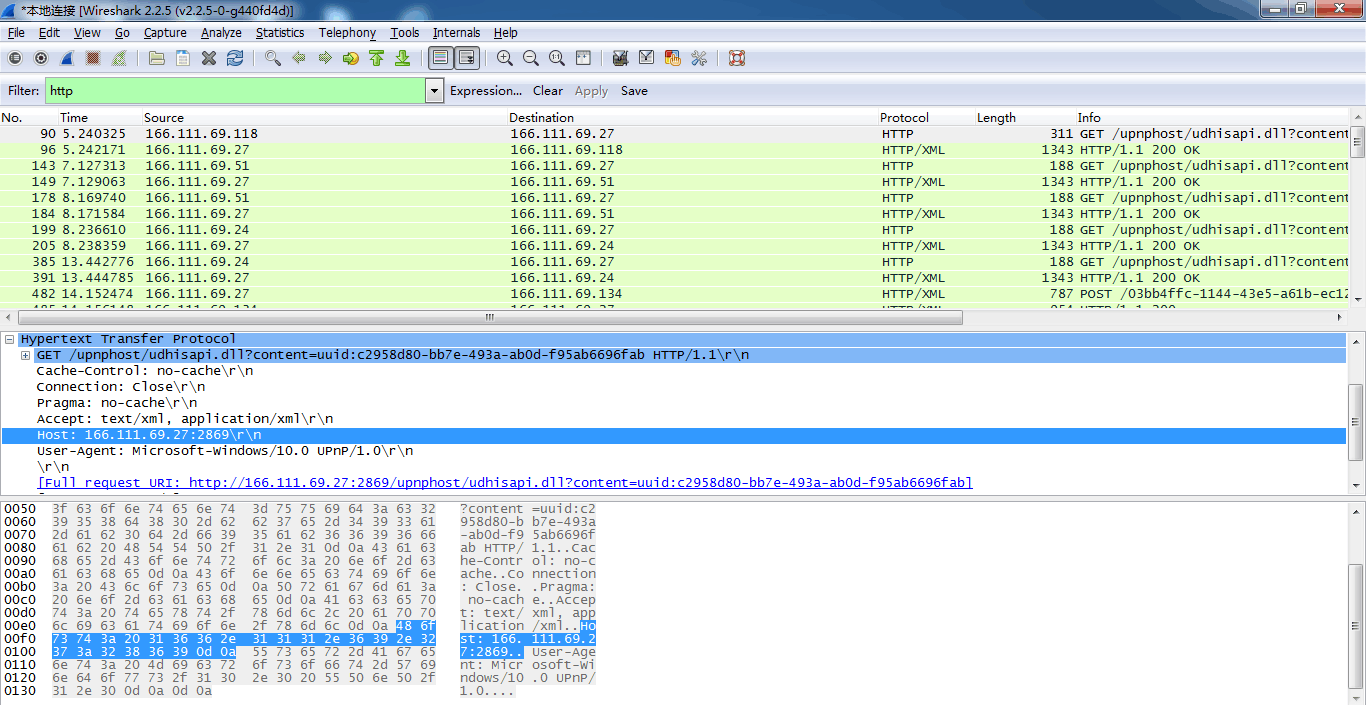
从服务器向你的浏览器返回的状态代码是多少？

Status Code: 200

1. **HTTP 条件 GET/response 交互**

**过程：**

启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单 中的“Internet 选项”命令，在出现的对话框中，选择“删除文件”）。启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。在浏览器的地址栏中输入以下URL: http://hitgs.hit.edu.cn/news,在你的浏览器中重新输入相同的 URL 或单击浏览器中的“刷新”按钮。停止Wireshark 分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的 HTTP 报文。



**问题：**

分析你的浏览器向服务器发出的第一个 HTTP GET 请求的内容， 在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？

