



# 计算机网络实验三

## 互联网协议第四版 (IPv4)

信息学部 朱婉婷

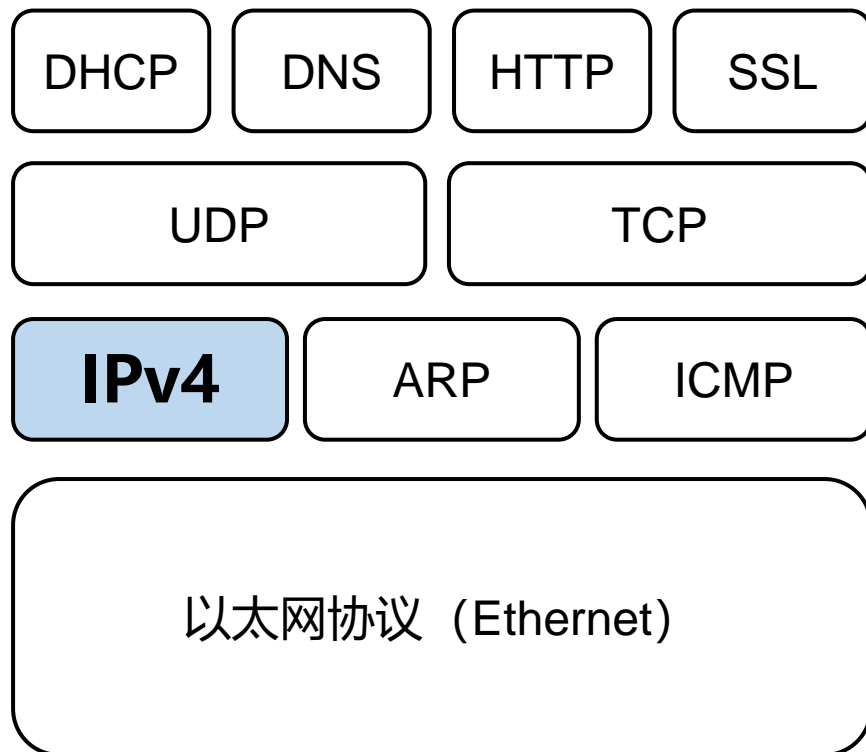
# 主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

# IP简介

## ◆网际互联协议 IP (Internet Protocol)

- IP是TCP/IP体系中两个最主要的协议之一。与IP协议配套使用的还有四个协议：
  - 地址解析协议 **ARP**
  - 逆地址解析协议 RARP
  - 网际控制报文协议 **ICMP**
  - 网际组管理协议 IGMP

