**《计算机网络》实验报告5**

利用Wireshark进行协议

**童超宇**

院 （系）：计算机科学与技术学院 专 业：计算机科学与技术

学　　号 ：1152130106 指导教师：刘亚维

**2018年5月**

# 目录

[1 实验目的 3](#_Toc876167027)

[2 实验内容 3](#_Toc585734057)

[3 实验过程 3](#_Toc697075922)

[3.1 HTTP分析(www.hit.edu.cn) 3](#_Toc2089933304)

[3.1.1 HTTP GET/response交互 3](#_Toc1640022211)

[3.1.2 HTTP条件GET/response交互 4](#_Toc1471254400)

[3.2 TCP分析 5](#_Toc172500763)

[3.3 IP分析 9](#_Toc636730649)

[3.4 ARP数据包 12](#_Toc1689612230)

[3.4.1 查看ARP缓存 12](#_Toc957203704)

[3.4.2 分析数据包 13](#_Toc1176166526)

[3.5 UDP数据包 14](#_Toc1542568212)

[3.6 DNS协议分析 15](#_Toc726211596)

# 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

# 实验内容

1)学习Wireshark的使用

2)利用Wireshark分析HTTP协议

3)利用Wireshark分析TCP协议

4)利用Wireshark分析IP协议

5)利用Wireshark分析Ethernet数据帧

选做内容：

a)利用Wireshark分析DNS协议