没有（因为缓存清空了要接收网页内容）

分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？

Status Code: 200

Content-Length: 32671\r\n

服务器发出状态码200而且发出了内容长度信息，可见服务器明确要返回文件内容

分析你的浏览器向服务器发出的较晚的“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？

If-Modified-Since: Wed, 02 Jul 2014 03:07:41 GMT\r\n

有，后面跟着该数据上次更新的时间。

服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是多少？

Status Code: 304

服务器是否明确返回了文件的内容？

没有返回

Response Phrase: Not Modified

## TCP 分析

**过程：**

A. 俘获大量的由本地主机到远程服务器的 TCP 分组 （1） 启动浏览器，打开http://gaia.cs.umass.edu/Wireshark-labs/alice.txt 网页，得到ALICE'S ADVENTURES IN WONDERLAND文本将该文件保存到你的主机上。（2） 打开http://gaia.cs.umass.edu/Wireshark-labs/TCP-Wireshark-file1.html，如图4-6所示，窗口如下图所示。在Browse按钮旁的文本框中 输入保存在你的主机上的文件ALICE'S ADVENTURES IN WONDERLAND的全名（含路径），此时不要按“Upload alice.txt file”按钮。图4-6 Wireshark-labs网页截图 （3） 启动Wireshark，开始分组俘获。 （4） 在浏览器中，单击“Upload alice.txt file”按钮，将文件上传到 gaia.cs.umass.edu服务器，一旦文件上传完毕，一个简短的贺 词信息将显示在你的浏览器窗口中。 （5） 停止俘获。

B. 浏览追踪信息 在显示筛选规则中输入“tcp”,可以看到在本地主机和服务器之间 传输的一系列 tcp 和 http 报文，你应该能看到包含 SYN 报文的三次握手。 也可以看到有主机向服务器发送的一个 HTTP POST 报文和一系列的 “http continuation”报文。

**问题：**

向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址和 TCP 端口号是多少？

IP：172.17.25.248

Port:13596

Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来 发送和接收 TCP 报文的端口号是多少？

IP：128.119.245.12

Port：80

客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号 （sequence number）是多少？在该报文段中，是用什么来标示该 报文段是 SYN 报文段的？

seq：0

标志位为1表示是syn报文段 标志位为0说明不是

服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段 中，Acknowledgement 字段的值是多少？Gaia.cs.umass.edu 服务器 是如何决定此值的？在该报文段中，是用什么来标示该报文段是 SYNACK 报文段的？