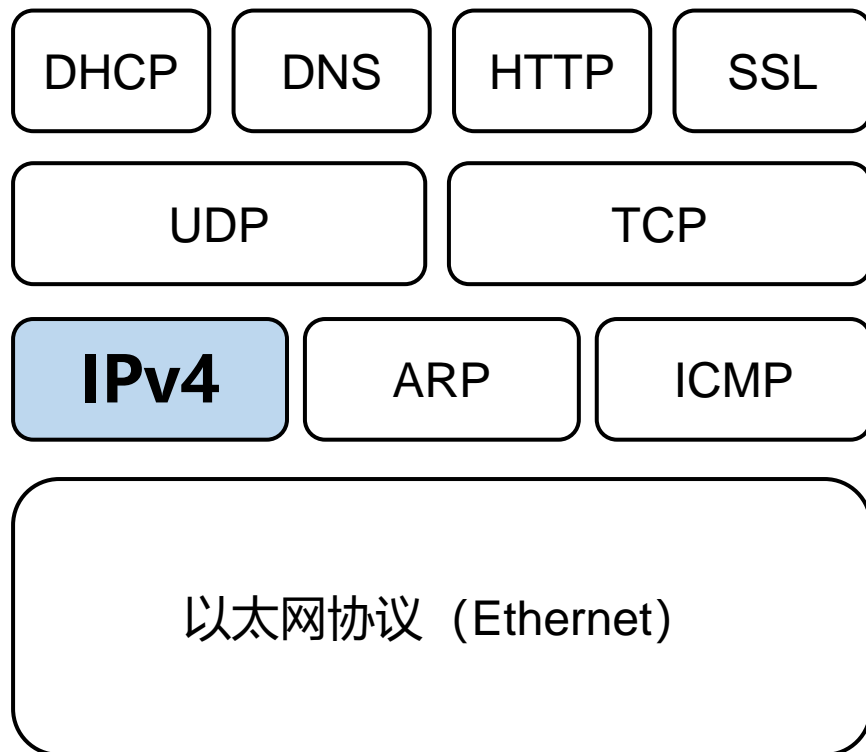


# IPv4简介

◆IPv4：指版本号为4的IP协议。

- IPv4协议，最主要特征是IP地址为32位。依然是目前惯常使用的IP协议。

- IPv6协议，指IP协议的版本号为 6。使用的IP地址为128位。



# IPv4数据报的格式

- 一个 IP 数据报由**首部**和**数据**两部分组成。
- IPv4数据报首部的前一部分是**固定部分**，共**20字节**，是所有 IPv4 数据报必须具有的。



# IPv4数据报的格式

- 在首部的固定部分的后面是一些**可选字段**，其长度是可变的。



# IPv4数据报的格式



版本：占 4 位，IPv4协议版本号为 4 (0100)

# IPv4数据报的格式



首部长度：占 4 位，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。

首部长度20字节 -> 5个单位 -> 0101



# IPv4数据报的格式



区分服务：占 8 位，用来获得更好的服务。分为DSCP和ECN两个字段。DSCP差分服务代码点，6比特，用来进行质量控制；ECN显式拥塞通告，2比特，用来报告网络拥堵情况。

# IPv4数据报的格式



总长度：占16位，指首部和数据之和的长度，单位为字节。  
总长度必须不超过最大传输单元MTU (以太网，1500字节)。

# IPv4数据报的格式



标识(identification)：占 16 位，它是一个计数器，用来产生数据报的标识，可用于分片重组。

# IPv4数据报的格式



标志(flag): 占 3 位, 目前只有两位有意义。

最低位是 **MF** (More Fragment),  $MF = 1$  表示后面 “还有分片”,  $MF = 0$  表示最后一个分片。

中间的一位是 **DF** (Don't Fragment), 只有当  $DF = 0$  时才允许分片。

# IPv4数据报的格式



片偏移：占13 位，指出分片后的某片在原分组中的相对位置。片偏移以 8 个字节为偏移单位。

# IPv4数据报的格式



生存时间：占8位，记为 TTL (Time To Live)  
数据报在网络中可通过的路由器数的最大值。

# IPv4数据报的格式



协议：占8位，指出此数据报携带的数据使用何种协议以便目的主机的IP层判断将数据部分上交给哪个处理过程

1: ICMP      2: IGMP      6: TCP      17: UDP

# IPv4数据报的格式



首部检验和：占16位，字段只检验数据报的首部  
不检验数据部分。



# IPv4数据报的格式



源地址、目的地址：各占 4 字节，32位。

# IPv4数据报的格式



- IP 首部的可变部分就是一个选项字段，可以用来支持排错、测量以及安全等措施，内容很丰富。
- 选项字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。

