

华东师范大学数据科学与工程学院上机实践报告

课程名称：计算机网络与编程

指导教师：张召

上机实践名称： week 14_ IP 协议分析

上机实践编号： 14

年级： 2022

姓名： 李芳

组号：

上机实践成绩：

学号： 10214602404

上机实践日期： 2024.06.07

上机实践时间：

一、题目要求及实现情况

task1: 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），请将实验结果附在实验报告中。

知识补充：

➤ IP 协议的报文格式：

版本（4）	首部长度（4）	优先级与服务类型（8）	总长度（16）	
标识符（16）			标志（3）	段偏移量（13）
TTL（8）	协议号（8）		首部校验和（16）	
源地址（32）				
目标地址（32）				
可选项				
数据				

- 版本：IP 的版本号，IPv4、IPv6
- 首部长度：IP 包头部长度，最少 20 字节，长度取决于可选项
- 优先级与服务类型：表示数据包的优先级和服务类型，通过在数据包中划分一定的优先级，用于实现 QoS（服务质量）的要求
- 总长度：IP 数据包的总长度，最长为 65535 字节
- 标识符：被分片的数据拥有一个统一的标识符，用于区分不同文件数据。当 IP 对上层数据进行分片时，它将给所有的分片分配一组编号，然后将这些编号放入标识符字段中，保证分片不会被错误地重组。（区分不同文件）
- 标志：对当前的包不能进行分片（当该包从一个以太网发送到另一个以太网时），或当一个包被分片后用以指示在一系列的分片中，最后一个分片是否已发出。

- 段偏移量：区分同一文件分片后的顺序，保证分片序列中各分片按顺序重新组合。（区分同一文件内分片位置）
 - TTL:生命周期，经过一个路由器 TTL-1，用于防止环路。当 TTL 的值为 0 时，数据包被丢弃。
 - 协议号：IP 数据包中封装的上层数据协议是 TCP 还是 UDP。TCP 的协议号为 6，UDP 的协议号为 17。
 - 首部校验和：差错校验，防止修改
 - 可选项：数据包创建时间等选项
- ICMP 协议：
- Internet 控制报文协议，是一个错误侦测与回馈机制，用来发送错误和控制消息，用于探测节点间网络连通性。通过 IP 数据包封装，属于网络层协议



- 应用：ping & tracert

实验流程：

- 首先打开 wireshark，点击 wlan 开始捕获。打开终端，使用 ping 命令，获取大于 1472 字节 ICMP 数据包，停止 wireshark 继续捕获，界面如下：