Seq = 0

Ack = 1

Syn 和ack的标志位都为1

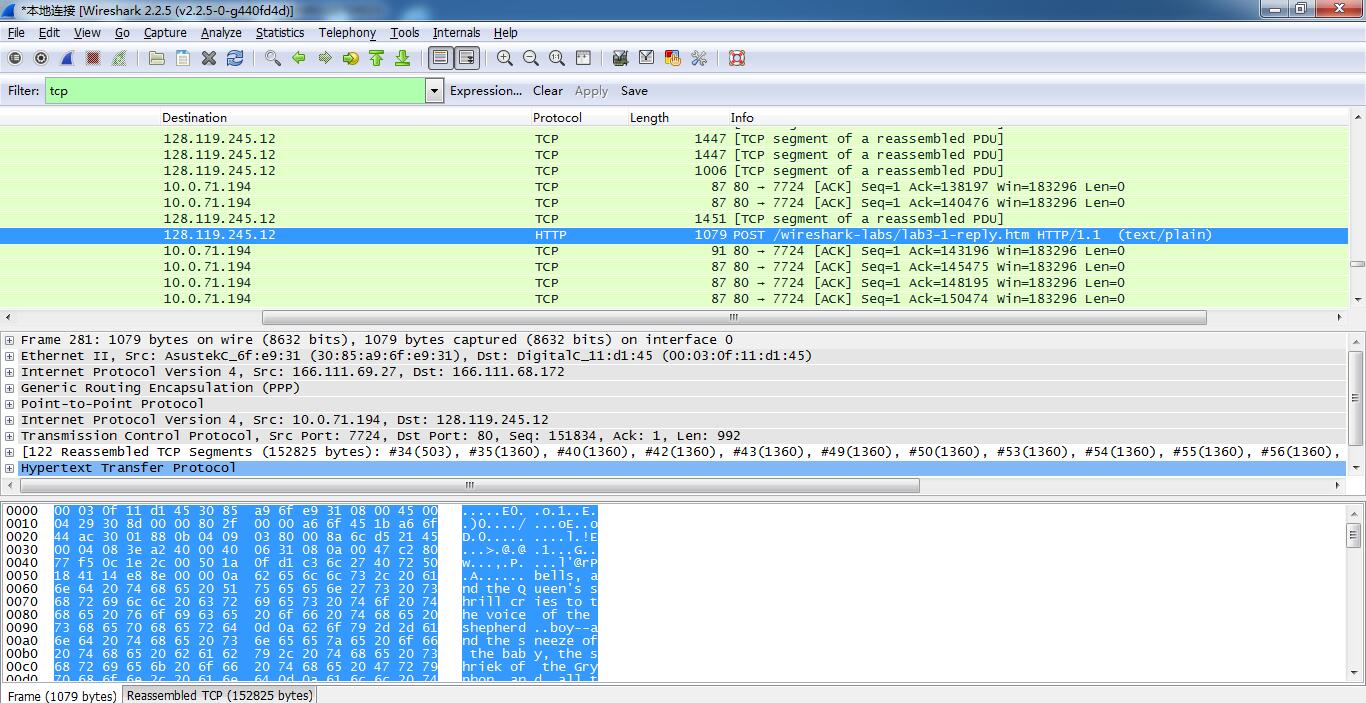
你能从捕获的数据包中分析出 tcp 三次握手过程吗？

第一次握手：seq = 0 syn标志位为1(意味着不能携带数据)

第二次握手：ack = 1（0+1） seq = 0 syn和ack标志位为1

第三次握手：seq = 1 ack = 1（0+1） ack标志位为1

包含 HTTP POST 命令的 TCP 报文段的序号是多少？



Seq = 1(我看到的是151834)

如果将包含 HTTP POST 命令的 TCP 报文段看作是 TCP 连接上的 第一个报文段，那么该 TCP 连接上的第六个报文段的序号是多少？是何时发送的？该报文段所对应的 ACK 是何时接收的？

4

3.23

3.24

前六个 TCP 报文段的长度各是多少？

483

1480

1480

1480

1480

1480

在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？ 限制发送端的传输以后，接收端的缓存是否仍然不够用？

在第六个ack报文段中看出接收窗口最小为65251所以可用缓存空间最小为64087 发送窗口16425 小于接收窗口所以没有受到限制

在跟踪文件中是否有重传的报文段？进行判断的依据是什么？

没有，seq 无重复

TCP 连接的 throughput (bytes transferred per unit time)是多少？

1496\*3/（2.488325000-2.488311000）/8 = 40071428.58 bytes/s

## **IP 分析**

**过程：**

通过分析执行 traceroute 程序发送和接收到的 IP 数据包，我们将研 究 IP 数据包的各个字段，并详细研究 IP 分片。 A. 通过执行 traceroute 执行捕获数据包 为了产生一系列 IP 数据报，我们利用 traceroute 程序发送具有不同 大小的数据包给目的主机 X。回顾之前 ICMP 实验中使用的 traceroute 程 序，源主机发送的第一个数据包的 TTL 设位 1，第二个为 2，第三个为 3， 等等。每当路由器收到一个包，都会将其 TTL 值减 1。这样，当第 n 个 数据包到达了第 n 个路由器时，第 n 个路由器发现该数据包的 TTL 已经 过期了。根据 IP 协议的规则，路由器将该数据包丢弃并将一个 ICMP 警 告消息送回源主机。 在Windows 自带的tracert命令不允许用户改变由 tracert 命令发送的 ICMP echo 请求消息（ping 消息）的大小。一个更优秀的 traceroute 程序 是 pingplotter，下载并安装 pingplotter。ICMP echo 请求消息的大小可以 通过下面方法在 pingplotter 中进行设置。Edit->Options->Packet，然后填写 Packet Size(in bytes，default=56)域。实验步骤： （1） 启动 Wireshark 并开始数据包捕获 （2） 启动pingplotter并“Address to Trace Window”域中输入目的地址。 在“# of times to Trace”域中输入“3”，这样就不过采集过多的数据。 Edit->Options->Packet，将 Packet Size(in bytes,default=56)域设为 56，这 样将发送一系列大小为 56 字节的包。然后按下“Trace”按钮。得到的 pingplotter 窗口如图 4-7 所示。