# 首部检验和计算方法

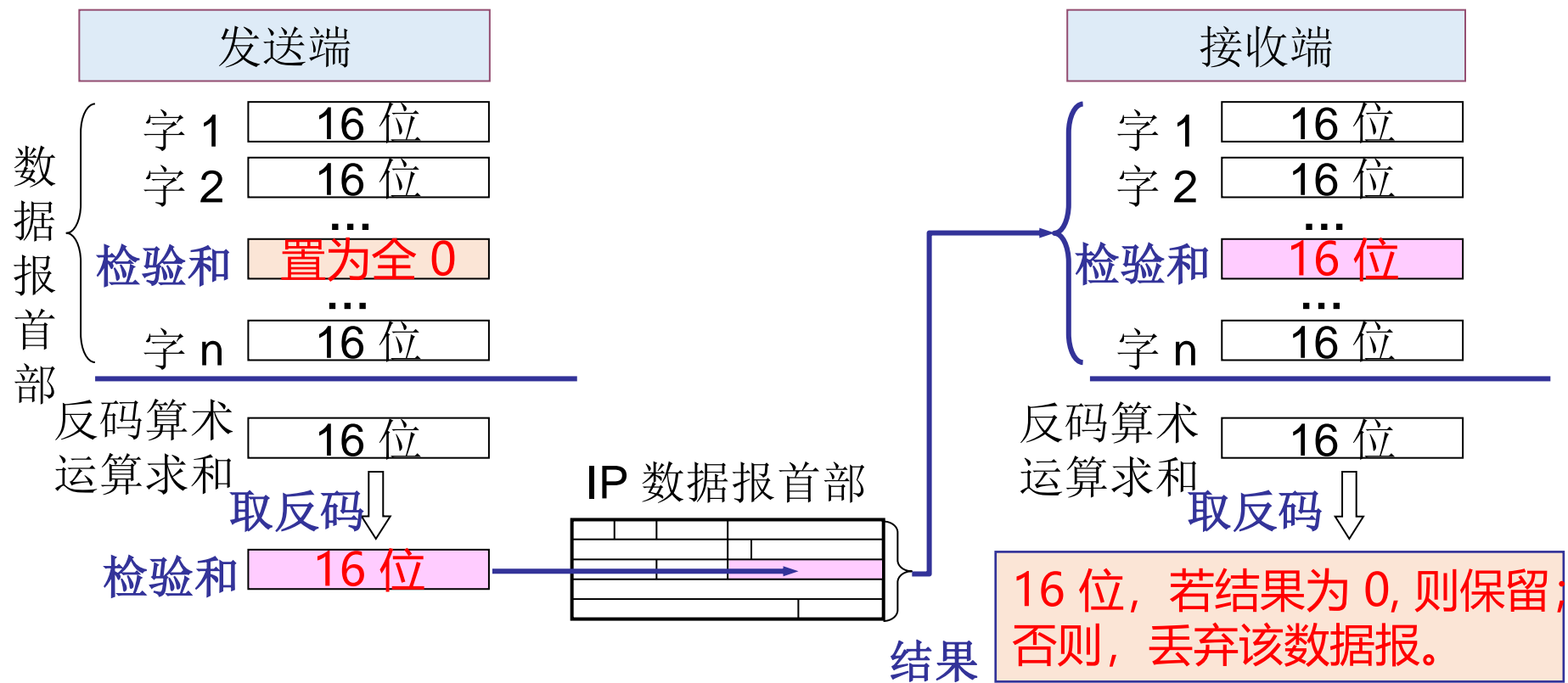
## ◆反码求和的基本计算方法：

- 0和0相加是0，0和1相加是1，1和1相加是0但要产生一个进位1，加到下一列。
- 若最高位相加后产生进位，则最后得到的结果要加1。

## ◆注意：数据部分不参与首部检验和的计算。

# 首部检验和计算方法

◆采用反码算术运算求和，和的反码作为首部校验和字段。



# 主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

# 实验环境搭建

列出本次实验所使用的平台和相关软件，以下为例：

(打开cmd指令窗口，输入指令 “ipconfig /all”查看)

- 1、主机：联想笔记本 (Win10系统) ； 主机IP地址：192.168.1.106； 子网掩码：255.255.255.0； 主机网卡MAC地址：34-F6-4B-C0-90-40。
- 2、网络连接方式：无线连接； 默认网关地址：192.168.1.1。
- 3、抓包工具：Wireshark (v3.6.2) 。

