华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程	**年级：**大一	**上机实践成绩：**
指导教师：张召	**姓名：**林子骥	**学号：**10225501460
上机实践名称：IP 协议分析		**上机实践日期：**6.10
上机实践编号：No.14	**组号：**	**上机实践时间：**6.10

一、 实验目的

- 快速简单了解 IP 协议，特别是 IP 数据报
- 了解 IP 数据报各字段的含义
- 研究 IP 数据的分片方法

二、 实验任务

- 使用 Wireshark 快速了解 IP 协议

三、 使用环境

- Wireshark

四、 实验过程

首先对 www.ecnu,edu.cn 发包，发现一直显示请求超时

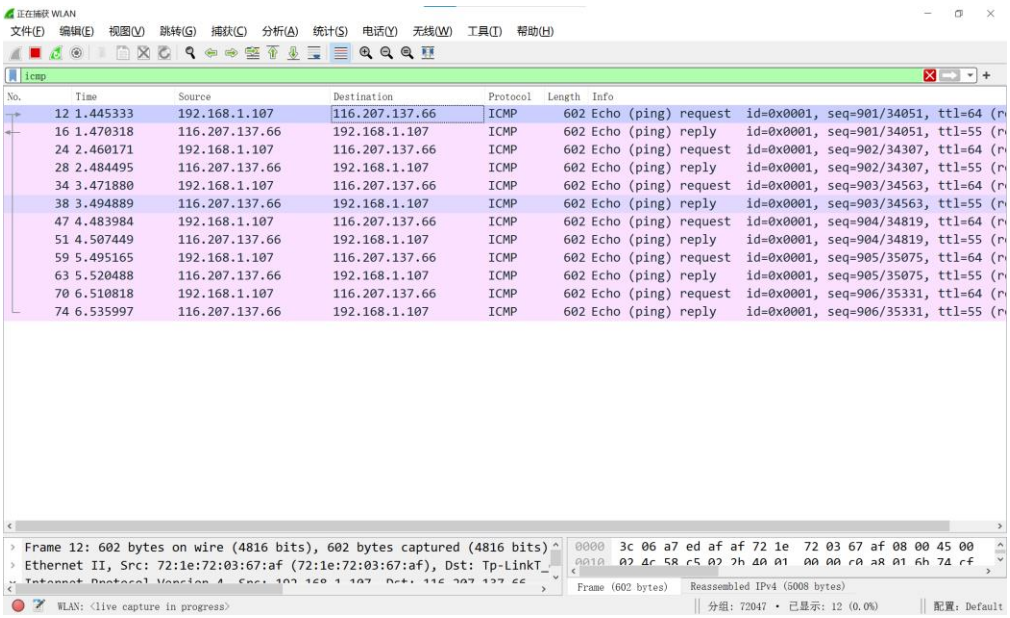
```
C:\Users\Lenovo>ping -l 3005 www.ecnu.edu.cn

正在 Ping www.ecnu.edu.cn [202.120.92.60] 具有 3005 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

202.120.92.60 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

对于 ping 请求超时，可以做出下面的可能性假设：

（1）对方与自己不在同一网段内，通过路由也无法找到对方，但有时对方确实是存在的，当然不存在也是返回超时的信息；

（2）对方确实存在，但设置了 ICMP 数据包过滤（比如防火墙设置）。

接下来换一个网站 www.bilibili.com 进行实验，如下图




```
C:\Users\Lenovo>ping -n 6 -l 5000 www.bilibili.com

正在 Ping a.w.bilicdn1.com [116.207.137.66] 具有 5000 字节的数据:
来自 116.207.137.66 的回复: 字节=5000 时间=25ms TTL=55
来自 116.207.137.66 的回复: 字节=5000 时间=24ms TTL=55
来自 116.207.137.66 的回复: 字节=5000 时间=23ms TTL=55
来自 116.207.137.66 的回复: 字节=5000 时间=23ms TTL=55
来自 116.207.137.66 的回复: 字节=5000 时间=25ms TTL=55
来自 116.207.137.66 的回复: 字节=5000 时间=25ms TTL=55