图 4-7 pingplotter 窗口 （1） Edit->Options->Packet，然后将 Packet Size(in bytes,default=56) 域改为 2000，这样将发送一系列大小为 2000 字节的包。然后按下 “Resume”按钮。 （2） 最后，将 Packet Size(in bytes,default=56)域改为 3500，发送一 系列大小为 3500 字节的包。然后按下“Resume”按钮。 （3） 停止 Wireshark 的分组捕获。 注：如无法访问可与实验 TA 联系，下载已有的 ip-Wireshark-trace 文件，利用该文件进行 IP 协议分析

B. 对捕获的数据包进行分析 （1）在你的捕获窗口中，应该能看到由你的主机发出的一系列ICMP Echo Request包和中间路由器返回的一系列ICMP TTL-exceeded消息。选 择第一个你的主机发出的ICMP Echo Request消息，在packet details窗口 展开数据包的Internet Protocol部分，如图4-8所示。

**问题：**

你主机的IP地址是什么？

172.17.25.248

在IP数据包头中，上层协议（upper layer）字段的值是什么？

Protocol: ICMP (1)

IP头有多少字节？该IP数据包的净载为多少字节？并解释你是怎样确定

该IP数据包的净载大小的？

Header Length: 20 bytes

Total Length: 56

56-20-8=28

该IP数据包分片了吗？解释你是如何确定该P数据包是否进行了分片

没分片因为total length = 56

（2）单击Source列按钮，这样将对捕获的数据包按源IP地址排序。 选择第一个你的主机发出的ICMP Echo Request消息，在packet details窗 口展开数据包的Internet Protocol部分。在“listing of captured packets”窗口， 你会看到许多后续的ICMP消息（或许还有你主机上运行的其他协议的数 据包）

**问题：**

你主机发出的一系列ICMP消息中IP数据报中哪些字段总是发生改变？

Seq

Ttl

Identification

哪些字段必须保持常量？哪些字段必须改变？为什么？

不变:ID

变化:Seq Ttl Identification

身份不变

数据编号递增

ttl要递增测经过路由器的跳数

IP软件维持一个计数器没产生一个数据包就加1并付给标示字段

描述你看到的IP数据包Identification字段值的形式。

Identification: 0x7ebb (32443)

（3）找到由最近的路由器（第一跳）返回给你主机的ICMP Time-to-live exceeded消息。

**问题：**

Identification字段和TTL字段的值是什么？

Identification: 0xe6e2 (59106)