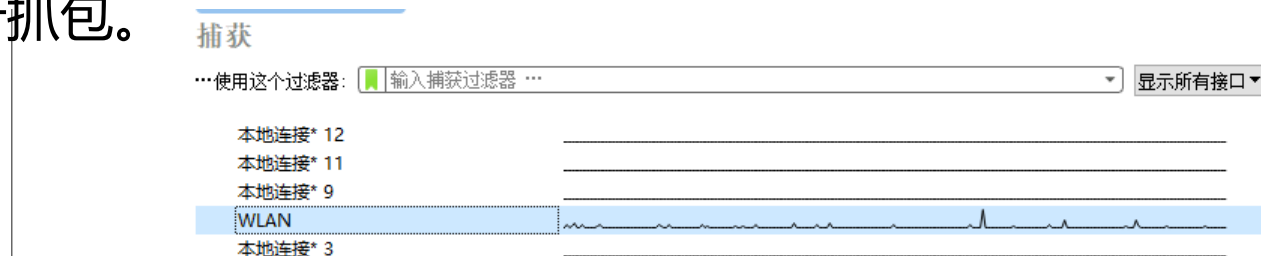
# 实验具体步骤

1、通过ping命令获取北京工业大学官网的IP地址。

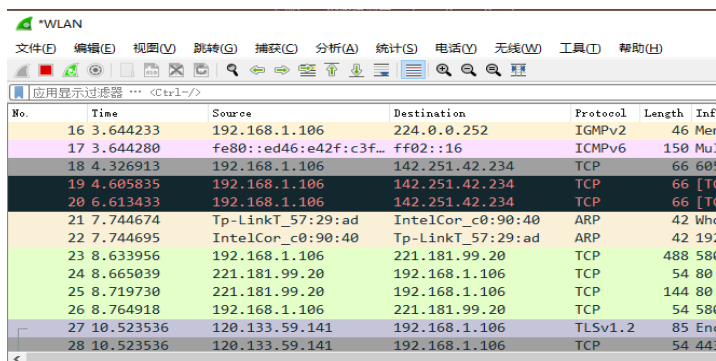
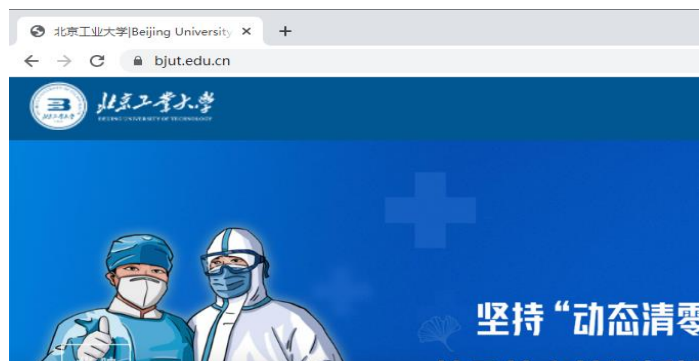
```
C:\Users\zwt717>ping www.bjut.edu.cn
```

```
正在 Ping bjut-edu-cn.cname.saaswaf.com [27.221.108.54] 具有 32 字节的数据:
```