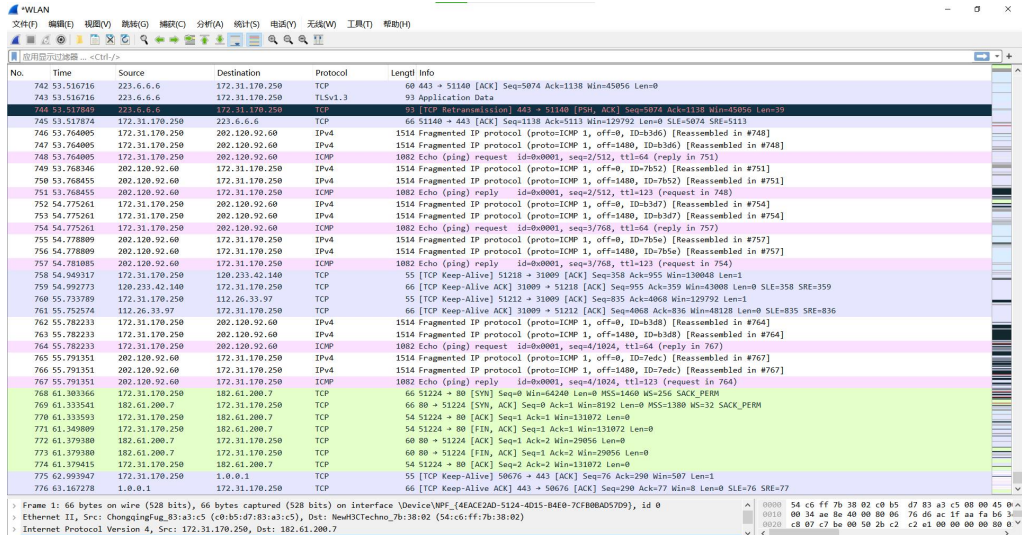
```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

尝试新的跨平台 PowerShell https://aka.ms/pscore6

加载个人及系统配置文件用了 7893 毫秒。
(base) PS C:\Users\HUAWEI> ping -l 4000 www.ecnu.edu.cn

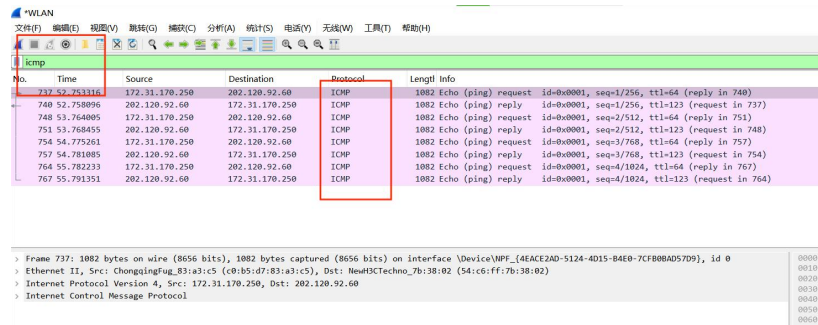
正在 Ping www.ecnu.edu.cn [202.120.92.60] 具有 4000 字节的数据:
来自 202.120.92.60 的回复: 字节=4000 时间=4ms TTL=123 1
来自 202.120.92.60 的回复: 字节=4000 时间=4ms TTL=123 2
来自 202.120.92.60 的回复: 字节=4000 时间=5ms TTL=123 3
来自 202.120.92.60 的回复: 字节=4000 时间=9ms TTL=123 4

202.120.92.60 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 4ms, 最长 = 9ms, 平均 = 5ms
(base) PS C:\Users\HUAWEI> |
```



No.	Time	Source	Destination	Protocol	Length	Info
742	53.516716	223.6.6.6	172.31.170.250	TCP	60	443 → 51140 [ACK] Seq=5074 Ack=1138 Win=45056 Len=0
743	53.516716	223.6.6.6	172.31.170.250	TLSv1.3	93	Application Data
744	53.517849	223.6.6.6	172.31.170.250	TCP	93	[TCP Retransmission] 443 → 51140 [PSH, ACK] Seq=5074 Ack=1138 Win=45056 Len=0
745	53.517874	172.31.170.250	223.6.6.6	TCP	66	51140 → 443 [ACK] Seq=1138 Ack=5113 Win=129792 Len=0 SLE=5074 SRE=5113
746	53.764005	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=b360) [Reassembled in #748]
747	53.764005	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1400, ID=b360) [Reassembled in #748]
748	53.764005	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 751)
749	53.768346	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7652) [Reassembled in #751]
750	53.768345	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1400, ID=7652) [Reassembled in #751]
751	53.768455	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=2/512, ttl=123 (request in 748)
752	54.775261	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=b3d7) [Reassembled in #754]
753	54.775261	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1400, ID=b3d7) [Reassembled in #754]
754	54.775261	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 757)
755	54.778895	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7b5e) [Reassembled in #757]
756	54.778895	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1400, ID=7b5e) [Reassembled in #757]
757	54.781085	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=3/768, ttl=123 (request in 754)
758	54.940317	172.31.170.250	120.233.42.140	TCP	55	[TCP Keep-Alive] 51218 → 31009 [ACK] Seq=358 Ack=955 Win=130048 Len=1
759	54.992773	120.233.42.140	172.31.170.250	TCP	66	[TCP Keep-Alive] 51218 → 31009 [ACK] Seq=955 Ack=358 Win=43008 Len=0 SLE=358 SRE=359
760	55.733789	172.31.170.250	112.26.33.97	TCP	55	[TCP Keep-Alive] 51212 → 31009 [ACK] Seq=835 Ack=4068 Win=129792 Len=1
761	55.752574	112.26.33.97	172.31.170.250	TCP	66	[TCP Keep-Alive] 51212 → 31009 [ACK] Seq=4068 Ack=836 Win=48128 Len=0 SLE=835 SRE=836
762	55.782233	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=b3d8) [Reassembled in #764]
763	55.782233	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1400, ID=b3d8) [Reassembled in #764]
764	55.782233	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 767)
765	55.791351	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=7edc) [Reassembled in #767]
766	55.791351	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1400, ID=7edc) [Reassembled in #767]
767	55.791351	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=4/1024, ttl=123 (request in 764)
768	61.303366	172.31.170.250	182.61.200.7	TCP	66	51224 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
769	61.333541	182.61.200.7	172.31.170.250	TCP	66	80 → 51224 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1300 WS=32 SACK_PERM
770	61.333593	172.31.170.250	182.61.200.7	TCP	54	51224 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
771	61.349809	172.31.170.250	182.61.200.7	TCP	54	51224 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131072 Len=0
772	61.379380	182.61.200.7	172.31.170.250	TCP	60	80 → 51224 [ACK] Seq=1 Ack=2 Win=29056 Len=0
773	61.379380	182.61.200.7	172.31.170.250	TCP	60	80 → 51224 [FIN, ACK] Seq=1 Ack=2 Win=29056 Len=0
774	61.379415	172.31.170.250	182.61.200.7	TCP	54	51224 → 80 [ACK] Seq=2 Ack=2 Win=131072 Len=0
775	62.993947	172.31.170.250	1.0.0.1	TCP	55	[TCP Keep-Alive] 50676 → 443 [ACK] Seq=76 Ack=290 Win=507 Len=1
776	63.167278	1.0.0.1	172.31.170.250	TCP	66	[TCP Keep-Alive] 50676 → 443 [ACK] Seq=290 Ack=77 Win=0 SLE=76 SRE=77