Time to live: 236

最近的路由器（第一跳）返回给你主机的ICMP Time-to-live exceeded消息中这些值是否保持不变？为什么？

Identification:变化 每一次都根据计数器变化

Time to live: 要长

（4）单击Time列按钮，这样将对捕获的数据包按时间排序。找到在 将包大小改为2000字节后你的主机发送的第一个ICMP Echo Request消 息。

**问题：**

该消息是否被分解成不止一个IP数据报？

分解了

观察第一个IP分片，IP头部的哪些信息表明数据包被进行了分片？IP头部的哪些信息表明数据包是第一个而不是最后一个分 片？该分片的长度是多少

Fragment offset

Fragment count区分是第一还是最后

1456

C. 找到在将包大小改为3500字节后你的主机发送的第一个ICMP Echo Request消息。

**问题：**

原始数据包被分成了多少片？

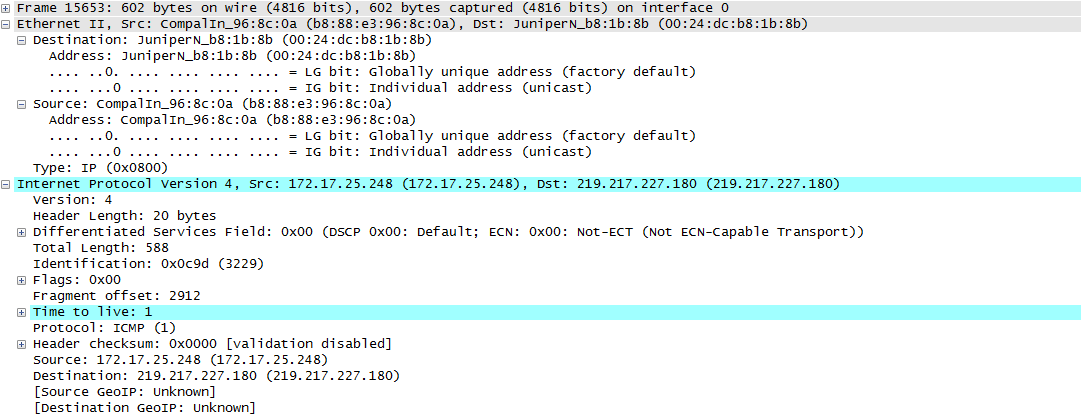
3片

这些分片中IP数据报头部哪些字段发生了变化？

Fragment offset

Fragment count

## 以太网数据帧分析



由上图可知以太网数据帧的Arrival Time: Jun 6, 2015 21:08:13.415229000 中国标准时间

帧数Frame Number: 15653

帧长Frame Length: 602 bytes (4816 bits)

目的mac Destination: JuniperN\_b8:1b:8b (00:24:dc:b8:1b:8b)

源mac Source: CompalIn\_96:8c:0a (b8:88:e3:96:8c:0a)

类型 Type: IP (0x0800)

版本Version: 4

头长Header Length: 20 bytes

总长Total Length: 588

服务类型域Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

标示域Identification: 0x0c9d (3229)

偏移量Fragment offset: 2912

生存时间Time to live: 1

协议域Protocol: ICMP (1)

头部校验和Header checksum: 0x0000 [validation disabled]保证头部完整性

源ip Source: 172.17.25.248 (172.17.25.248)

目的ip Destination: 219.217.227.180 (219.217.227.180)

数据长度Data (3472 bytes)

## ARP分析

**过程：**

（1）利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机 上 ARP 缓存的内容。 （2）在命令行模式下输入：ping 192.168.1.82（或其他 IP 地址） （3）启动 Wireshark，开始分组俘获。抓取的数据包大致如下图 4-9 所示。

图 4-9 ARP 广播包 从 Wireshark 的第一栏中，我们看到这是个 ARP 解析的广播包，如 上图。由于这个版本的 Wireshark 使用的是 Ethernet II 来解码的，我们先 看看 Ethernet II 的封装格式。如图 4-10 所示。

图 4-10 Ethernet II 的封装格式 从 Ethernet II 知道了是 ARP 解析以后，我们来看看 Wireshark 是如 何判断是 ARP 请求呢还是应答的。 以太网的 ARP 请求和应答的分组格式，如图 4-11 所示。

图 4-11 ARP 请求和应答的分组格式 从上图中我们了解到判断一个ARP 分组是ARP 请求还是应答的字 段是“OP”，当其值为 0×0001 时是请求，为 0×0002 时是应答。如下两

**问题：**

利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机 上 ARP 缓存的内容。说明 ARP 缓存中每一列的含义是什么?

Internet 地址 物理地址 类型

172.17.25.3 78-84-3c-b4-f6-44 动态

172.17.25.4 74-d0-2b-61-4c-2d 动态

172.17.25.10 3c-97-0e-fa-b2-d0 动态

172.17.25.24 f0-76-1c-a6-8d-fb 动态

172.17.25.73 74-46-a0-53-12-2e 动态

172.17.25.114 e0-db-55-a5-a5-e8 动态

172.17.25.144 20-1a-06-1c-38-a4 动态

172.17.25.146 dc-0e-a1-dc-3d-e2 动态

172.17.25.254 00-24-dc-b8-1b-8b 动态

224.0.0.22 01-00-5e-00-00-16 静态

224.0.0.100 01-00-5e-00-00-64 静态

224.0.0.253 01-00-5e-00-00-fd 静态

227.76.63.113 01-00-5e-4c-3f-71 静态

227.114.0.0 01-00-5e-72-00-00 静态

230.1.3.8 01-00-5e-01-03-08 静态

230.119.194.57 01-00-5e-77-c2-39 静态

236.36.37.43 01-00-5e-24-25-2b 静态

239.192.152.143 01-00-5e-40-98-8f 静态

239.255.255.239 01-00-5e-7f-ff-ef 静态

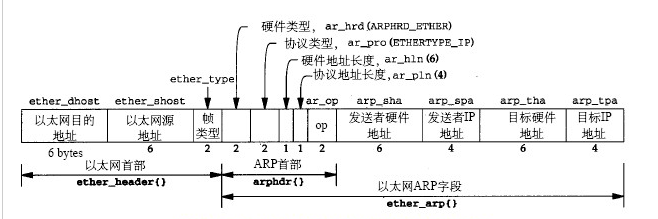
239.255.255.250 01-00-5e-7f-ff-fa 静态

239.255.255.251 01-00-5e-7f-ff-fb 静态

清除主机上 ARP 缓存的内容,抓取 ping 命令时的数据包。

**问题：**

ARP数据包的格式是怎样的？由几部分构成，各个部分所占的字 节数是多少？



如何判断一个ARP数据是请求包还是应答包？

Opcode: request (1)