2、打开Wireshark软件，双击本次实验正在使用的网络接口，开始进行抓包。



3、然后打开浏览器，在网页地址栏中输入网址，对北京工业大学官网进行访问，浏览校园新闻。

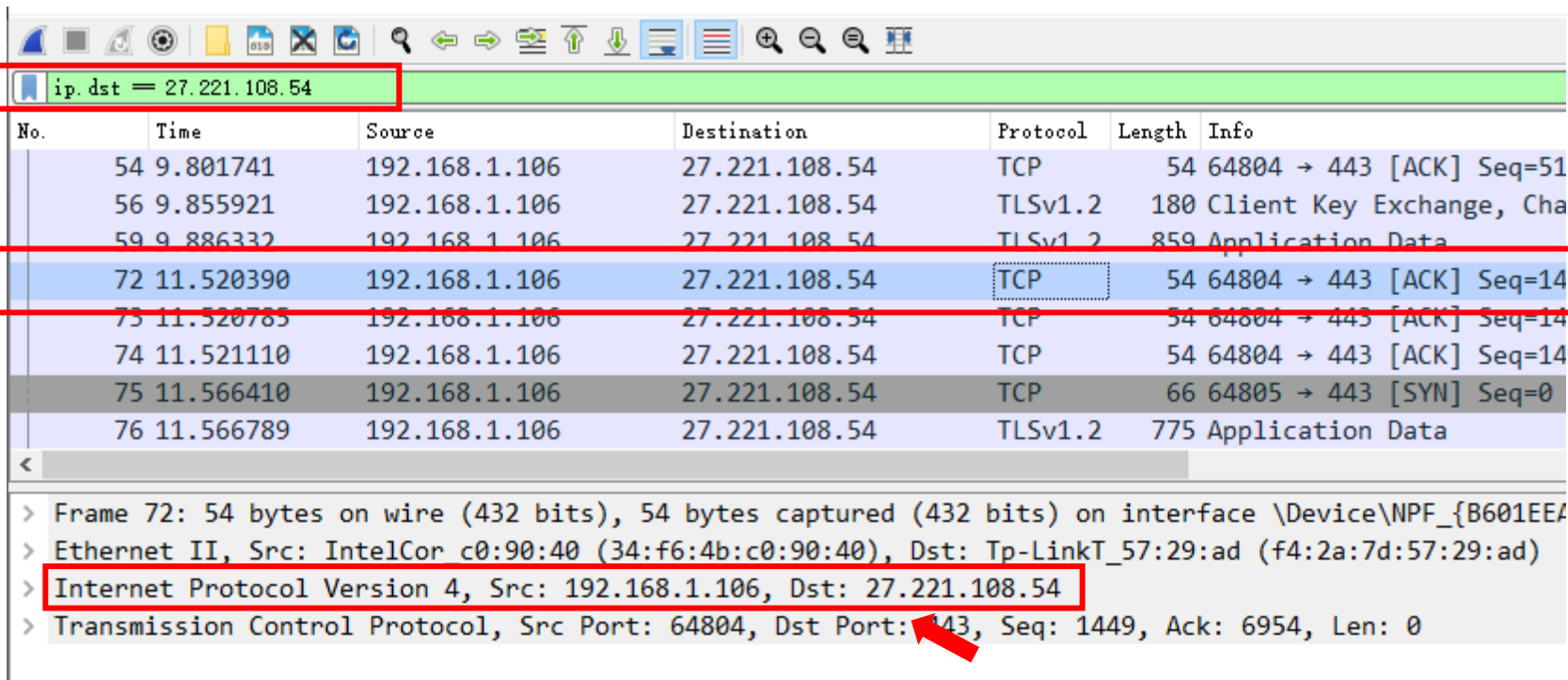


# 实验具体步骤

4、使用过滤表达式对捕获的数据包进行筛选。

ip.dst == 27.221.108.54 (此处IP地址为北工大官网的IP地址)

5、从中选取合适的数据包，观察IPv4数据报格式，并进行分析。



ip.dst == 27.221.108.54

No.	Time	Source	Destination	Protocol	Length	Info
54	9.801741	192.168.1.106	27.221.108.54	TCP	54	64804 → 443 [ACK] Seq=51
56	9.855921	192.168.1.106	27.221.108.54	TLSv1.2	180	Client Key Exchange, Cha
59	9.886332	192.168.1.106	27.221.108.54	TLSv1.2	859	Application Data
72	11.520390	192.168.1.106	27.221.108.54	TCP	54	64804 → 443 [ACK] Seq=14
73	11.520785	192.168.1.106	27.221.108.54	TCP	54	64804 → 443 [ACK] Seq=14
74	11.521110	192.168.1.106	27.221.108.54	TCP	54	64804 → 443 [ACK] Seq=14
75	11.566410	192.168.1.106	27.221.108.54	TCP	66	64805 → 443 [SYN] Seq=0
76	11.566789	192.168.1.106	27.221.108.54	TLSv1.2	775	Application Data