- 上一步骤可知，一共发出了 4 次请求，4 次回应，全部成功。因此，在 wireshark 中对捕获数据包进行筛选，icmp 格式，也可以看到有 4 对数据包：



No.	Time	Source	Destination	Protocol	Length	Info
737	52.753316	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 740)
738	52.758096	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=1/256, ttl=123 (request in 737)
748	53.764005	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 751)
751	53.768455	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=2/512, ttl=123 (request in 748)
754	54.775261	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 757)
757	54.781085	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=3/768, ttl=123 (request in 754)
764	55.782233	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 767)
767	55.791351	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=4/1024, ttl=123 (request in 764)

> Frame 737: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits) on interface \Device\NPF_{4EACE2AD-5124-4D15-B4E0-7CFB0BADA57D9}, id 0

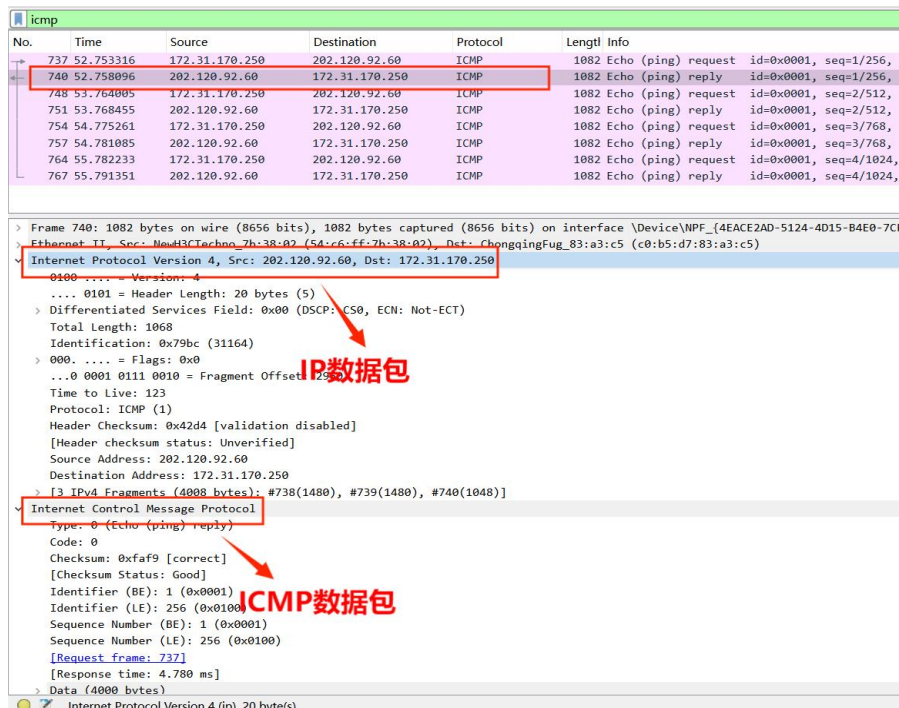
> Ethernet II, Src: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5), Dst: NewH3CTechno_7b:38:02 (54:c6:ff:7b:38:02)