116.207.137.66 的 Ping 统计信息:
    数据包: 已发送 = 6，已接收 = 6，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 23ms，最长 = 25ms，平均 = 24ms
```

Task1

Ip 报文格式：任取一个有 IP 协议的 ICMP 数据报并根据该报文分析 IP 协议的报文格式（正确标注每一个部 分）。

```
Internet Protocol Version 4, Src: 192.168.1.107, Dst: 116.207.137.66
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 588
    Identification: 0x58c5 (22725)
  > 000. .... = Flags: 0x0
    ...0 0010 0010 1011 = Fragment Offset: 4440
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.107
    Destination Address: 116.207.137.66
  > [4 IPv4 Fragments (5008 bytes): #9(1480), #10(1480), #11(1480), #12(568)]
Internet Control Message Protocol
```

版本：目前广泛使用的 P 协议版本号为 4，即 IPv4。

```
0100 .... = Version: 4
```

首部长度：

```
.... 0101 = Header Length: 20 bytes (5)
```

区分服务：优先级标志位和服务类型标志位，被路由器用来进行流量的优先排序

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

总长度：指 IP 首部和数据报中数据之后的长度，单位为字节。

```
Total Length: 588
```

标识字段：一个唯一的标识数字，用来识别一个数据报或者被分片数据包的次序。

```
Identification: 0x58c5 (22725)
```

标志：用来标识一个数据报是否是一组分片数据报的一部分。标志字段中的最低位记为 MF（More Fragment）。MF=1 即表示后面“还有分片”的数据报。MF=0 表示这已是若干 数据包分片中的最后一个。标志字段中间的一位记为 DF（Don’t Fragment），意思是“不能分片”。只有当 DF=0 时，才允许分片。

```
000. .... = Flags: 0x0
   0... .... = Reserved bit: Not set
   .0.. .... = Don't fragment: Not set
   ..0. .... = More fragments: Not set
```

片偏移：一个数据报是一个分片，这个域中的值就会被用来将数据报以正确的顺序重新组装。下面的报文中显示值为 4440。这里解释原因：

最开始设置发送字节大小为 5000 的包

因为 MTU，需要进行分片，分成了 4 个包

每个包的大小为 1500 字节，除去 ip 首部，剩余 1480 个字节

这里由之前的 flag 标志可以看出是最后一个包，所以偏移量为：1480*3=4440 字节

```
...0 0010 0010 1011 = Fragment Offset: 4440
```

生存时间：确保不会在网络中无限循环，每一台路由器处理数据时，值减一