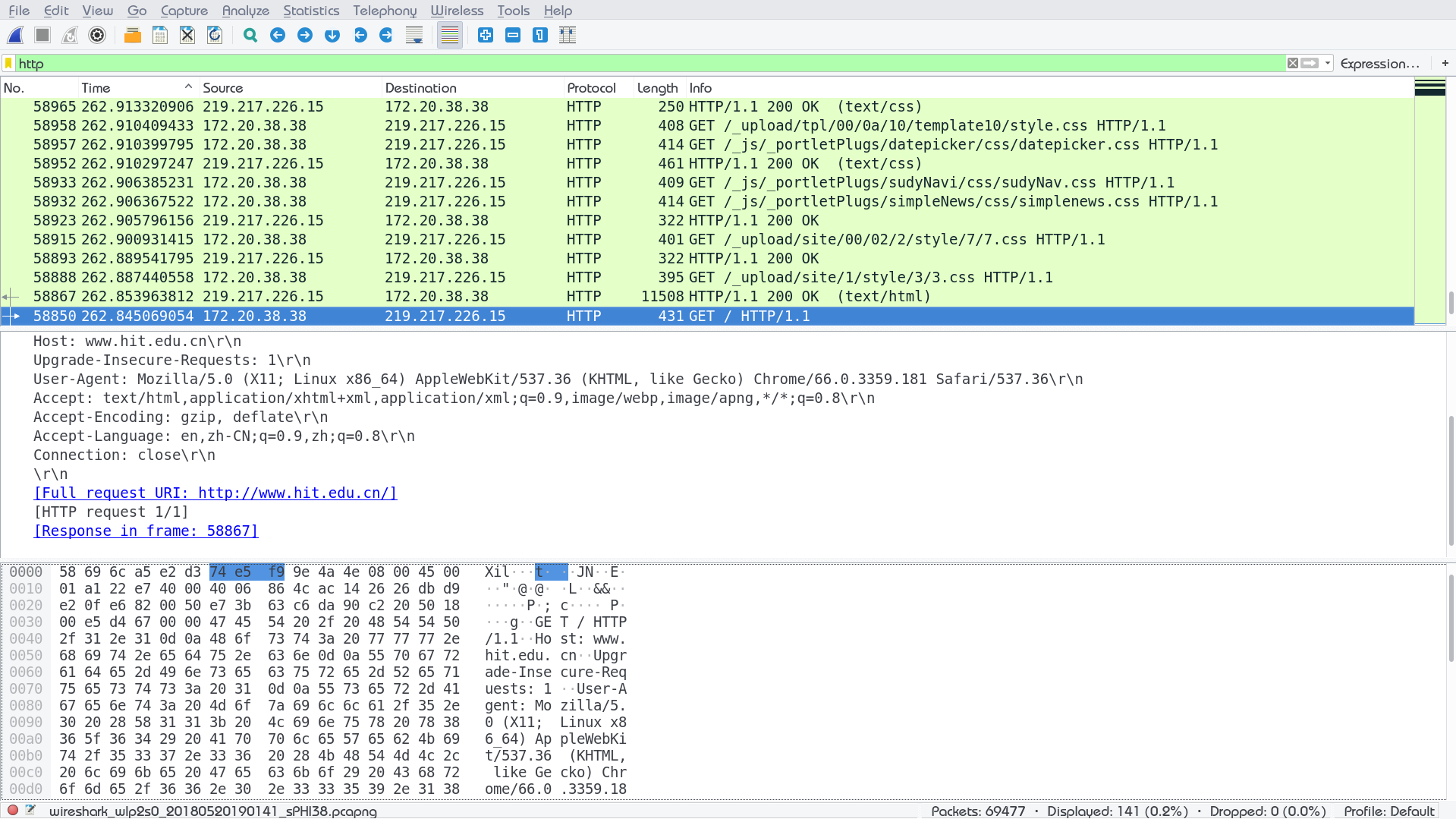
b)利用Wireshark分析UDP协议

c)利用Wireshark分析ARP协议

# 实验过程

## HTTP分析(www.hit.edu.cn)

### HTTP GET/response交互



1. 你的浏览器运行的是HTTP1.0，还是HTTP1.1？你所访问的服务器所运行HTTP协议的版本号是多少？



都是HTTP1.1

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？



en,zh-CN

1. 你的计算机的IP地址是什么？服务器http://www.hit.edu.cn的IP地址是多少？



本机172.20.38.38

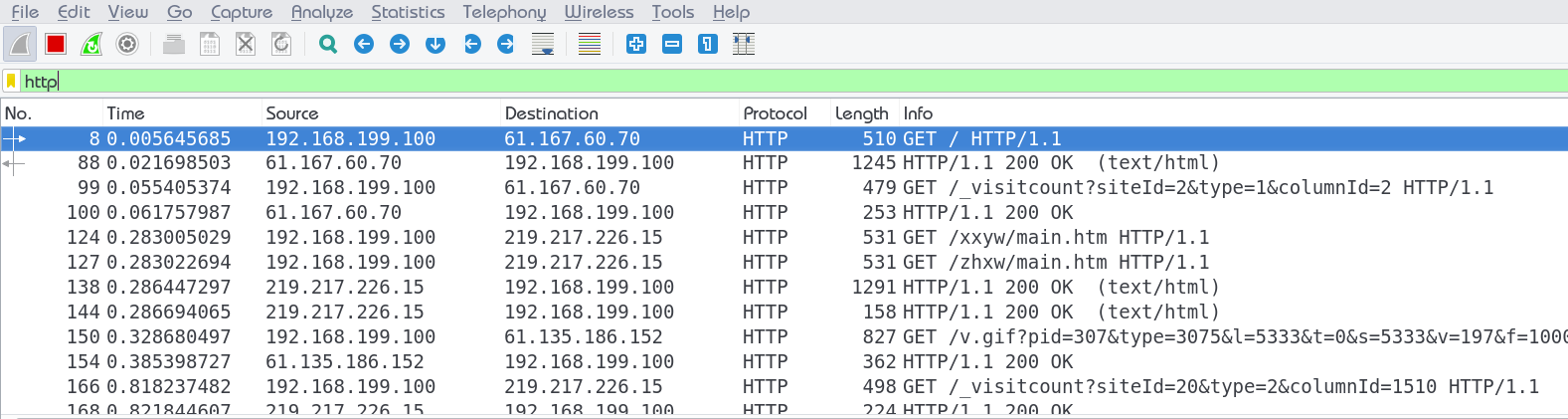
服务器219.217.226.15

1. 从服务器向你的浏览器返回的状态代码是多少？

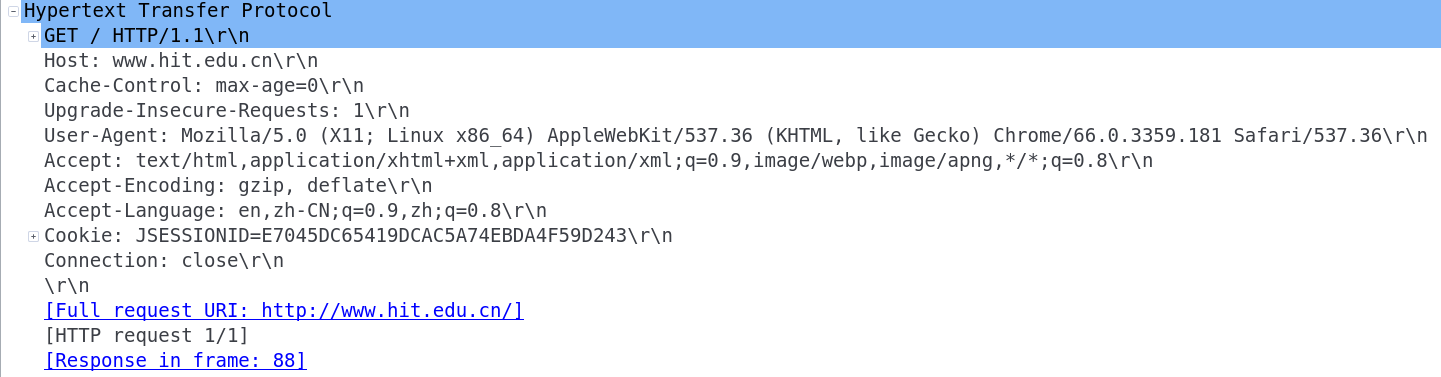
200



### HTTP条件GET/response交互

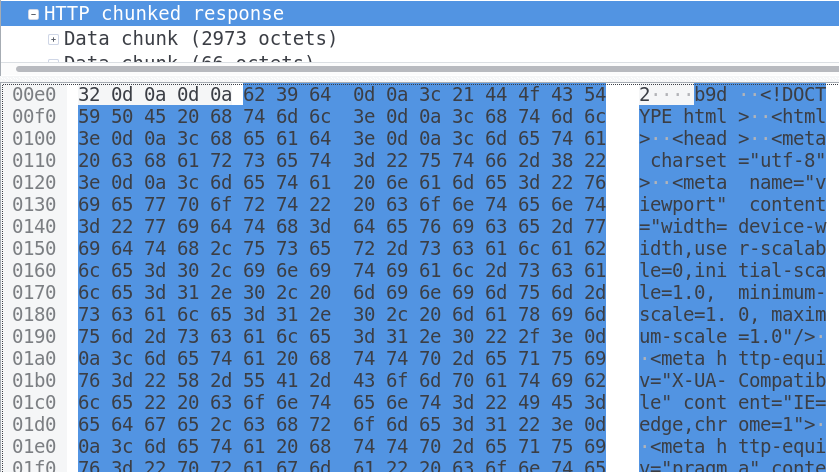


1. 分析你的浏览器向服务器发出的第一个HTTP GET请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE？



没有IF-MODIFIED-SINCE

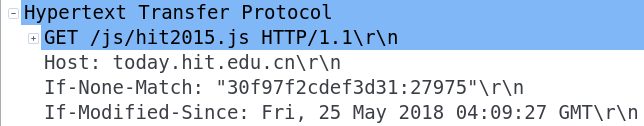
1. 分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？



服务器返回了文件内容

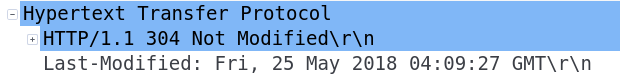