> Internet Protocol Version 4, Src: 172.31.170.250, Dst: 202.120.92.60

> Internet Control Message Protocol

实验结果：

- 选取其中一个 ICMP 数据包进行详细分析：



No.	Time	Source	Destination	Protocol	Length	Info
737	52.753316	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 740)
740	52.758096	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=1/256, ttl=123 (request in 737)
748	53.764005	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 751)
751	53.768455	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=2/512, ttl=123 (request in 748)
754	54.775261	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 757)
757	54.781085	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=3/768, ttl=123 (request in 754)
764	55.782233	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 767)
767	55.791351	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=4/1024, ttl=123 (request in 764)

> Frame 740: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits) on interface \Device\NPF_{4EACE2AD-5124-4D15-B4E0-7CFB0BADA57D9}, id 0

> Ethernet II, Src: NewH3CTechno_7b:38:02 (54:c6:ff:7b:38:02), Dst: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5)

> Internet Protocol Version 4, Src: 202.120.92.60, Dst: 172.31.170.250

0100 = Version: 4

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

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

Total Length: 1068

Identification: 0x79bc (31164)

0000 = Flags: 0x0

...0 0001 0111 0010 = Fragment Offset: 25

Time to Live: 123

Protocol: ICMP (1)

Header Checksum: 0x42d4 [validation disabled]

[Header checksum status: Unverified]

Source Address: 202.120.92.60

Destination Address: 172.31.170.250

> [3 IPv4 Fragments (4008 bytes): #738(1480), #739(1480), #740(1048)]

> Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xaf9 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[Request frame: 737]

[Response time: 4.780 ms]

> Data (4000 bytes)

Internet Protocol Version 4 (fin) 20 bytes(c)