```
Time to Live: 64
```

协议：采用 icmp 协议

```
Protocol: ICMP (1)
```

首部检验和：只检验首部和，不涉及数据部分

```
Header Checksum: 0x0000 [validation disabled]
```

源地址

```
Source Address: 192.168.1.107
```

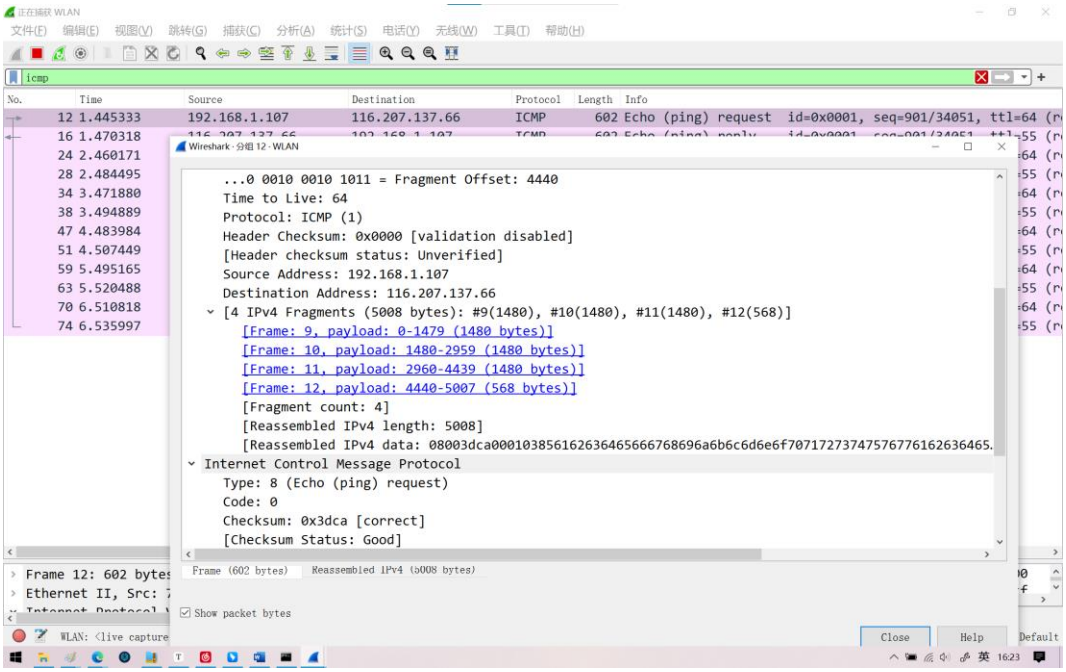
目的地址

```
Destination Address: 116.207.137.66
```

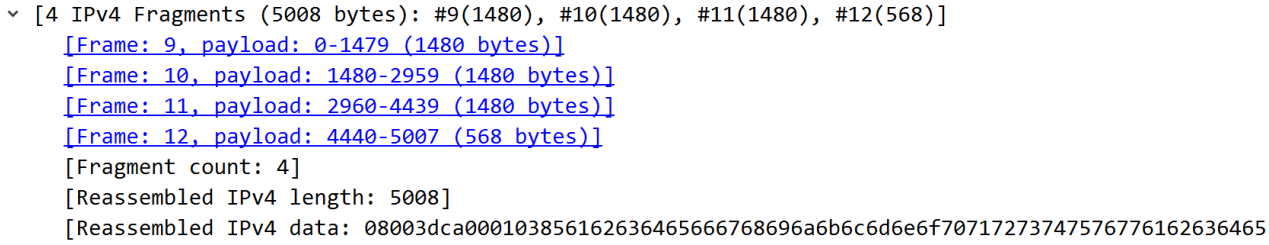
可选字段：此报文中没有

Task2

对截获的报文进行分析，将属于同一个 ICMP 请求报文的分片找出来，并分析其字节长度特点 （如，每个分片的大小，片偏移等）。



图中的 ICMP 请求报文被分成了 4 个分片



其分片大小

Frame：9，1500 字节，有效负载 1480 字节

Frame：10，1500 字节，有效负载 1480 字节

Frame：11，1500 字节，有效负载 1480 字节

Frame：12，578 字节，有效负载 1480 字节

可见前三个分片的大小与 MTU 相等，最后一个分片包含不到 1480 个字节的有效内容。假设所有分片按序到达，其片偏移为前一个分片传输数据后，数据流接下来可以接受的位置。

Question：为什么发送的数据包的总长度（5000）会小于 Reassembled IPv4 length（5008）？

Answer：

在重组过程中，所有分片的有效负载都将被组装在一起，从而构成原始数据包。由于在每个分片中包含 IP 包头和 ICMP 包头的信息，因此在重组过程中，这些信息会被添加到有效负载中，从而导致重组后的 IPv4 总长度比原数据包大小要大一些。因此，Reassembled IPv4 length 为 5008，比 ping -l 5000 命令设置的数据包大小大了 8 个字节。

总结：

通过对 IP 数据包的分析，进一步了解了 IP 数据包头部各个字段的值以及有效载荷的内容等。同时还了解了需要根据数据包的具体情况进行相关分析和评估，例如，数据包的传输效率、丢包情况、延迟和重组等。

通过 IP 协议分析实验，深入了解 Internet 网络的基本原理和协议结构，很有帮助。