通过状态码判断，如304表示不返回内容，如200表示返回内容

1. 分析你的浏览器向服务器发出的较晚的“HTTPGET”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？



请求/js/hit2015.js文件时有IF-MODIFIED-SINCE，后面跟着的一般为上次响应中的Last-Modified

1. 服务器对较晚的HTTPGET请求的响应中的HTTP状态代码是多少？服务器是否明确返回了文件的内容？请解释。

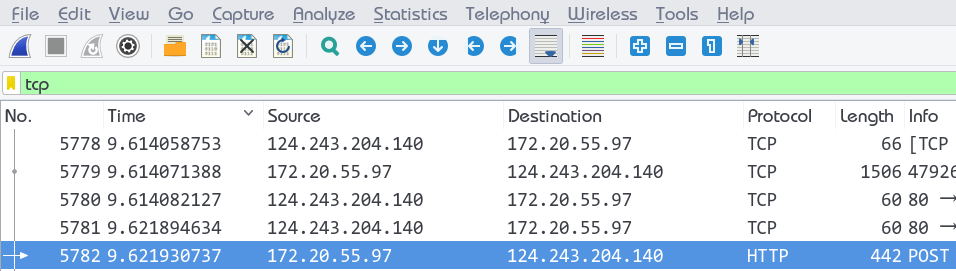


304，表示自从上次请求后，请求的网页未修改过

服务器返回此响应时，不会返回网页内容

## TCP分析

在http://en.miui.com/home.php?mod=spacecp&ac=avatar上传图片



1. 向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？



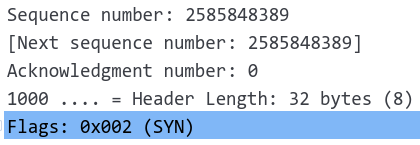
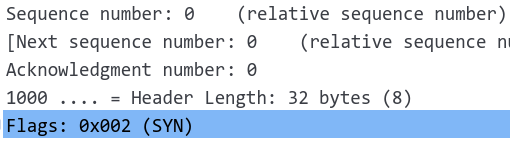
客户端ip 172.20.55.97，tcp端口47926

1. 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？



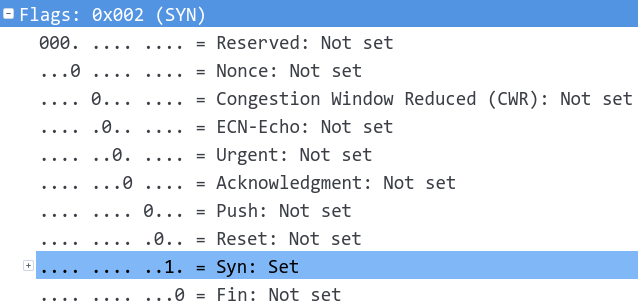
服务器ip 124.243.204.140，tcp端口80

1. 客户服务器之间用于初始化TCP连接的TCPSYN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？