➤ IP 数据包对应分析：

```

> Ethernet II, Src: NewH3CTechno_7b:38:02 (54:c6:ff:7b:38:02), Dst: ChongqingFug_83:a3:c5 (c0:b5:d7:83:a3:c5)
v Internet Protocol Version 4, Src: 202.120.92.60, Dst: 172.31.170.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1068
    Identification: 0x79bc (31164)
    v 000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
        ...0 0001 0111 0010 = Fragment Offset: 2960
    Time to Live: 123
    Protocol: ICMP (1)
    Header Checksum: 0x42d4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 202.120.92.60
    Destination Address: 172.31.170.250
    v [ 3 IPv4 Fragments (4008 bytes): #738(1480), #739(1480), #740(1048)]
        [Frame: 738, payload: 0-1479 (1480 bytes)]
        [Frame: 739, payload: 1480-2959 (1480 bytes)]
        [Frame: 740, payload: 2960-4007 (1048 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 4008]
        [Reassembled IPv4 data [truncated]: 0000faf9000100016162636465666768696a6b6c6d6e6f707172737475767768696a6b6c6d6e6f70717273747576

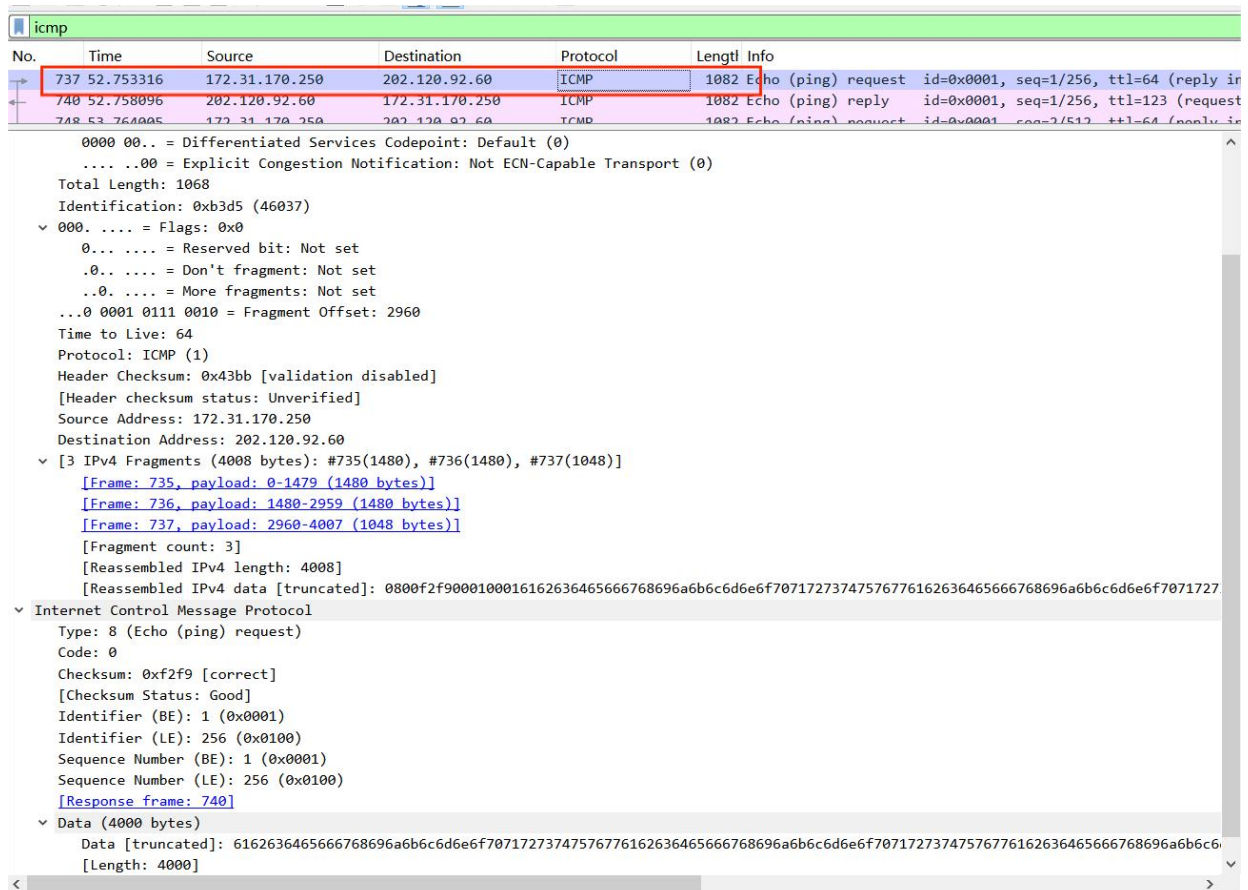
```

■ IP 协议报文格式分析：

- ◆ 版本：IPv4 (4)
- ◆ 头部长度的：20 字节 (5 个 32-bit 字)
- ◆ 优先级与服务类型：
 - 服务类型 (DSCP 和 ECN) :
 - 区分服务代码点 (DSCP) : 0 (默认)
 - 显式拥塞通知 (ECN) : 0 (不支持 ECN)
- ◆ 总长度：1068 字节
- ◆ 标识符：0x79bc (31164)
- ◆ 标志和片偏移：
 - 标志：0x0
 - 保留位：未设置
 - 不分片 (DF) : 未设置
 - 更多片 (MF) : 未设置
 - 片偏移：2960
- ◆ TTL 生存时间：123
- ◆ 协议号：ICMP (1)
- ◆ 首部校验和：0x42d4

- 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），请将实验结果附在实验报告中。

➤ 选取第一个 ICMP 请求报文:



➤ IP 数据包部分：

```

v Internet Protocol Version 4, Src: 172.31.170.250, Dst: 202.120.92.60
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1068
  Identification: 0xb3d5 (46037)
  v 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x43bb [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.31.170.250
  Destination Address: 202.120.92.60
  v [3 IPv4 Fragments (4008 bytes): #735(1480), #736(1480), #737(1048)]
    [Frame: 735, payload: 0-1479 (1480 bytes)]
    [Frame: 736, payload: 1480-2959 (1480 bytes)]
    [Frame: 737, payload: 2960-4007 (1048 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 4008]
    [Reassembled IPv4 data [truncated]: 0800f2f9000100016162636465666768696a6b6c6d6e6f707172737475767
  
```

■ IP 首部结构分析：

- ◆ 版本：4
- ◆ 头部长度的：20 字节 (5)
- ◆ 区分服务字段：0x00 (DSCP: CS0, ECN: Not-ECT)
- ◆ 总长度：1068 字节
- ◆ 标识符：0xb3d5 (46037)
- ◆ 标志位：0x0
 - 保留位：未设置
 - 不分片：未设置
 - 更多分片：未设置，表示这是最后一个分片
- ◆ 片偏移：2960
- ◆ 生存时间 (TTL)：64
- ◆ 协议：ICMP (1)
- ◆ 头部校验和：0x43bb (未验证)
- ◆ 源地址：172.31.170.250
- ◆ 目标地址：202.120.92.60

➤ ICMP 数据包部分：

```

  v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf2f9 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 740]
  v Data (4000 bytes)
    Data [truncated]: 6162636465666768696a6b6c6d6e6f70717273747576776162636465
    [Length: 4000]

```

■ ICMP 数据包结构分析：

- ◆ 类型：8 (Echo (ping) request)
- ◆ 代码：0
- ◆ 校验和：0xf2f9 (正确)
- ◆ 标识符：
 - 大端字节序：1 (0x0001)
 - 小端字节序：256 (0x0100)
- ◆ 序列号：
 - 大端字节序：1 (0x0001)
 - 小端字节序：256 (0x0100)
- ◆ 响应帧：Frame 740
- ◆ 数据长度：4000 字节

➤ 上面的 Frame737 是 ICMP 请求报文第三个分片，总长度为 1068 字节，其中 IP 头部为 20 字节，数据部分为 1048 字节，此帧的片偏移为 2960，标识为 0xb3d5，且标志位中的“更多分片”未设置，表示这是最后一个分片，对应的响应帧为 740。

