

中国科学技术大学计算机学院

计算机网络实验报告

实验四

利用 Wireshark 观察 IP 数据报

学 号： JL19110004

姓 名： 徐语林

专 业： 计算机科学与技术

指导老师： 张信明

中国科学技术大学计算机学院

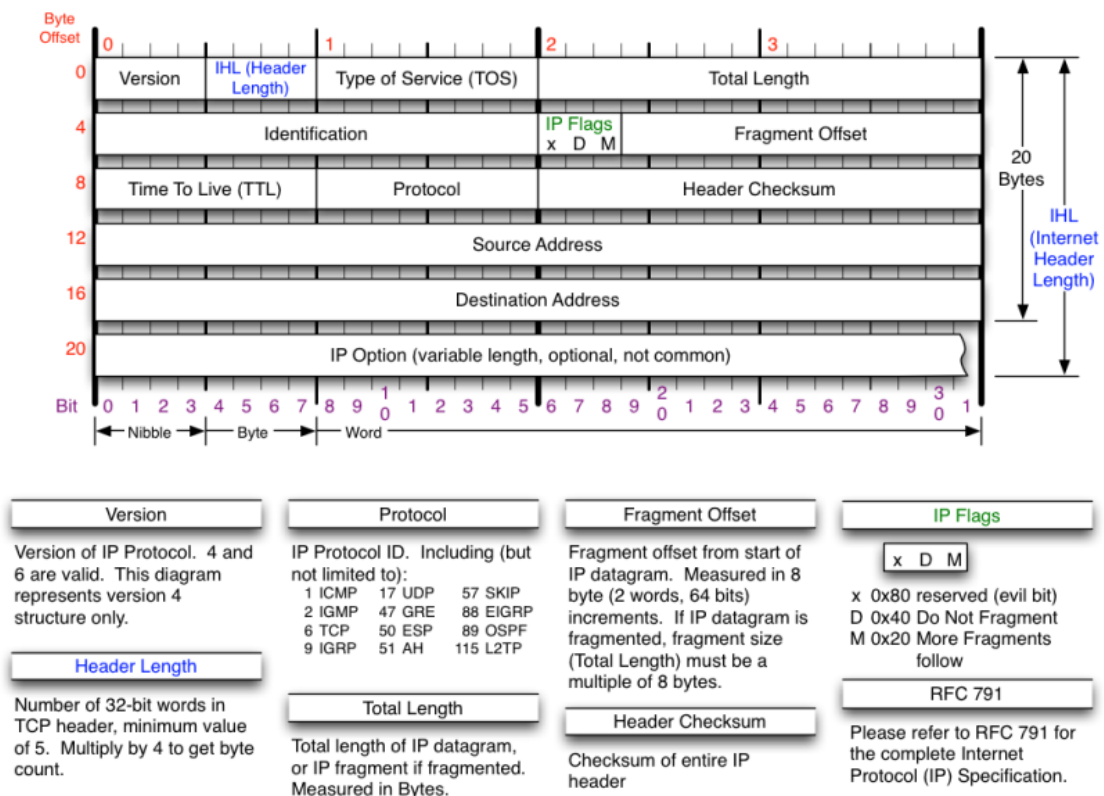
2020 年 12 月 10 日

一. 实验目的

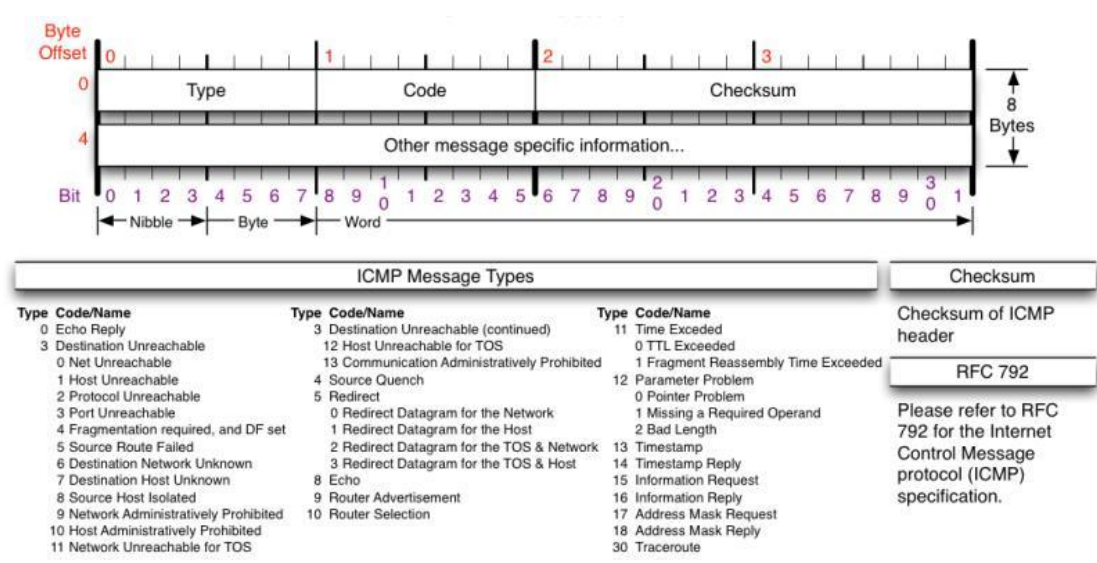
1. 通过捕获观察并分析 IP 数据报的结构
2. 掌握 traceroute 的使用 (Windows 下替换为 PingPlotter)