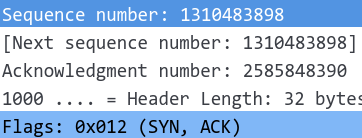
相对sequence number为0（左图）

实际sequence number为2585848389（右图）



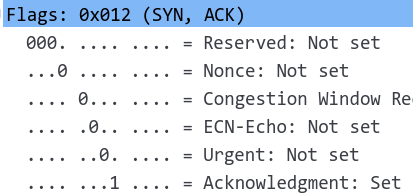
通过标志位中的syn置1来表示SYN报文段

1. 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？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？



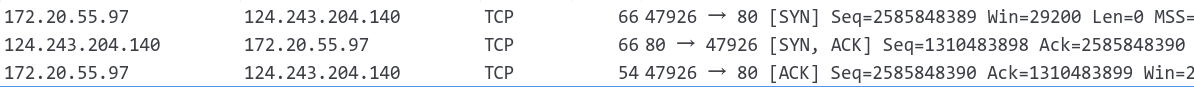
seq number为1310483898

ack number为2585848390，即发送端syn包的seq number+1



通过标志位中的ack字段置1来表示SYNACK报文段

1. 你能从捕获的数据包中分析出tcp三次握手过程吗？

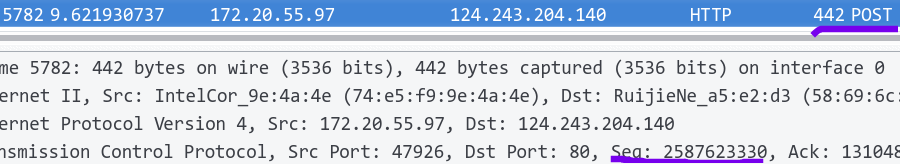


客户端向服务器发送seq=2585848389的SYN报文来请求建立连接

服务器向客户端返回seq=1310483898,ack=2585848390的SYNACK报文响应

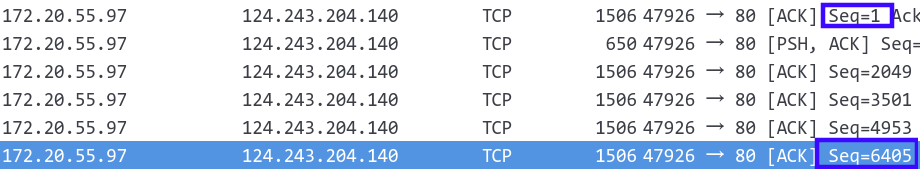
客户端向服务器发送seq=2585848390,ack=1310483899的ACK报文完成建立