➤ wireshark 重新筛选 ip 数据包，根据刚才获取的信息去查找对应的分片 ipv4 数据包：

No.	Time	Source	Destination	Protocol	Length	Info
732	51.322415	172.31.170.250	182.61.200.7	TCP	54	51223 → 80 [ACK] Seq=2 Ack=2 Win=131072 Len=0
733	52.738839	172.31.170.250	202.120.80.2	DNS	75	Standard query 0x67f3 A www.ecnu.edu.cn
734	52.743128	202.120.80.2	172.31.170.250	DNS	91	Standard query response 0x67f3 A www.ecnu.edu.cn A 202.120.92.60
735	52.753316	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=b3d5) [Reassembled in #737]
736	52.753316	172.31.170.250	202.120.92.60	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b3d5) [Reassembled in #737]
737	52.753316	172.31.170.250	202.120.92.60	ICMP	1082	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 740)
738	52.757937	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=79bc) [Reassembled in #740]
739	52.758050	202.120.92.60	172.31.170.250	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=79bc) [Reassembled in #740]
740	52.758096	202.120.92.60	172.31.170.250	ICMP	1082	Echo (ping) reply id=0x0001, seq=1/256, ttl=123 (request in 737)

- ```

File(F) 编辑(E) 视图(V) 翻译(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip

No. Time Source Destination Protocol Length Info

732 51.322415 172.31.170.250 182.61.208.7 TCP 54 51223 → 80 [ACK] Seq=2 Ack=2 Win=131072 Len=0
733 52.738839 172.31.170.250 282.128.98.2 DNS 75 Standard query 0x67f3 A www.ecnu.edu.cn
734 52.743118 202.128.98.2 172.31.170.250 DNS 91 Standard query response 0x67f3 A www.ecnu.edu.cn A 202.120.92.60
735 52.753316 172.31.170.250 202.120.92.60 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b3d5) [Reassembled in #737]
736 52.753316 172.31.170.250 202.120.92.60 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b3d5) [Reassembled in #737]
737 52.753316 172.31.170.250 202.120.92.60 ICMP 1082 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 740)
738 52.757937 172.31.170.250 172.31.170.250 ICMP 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=79bc) [Reassembled in #740]
739 52.758050 202.120.92.60 172.31.170.250 ICMP 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=79bc) [Reassembled in #740]
740 52.758096 202.120.92.60 172.31.170.250 ICMP 1082 Echo (ping) reply id=0x0001, seq=1/256, ttl=123 (request in 737)

Frame 735: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface Vmnet\NPF_{4EAC2A05-5124-4015-84B8-7FCBB0A87D99}, id 00000000
Ethernet II, Src: ChongqingHu...a:1c:5 (c0:b5:d7:7b:38:02), Dst: NetBiosTechno...b:38:02 (54:c6:f7:7b:38:02)
Internet Protocol Version 4, Src: 172.31.170.250, Dst: 202.120.92.60
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 1500
Identification: 0xb3d5 (46037)
001 = Flags: 0x1, More fragments
0... = Reserved bit: Not set
0... = Don't fragment: Not set
...1.... = More fragments: Set
0...0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x237d [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.31.170.250
Destination Address: 202.120.92.60
[Reassembled IPv4 in frame: 737]

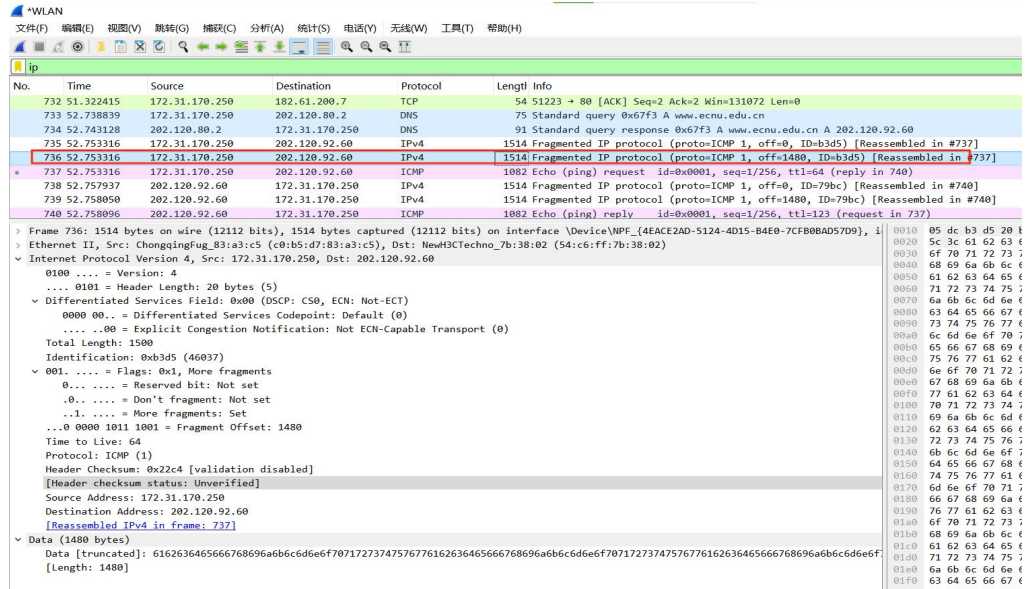
Data (1480 bytes)
Data [truncated]: 0800f790001001612636465666768096abc6c6d6ef7017273747576776162636465666768096abc6c6d6ef70172737475767761626364656667
[Length: 1480]

```



- **Frame 735 是 ICMP 请求报文的第一个分片，总长度为 1500 字节，其中 IP 头部为 20 字节，数据部分为 1480 字节。此帧的片偏移为 0，标识为 0xb3d5，且标志位中的“更多分片”被设置，表示这是一个分片并且后续还有分片，对应的响应帧为 740。**