二. 实验原理

1. Wireshark 是一种非常流行的网络封包分析软件, 功能十分强大。可以截取各种网络封包, 显示网络封包的各种详细信息。Wireshark 使用 Npcap 作为接口, 直接与网卡进行数据报文交换, 监听共享网络上传送的数据包
2. TTL 是 IP 数据包在计算机网络中可以转发的最大跳数, 可以由发送者来设置, 每经过一个路由器, 路由器就会修改这个 TTL 字段值, 具体的做法就是把该 TTL 的值减一, 再把 IP 包发送出去。如果在 IP 包到达目的 IP 之前, TTL 减少为 0, 路由器将会丢弃这个 IP 包并向 IP 包的发送者发送 ICMP time exceeded 的消息。而 traceroute 或者是 pingplotter 也就是设置 ttl, 通过一次次的重传, 与 ttl+1 来得到到达目的地址的路径上的路由器的信息。
3. IPV4 报文:



4. ICMP 报文：

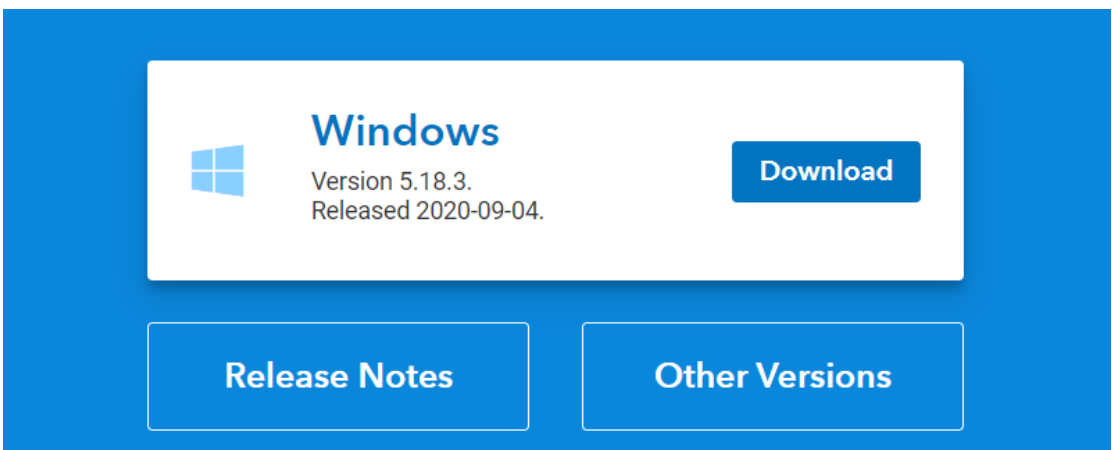


三. 实验条件

由于是 Windows 系统,所以利用的是 Pingplotter 以及之前安装好的 wireshark.

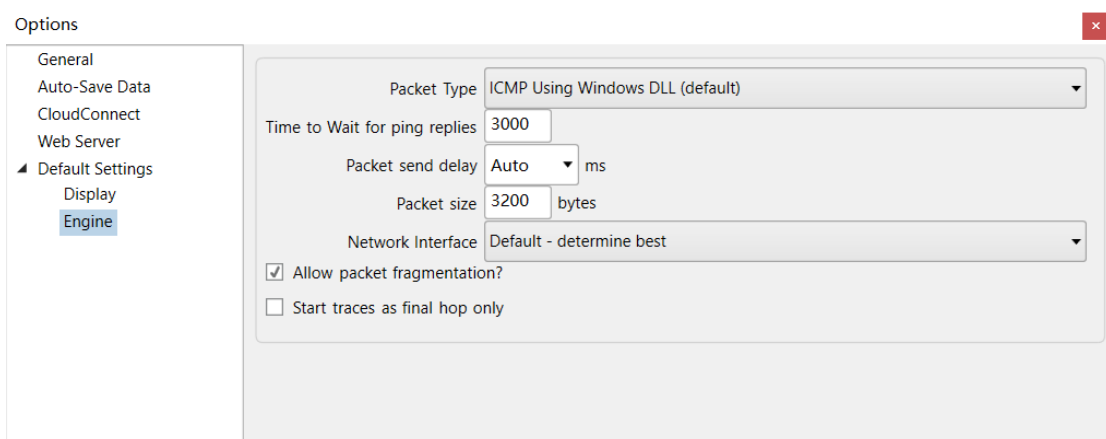
四. 实验过程

1. 官网上下载实验要用的 Pingplotter:

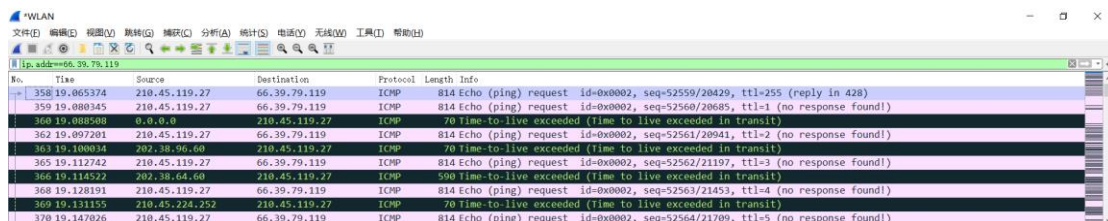


2. 利用 PingPlotter 发包并用 wireshark 来捕获查看. 用 wireshark 开始捕获, 用 PingPlotter 发送 800, 1600, 3200 的包.

如下是在 PingPlotter 界面进行的设置:



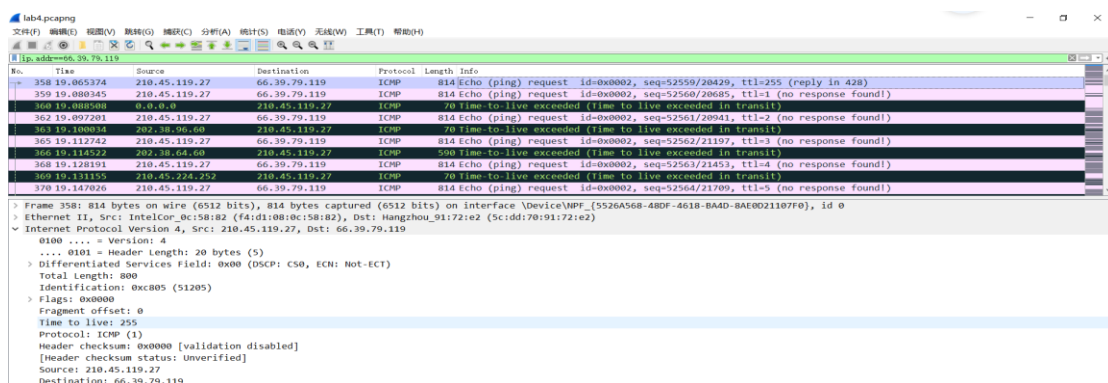
捕获完后在 wireshark 中写入筛选的条件：



五. 回答问题

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

答：我的 ip 地址为 210.45.119.27



2. Within the IP packet header, what is the value in the upper layer

protocol field?

```
Fragment Offset: 0
> Time to live: 1
Protocol: ICMP (1)
```

答：

可见上层协议区域的值为 ICMP (1) 。

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

答：

:

```
> Frame 359: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0xc806 (51206)
    Flags: 0x0000
    Fragment offset: 0
    > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 210.45.119.27
    Destination: 66.39.79.119
> Internet Control Message Protocol
```

20 字节；

Payload 字节数：800-20=780.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

答：该数据包没有被分割，由于在 flags 的标记中，more fragments 位没有被置为 1.

```
Flags: 0x0000
0... .. = Reserved bit: Not set
.0.. .. = Don't fragment: Not set
..0. .... = More fragments: Not set
```

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

答：

:

```
> Frame 359: 814 bytes on wire (6512 bits), 814 Bytes captured (6512 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE021107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0xc806 (51206)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
      Protocol: ICMP (1)
      Header checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source: 210.45.119.27
      Destination: 66.39.79.119
  > Internet Control Message Protocol

> Frame 362: 814 bytes on wire (6512 bits), 814 Bytes captured (6512 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE021107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0xc807 (51207)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 2
    > [Expert Info (Note/Sequence): "Time To Live" only 2]
      Protocol: ICMP (1)
      Header checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source: 210.45.119.27
      Destination: 66.39.79.119
  > Internet Control Message Protocol
```

从中可以看出 TTL, Identification 是在改变的。

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

答：保持不变的字段有：Version, Protocol, Header Length, Differentiated Services Field, Source, Destination.