1. 包含HTTP POST命令的TCP报文段的序号是多少？



Seq=2587623330，相对1774941

1. 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？



第六个报文段相对Seq=6405

它在http post结束前，tcp连接建立后发送，时间戳

对应ack如下，ack=6405



时间戳

1. 前六个TCP报文段的长度各是多少？



长度如上图所示，如第一个为1452字节

1. 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？

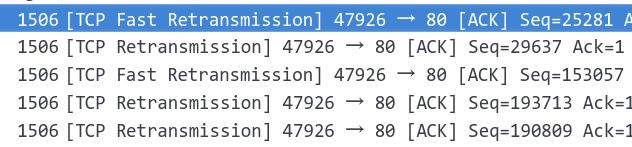


通过window size value可知接收端公示的最小可用缓存空间是29200字节

该窗口大小会一直增加，不会出现接收端的缓存不够用问题

1. 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？

有重传



利用tcp.analysis.retransmission过滤得到如上的重传报文

通过序列号是否与已发送序列号重复来判断是否是重传

1. TCP连接的throughput(bytes transferred per unit time)是多少？请写出你的计算过程



共发送1775328字节（1.69M）



发送端握手后第一个包发送时间

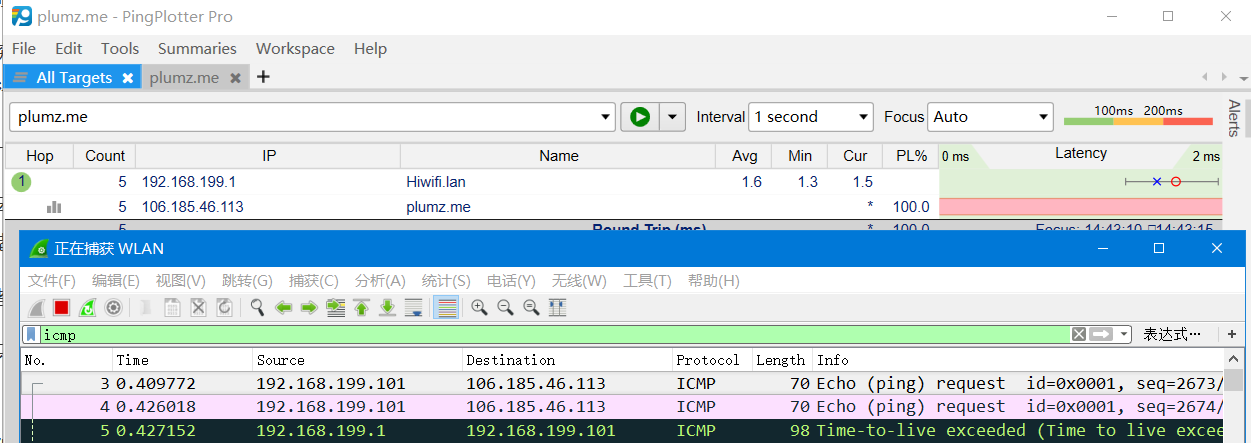
最后一个包发送时间

时间总计3159ms

吞吐量为1775328B/3159ms=4.28Mbps

## IP分析

向plumz.me发ping

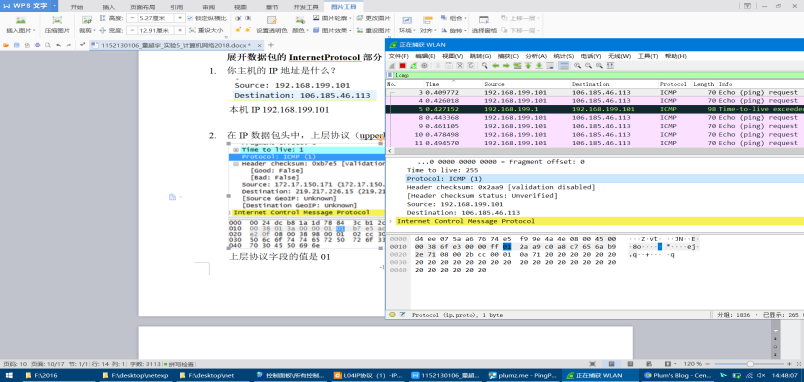


1. **选择第一个你的主机发出的ICMP Echo Request消息，在packet details窗口展开数据包的Internet Protocol部分**
2. 你主机的IP地址是什么？



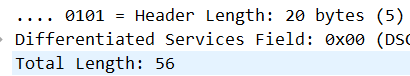
本机IP 192.168.199.101

1. 在IP数据包头中，上层协议（upper layer）字段的值是什么？



上层协议字段的值是01，表示ICMP协议

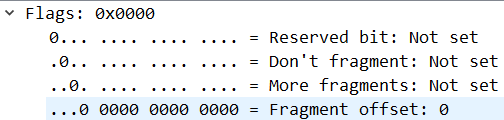
1. IP头有多少字节？该IP数据包的净载为多少字节？并解释你是怎样确定该IP数据包的净载大小的？



IP头有20字节，总长56字节

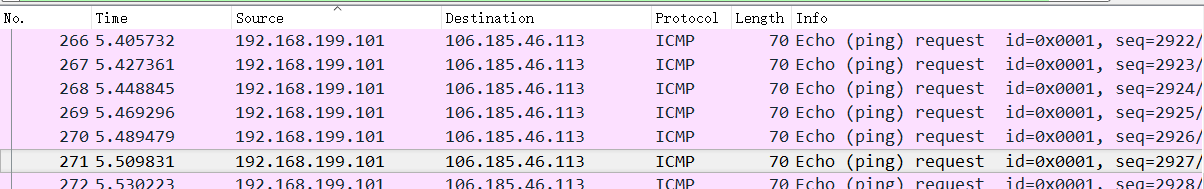
净载为Total Length-Header Length=56B-20B=36B

1. 该IP数据包分片了吗？解释你是如何确定该IP数据包是否进行了分片



没有，因为More fragments为0，且Fragment offest为0，表示无分片

1. **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ICMPEchoRequest消息，在packetdetails窗口展开数据包的InternetProtocol部分。在“listingofcapturedpackets”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）**



1. 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？

id，ttl，header checksun

1. 哪些字段必须保持常量？哪些字段必须改变？为什么？

id必须改变：identification是标识，用于区分不同的数据包

ttl必须改变：来自于traceroute的要求，用来测试路径上的路由信息

header checksum必须改变：首部校验和，由于id与ttl字段变化，需要重新计算header checksum

其他字段保持常量

1. 描述你看到的IP数据包Identification字段值的形式

16位，+1递增，如下图所示

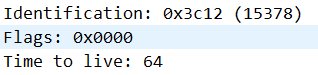




1. **找到由最近的路由器（第一跳）返回给你主机的ICMPTime-to-liveexceeded消息**



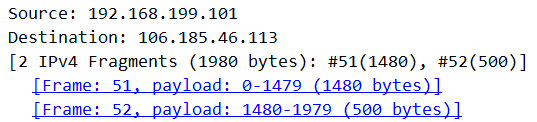
1. Identification字段和TTL字段的值是什么？



1. 最近的路由器（第一跳）返回给你主机的ICMPTime-to-liveexceeded消息中这些值是否保持不变？为什么？

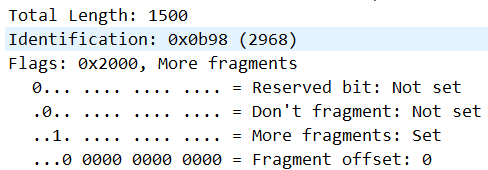
不变，因为给同一个主机返回的ICMP报文的标识不代表序号，所以TTL消息是相同的，因此Identification也不变