> Frame 72: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{B601EEA...}

> Ethernet II, Src: IntelCor c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT\_57:29:ad (f4:2a:7d:57:29:ad)

> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 27.221.108.54

> Transmission Control Protocol, Src Port: 64804, Dst Port: 443, Seq: 1449, Ack: 6954, Len: 0



# 主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

# IPv4数据报首部

## 实验结果:

No.	Time	Source	Destination	Protocol	Length	Info
72	11.520390	192.168.1.106	27.221.108.54	TCP	54	64804 → 443 [ACK] Seq=1449 Ack=6
<						
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 27.221.108.54						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 40						
Identification: 0x196b (6507)						
v Flags: 0x40, Don't fragment						
0... .... = Reserved bit: Not set						
.1... .... = Don't fragment: Set						
..0. .... = More fragments: Not set						
...0 0000 0000 0000 = Fragment Offset: 0						
Time to Live: 64						
Protocol: TCP (6)						
Header Checksum: 0xd73f [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 192.168.1.106						
Destination Address: 27.221.108.54						
> Transmission Control Protocol, Src Port: 64804, Dst Port: 443, Seq: 1449, Ack: 6954, Len: 0						
<						
0000	f4 2a 7d 57 29 ad 34 f6 4b c0 90 40 08 00 45 00	.*}W).4. K..@..E.				
0010	00 28 19 6b 40 00 40 06 d7 3f c0 a8 01 6a 1b dd	.(.k@.@. ?...j..				
0020	6c 36 fd 24 01 bb a2 a2 99 d4 57 fb d3 45 50 10	16.\$.... ..W..EP.				
0030	02 05 fd 11 00 00	.....				

# 实验结果与分析

## 实验分析：

- 版本 (Version) : 4
- 首部长度 (Header Length) : 20 bytes (5)
- 区分服务 (Differentiated Services Field) : 0x00 (DSCP: CS0, ECN: Not-ECT)
- 总长度 (Total Length) : 40
- 标识 (Identification) : 0x196b (6507)
- 标志 (Flags) : 0x40, DF=1未分片, MF=0无后续分片。
- 片偏移 (Fragment Offset) : 0

# 实验结果与分析

## 实验分析：

- 生存时间 (Time to Live) : 64
- 协议 (Protocol) : TCP (6)
- 首部检验和 (Header Checksum) : 0xd73f [validation disabled]
- 源IP地址 (Source Address) : 192.168.1.106
- 目的IP地址 (Destination Address) : 27.221.108.54

## 实验结果与分析

## 绘制IPv4数据报首部格式:

Version : 4	Header Length: 20 bytes	Differentiated Services Field: 0x00	Total Length: 40			
Identification: 0x196b (6507)			0	1	0	Fragment Offset: 0
Time to Live: 64		Protocol: TCP (6)	Header Checksum: 0xd73f			
Source Address: 192.168.1.106						
Destination Address: 27.221.108.54						

# 首部检验和计算

实验结果：

0000	f4	2a	7d	57	29	ad	34	f6	4b	c0	90	40	08	00	45	00
0010	00	28	19	6b	40	00	40	06	d7	3f	c0	a8	01	6a	1b	dd
0020	6c	36	fd	24	01	bb	a2	a2	99	d4	57	fb	d3	45	50	10
0030	02	05	fd	11	00	00										

实验分析：

发送方发送的数据包，首部检验和置全0，相加求和再取反

- $0x4500 + 0x0028 + 0x196b + 0x4000 + 0x4006 + 0x0000 + 0xc0a8 + 0x016a + 0x1bdd + 0x6c36 = 0x228be$
- $0x28be + 0x2 = 0x28c0$
- $0x28c0$ 取反后结果为 $0xd73f$ ，与观察到的首部检验和结果相符。

## 思考题

思考题：选择一条接收方接收到的数据包，进行首部检验和计算，看取反后结果是否全部为0000，检验传输过程当中是否出现错误。