为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明 确目的局域网地址的帧中传送？

主机发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机，并接收返回消息，以此确定目标的物理地址

响应要有明确地址是为了防止局域网内无线传送

## **UDP** 分析

**过程：**

（1）启动 Wireshark，开始分组捕获； （2）发送 QQ 消息给你的好友； （3）停止 Wireshark 组捕获； （4）在显示筛选规则中输入“udp”并展开数据包的细节，如图 4-14 所示。分析 QQ 通讯中捕获到的 UDP 数据包。

**问题：**

消息是基于UDP的还是TCP的？

Udp

你的主机ip地址是什么？目的主机ip地址是什么？

Source: 172.17.25.248 (172.17.25.248)

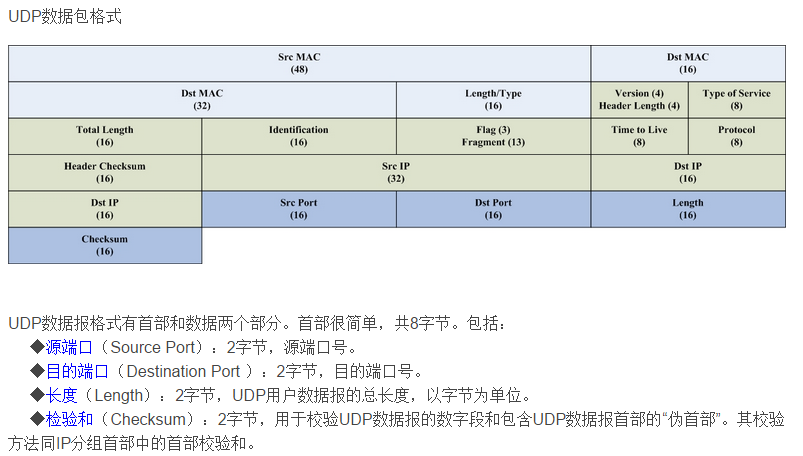
Destination: 182.254.1.37 (182.254.1.37)

你的主机发送QQ消息的端口号和QQ服务器的端口号分别是多 少？

Source Port: 4000 (4000)

Destination Port: 8000 (8000)

数据报的格式是什么样的？都包含哪些字段，分别占多少字节？



为什么你发送一个ICQ数据包后，服务器又返回给你的主机一个 ICQ数据包？这UDP的不可靠数据传输有什么联系？对比前面的 TCP协议分析，你能看出UDP是无连接的吗？

因为udp是不可靠连接 你不知道自己的信息有没有发送到服务器 这样本地软件就无法做出动作响应 当接收到服务器发送过来的信息时才知道自己的信息发送成功这时候客户端会做出发送成功的响应 而前面tcp连接就不需要进行反馈信息接收 可见 udp是无连接的。

## DNS 分析

**过程：**

（1）打开浏览器键入:www.baidu.com

（2）打开 Wireshark,启动抓包.

（3）在控制台回车执行完毕后停止抓包.Wireshark 捕获的

**协议分析：**

Destination: JuniperN\_b8:1b:8b (00:24:dc:b8:1b:8b)

Source: CompalIn\_96:8c:0a (b8:88:e3:96:8c:0a)

Type: IP (0x0800)

Version: 4

Header Length: 20 bytes

Total Length: 59

Identification: 0x4fae (20398)

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x0000 [validation disabled]

Source: 172.17.25.248 (172.17.25.248)

Destination: 114.114.114.114 (114.114.114.114)

Source Port: 58787 (58787)

Destination Port: 53 (53)

Checksum: 0xab26 [validation disabled]

报文的主要信息如上，从中可以看出的最重要信息是DNS服务器IP 114.114.114.114 port:53

是以UDP协议进行数据传输的