1. **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**
2. 该消息是否被分解成不止一个IP数据报？



是，分成了两个

1. 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

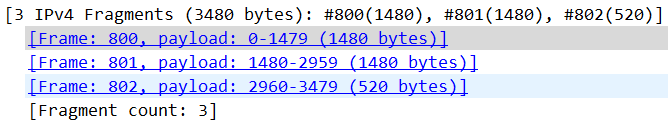


MF=1或位移>0表示进行了分片

MF=1且位移=0表示分片是第一个而不是最后一个

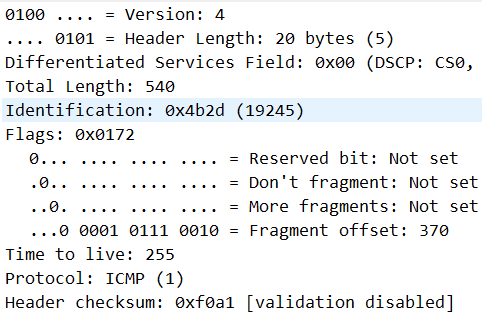
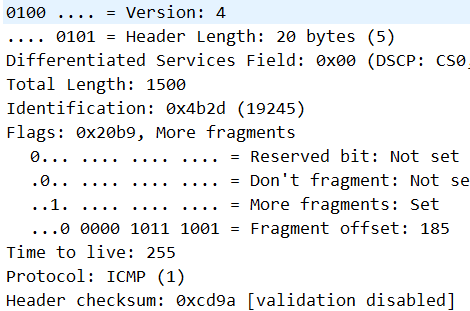
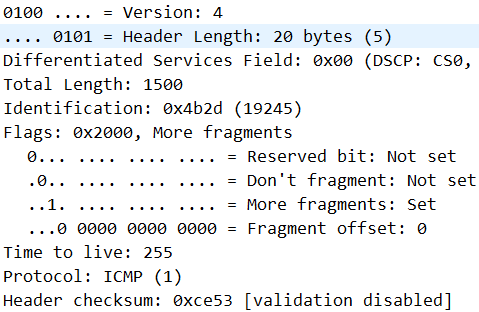
该分片的长度是1500B（total length）