➤ 第二个：



- **IP 头部：**
  - 版本：IPv4
  - 头部的长度：5 x 4 = 20 bytes
  - 服务的类型：默认值&不支持 ECN
  - 总长度：1500 bytes
  - 标识符：0xb3d5 (46037)
  - 标志：0x1 (More fragments)
    - ◆ 保留位：未设置。
    - ◆ 不分片：未设置。
    - ◆ 更多分片：设置，证明这不是最后一个分片。
  - 片偏移：1480，表示这是第二个分片。
  - 生存时间：64
  - 上层协议类型：ICMP (1)

- IP 头部校验和: 0x22c4
  - 源 IP 地址: 172.31.170.250
  - 目的 IP 地址: 202.120.92.60
  - **Frame 736 是 ICMP 请求报文的第二个分片，总长度为 1500 字节，其中 IP 头部为 20 字节，数据部分为 1480 字节。此帧的片偏移为 1480，标识为 0xb3d5，且标志位中的“更多分片”被设置，表示这是二个分片并且后续还有分片，对应的响应帧为 740。**
  - 这两个分片 IP 数据报部分最后都有一句：Reassembled IPv4 in frame: 737，表示此分片将在 frame 737 中重新组装（也就是第一个这部分第一个分析的数据包）
- 分片信息分析：
- ICMP Echo 请求报文被 IP 层分片为三个分片：
    - ◆ 分片 1
      - 帧：735
      - 大小：1480 字节
      - 片偏移：0-1479
      - 标识符：0xb3d5 (46037)
    - ◆ 分片 2
      - 帧：736
      - 大小：1480 字节
      - 片偏移：1480-2959
      - 标识符：0xb3d5 (46037)
    - ◆ 分片 3
      - 帧：737
      - 大小：1048 字节
      - 片偏移：2960-4007
      - 标识符：0xb3d5 (46037)
  - 这些分片合并后，总长度为 4008 字节（包括 IP 报头），其中数据部分为 4000 字节，与请求的

**指定字节大小 -l 4000 相对应。**

### **IP 分片:**

➤ 必要性:

- 最大传输单元: 不同网络链路的 MTU 限制了单个 IP 数据报的大小。
- 网络层的透明性: IP 层负责分片和重组, 使得上层协议 (TCP、UDP) 不需要关心底层网络的 MTU 限制。

➤ 机制:

- Identification 字段: 头部的一个唯一的标识, 属于同一数据报的所有分片。
- Flags 字段: 三个标志位
  - ◆ Reserved bit: 保留位, 通常为 0。
  - ◆ Don't Fragment (DF): 不分片标志位, 如果设置为 1, 则数据报不允许分片。如果数据报大小超过 MTU 且 DF 位设置为 1, 则数据报会被丢弃, 并发送 ICMP 错误消息。
  - ◆ More Fragments (MF): 更多分片标志位, 如果设置为 1, 则表示后面还有更多的分片; 如果为 0, 则表示这是最后一个分片。
  - ◆ Fragment Offset 字段: 表示分片在原始数据报中的相对位置, 单位为 8 字节 (64 位)。

- 重组: 接收端, 所有分片根据 Identification 和 Fragment Offset 字段进行重组 (**只有当所有分片到达后, 才能组合成完整的 IP 数据报**)

## **二、总结**

这次实验主要是通过 wireshark 配合 cmd 的 ping 命令, 进行 ICMP 数据包的捕获, 从而进一步对 IP 数据报文、ICMP 数据报文以及 IP 数据分片进行分析和理解。

完成的两个实验任务都各有收获:

Task1 详细分析了一个包含 IP 协议的 ICMP 请求报文, 识别了以太网帧头中的源和目的 MAC 地址、IP 报头中的版本、头部长度的、区分服务字段和总长度等字段。让我清楚了 IP 数据报文对应的结构组成究竟是什么。同时, 我还巩固复习了 IP 协议这部分的理论知识。

Task2 研究了同一 ICMP 请求报文的分片，确定了每个分片的大小和片偏移，通过分析分片报文中的标识字段、片偏移和更多分片标志，我理解了 IP 数据报的分片和重组机制，这部分是我理论课没搞懂的难点。

本次实验让我加深了对 IP 协议和分片技术的理解，同时也算是为理论课的网络协议学习打下了基础。