1. **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**
2. 原始数据包被分成了多少片？



分成了三片

1. 这些分片中IP数据报头部哪些字段发生了变化？



从左到右为三个分片

前2个分片MF=1，第3个为0

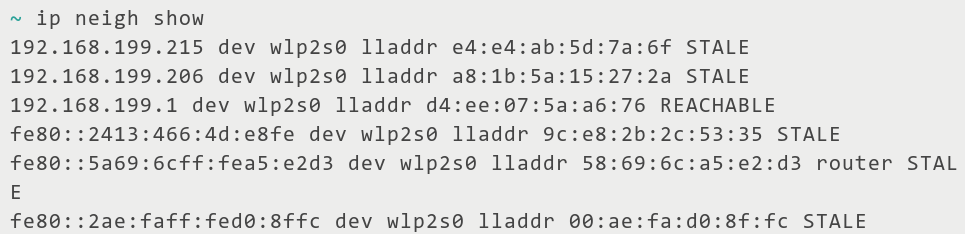
前2个分片total length=1500，第3个为540

片偏移与header checksum也是变化的，其他不变

## ARP数据包

### 查看ARP缓存

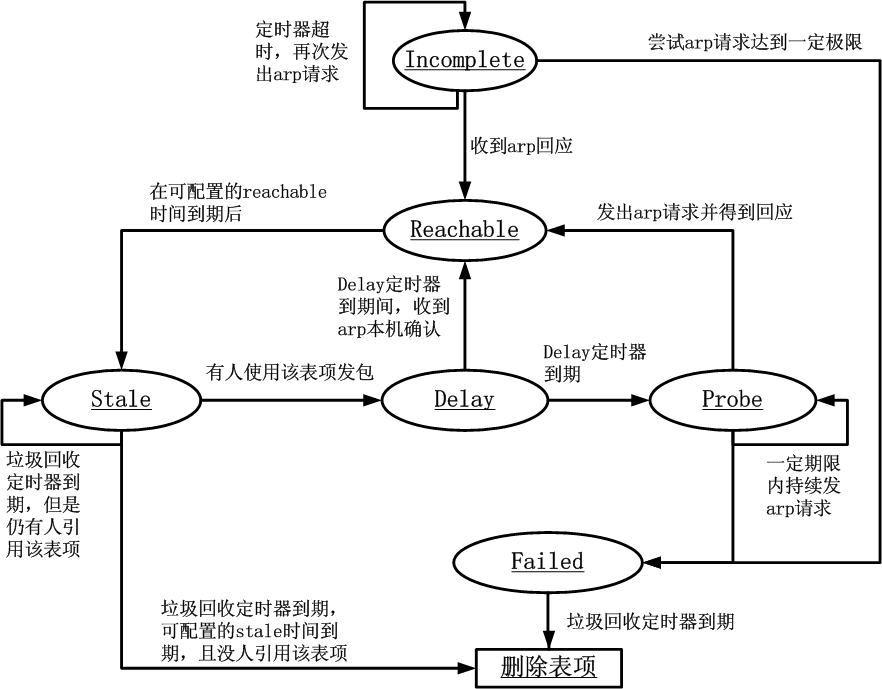
用ip neigh或arp（已弃用）查看ARP表



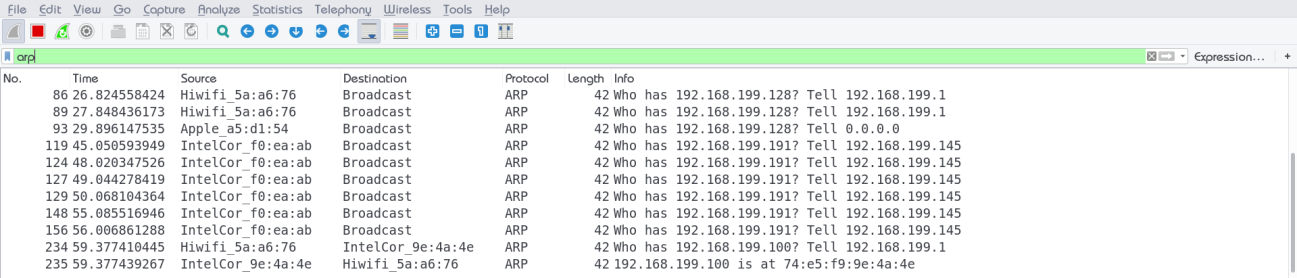
从左至右为ip（4/6），接口（网卡）名，链路层地址，状态

如第1条stale表示有效但可疑（已超时），第3条reachable表示有效且可信任（未超时）

它们的状态转换如下（https://blog.csdn.net/dog250/article/details/7251689）

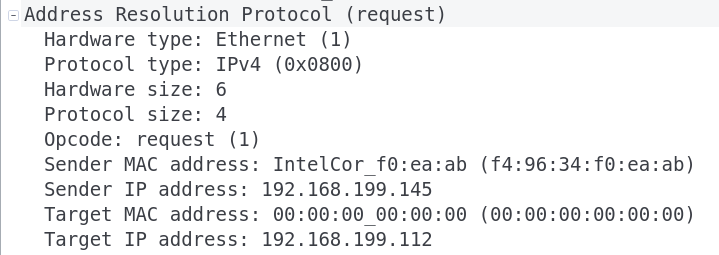


### 分析数据包



1. 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？

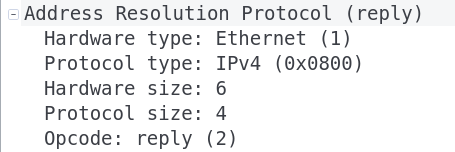
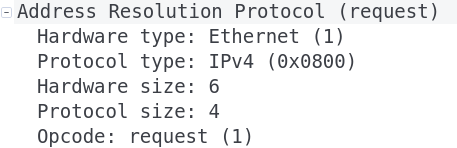
ARP数据包格式如下图：



如上图所示，由9部分构成，分别是硬件类型（2字节），协议类型（2字节），硬件地址长度（1字节），协议地址长度（1字节），OP（2字节)，发送端MAC地址（6字节），发送端IP地址（4字节），目的MAC地址（6字节），目的IP地址（4字节）



1. 如何判断一个ARP数据是请求包还是应答包？



OP字段值为0x0001时是请求包，为0x0002时是应答包

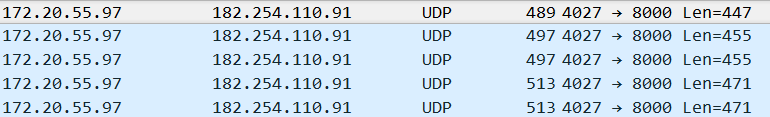
左图为请求包，右图为应答包

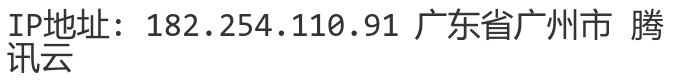
1. 为什么ARP查询要在广播帧中传送，而ARP响应要在一个有着明确目的局域网地址的帧中传送？

ARP查询时不知道目的IP地址对应的MAC地址，所以要广播

ARP响应报文知道查询主机的MAC地址（通过查询主机发出的查询报文获得），且局域网中的其他主机不需要此次查询的结果，所以要在一个有着明确目的局域网地址的帧中传送

## UDP数据包





1. 消息是基于UDP的还是TCP的？



UDP

1. 你的主机IP地址是什么？目的主机IP地址是什么？



本机IP：172.20.55.97

目的IP：182.254.110.91

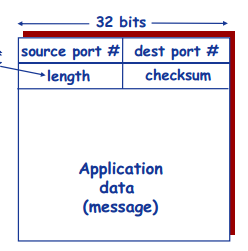
1. 你的主机发送QQ消息的端口号和QQ服务器的端口号分别是多少？

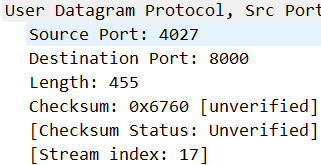


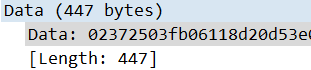
客户端端口号：4027

服务器端口号：8000

1. 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？

UDP数据报格式如下图：





由5部分构成，分别是源端口号（4字节），目的端口号（4字节），长度（4字节），校验和（4字节）和应用层数据

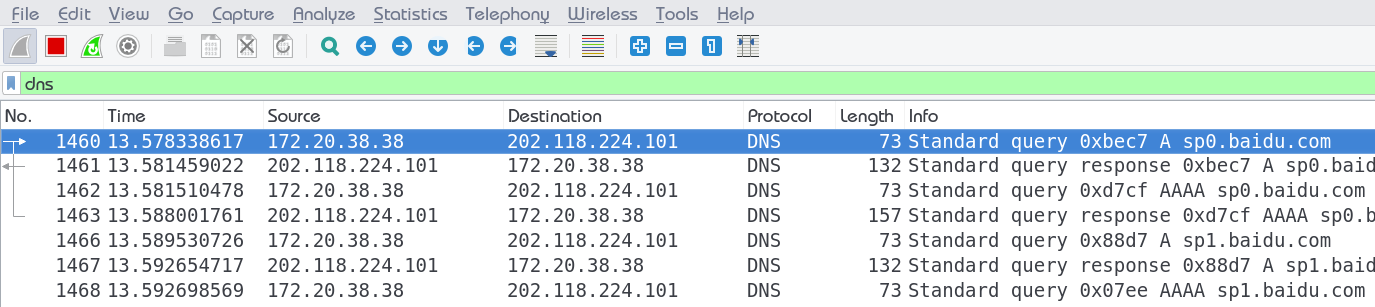
1. 为什么你发送一个ICQ数据包后，服务器又返回给你的主机一个ICQ数据包？这UDP的不可靠数据传输有什么联系？对比前面的TCP协议分析，你能看出UDP是无连接的吗？

服务器返回一个ICQ是起到ACK的作用，因为UDP是无连接的，所以服务器返回客户端一个ICO来确认收到

可以看出UDP是无连接的，因为UDP数据包没有序列号，每次只发送一个数据报，然后等待服务器响应，没有像TCP一样的握手过程

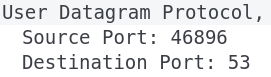
## DNS协议分析

1. 打开浏览器，输入[www.baidu.com,DNS](http://www.baidu.com,DNS)查询消息如下图：

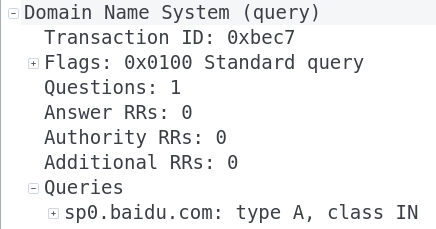


本机IP 172.20.38.38，本地域名服务器IP 202.118.224.101

1. UDP报文的源端口号46896，目的端口号53

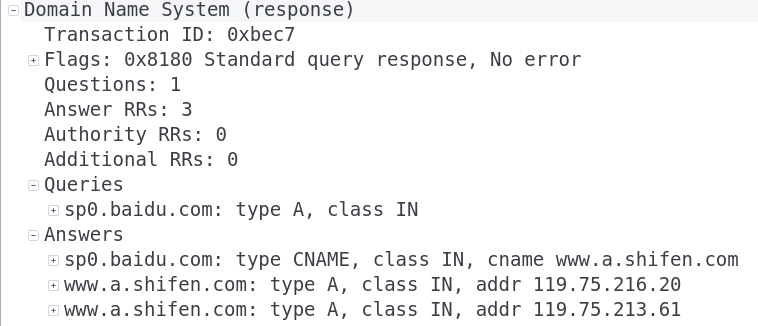


1. DNS查询报文内容如下



表示查询sp0.baidu.com的IP

1. DNS回复信息



这是一条cname记录，表示sp0.baidu.com被映射为www.a.shifen.com