理由：Version：都是 IPv4.

Protocol：都是 ICMP.

Header Length：都是 ICMP，所以不变

Differentiated Services Field：都是 ICMP.

Source 和 Destination：由于在这个过程中源，目的主机并不发生变化，所以这两个也不会改变

必须改变的有：TTL, Identification

理由：TTL：基于 ppt 上的原理可知 TTL 必须改变

Identification：数据报之间的 id 是不一样的

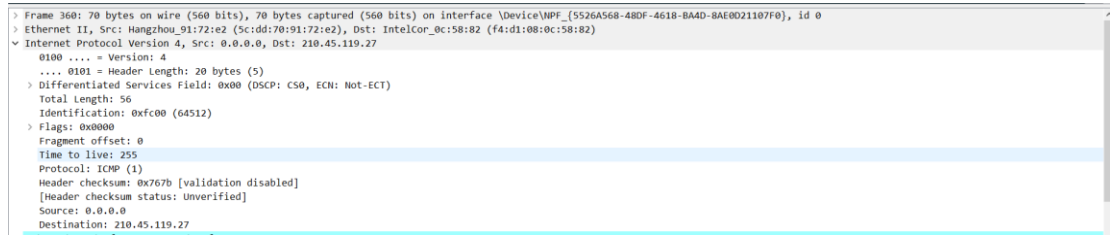
7. Describe the pattern you see in the values in the Identification field of the IP datagram

答：可参见第五题的图，id 会加一

8. What is the value in the Identification field and the TTL field?

答

:



```
> Frame 360: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0021107F0}, id 0
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_0c:58:82 (f4:d1:08:0c:58:82)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 210.45.119.27
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xfc00 (64512)
    Flags: 0x0000
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x767b [validation disabled]
    [Header checksum status: Unverified]
    Source: 0.0.0.0
    Destination: 210.45.119.27
```

第一跳的: Identification:0xfc00(64512)

TTL:255

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router?

Why?

答: id 变化. id 需要独立, 但是 ttl 不会发生变化, 电脑的第一条路由是不会发生变化的, ttl 初始值被设置为了 255, 便不会再发生改变。

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the ip-ethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation. 3]

答: 如图:

1665	38.143305	210.45.119.27	66.39.79.119	ICMP	134 Echo (ping) request id=0x0002, seq=53043/13263, ttl=1 (no response found)
1666	38.143160	0.0.0.0	210.45.119.27	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1667	38.184308	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=c9e9) [Reassembled in #1668]
1668	38.184308	210.45.119.27	66.39.79.119	ICMP	134 Echo (ping) request id=0x0002, seq=53044/13519, ttl=2 (no response found)


```

> Frame 1665: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor.0c:58:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 120
    Identification: 0xc9e9 (51689)
  > Flags: 0x00b9
    Fragment offset: 1480
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 210.45.119.27
    Destination: 66.39.79.119
  > [ 2 IPv4 Fragments (1500 bytes): #1664(1480), #1665(100)]
> Internet Control Message Protocol

```

被分成了两个 fragment.

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

答：

1664	38.143305	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=c9e9) [Reassembled in #1665]
1665	38.143305	210.45.119.27	66.39.79.119	ICMP	134 Echo (ping) request id=0x0002, seq=53043/13263, ttl=1 (no response found)
1666	38.143160	0.0.0.0	210.45.119.27	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1667	38.184308	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=c9e9) [Reassembled in #1668]
1668	38.184308	210.45.119.27	66.39.79.119	ICMP	134 Echo (ping) request id=0x0002, seq=53044/13519, ttl=2 (no response found)


```

> Frame 1664: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor.0c:58:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xc9e9 (51689)
  > Flags: 0x2000, More fragments
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 210.45.119.27
    Destination: 66.39.79.119
  > [Reassembled IPv4 in frame: 1665]
> Data (1480 bytes)

```

No. 1664 号 frame 可以知道其中的 more flag 被置为了 1, Fragment offset 为 0, 整个 ip 包长度为 1500 字节

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

答：找到 No. 1665 号。

1665	38.143305	210.45.119.27	66.39.79.119	ICMP	134 Echo (ping) request id=0x0002, seq=53043/13263, ttl=1 (no response found!)
1666	38.145168	0.0.0.0	210.45.119.27	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1667	38.184308	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=c9ea) [Reassembled in #1668]
1668	38.184308	210.45.119.27	66.39.79.119	ICMP	134 Echo (ping) request id=0x0002, seq=53044/13519, ttl=2 (no response found!)

> Frame 1665: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0	
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)	
Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 120	
Identification: 0xc9e9 (51689)	
> Flags: 0x00b9	
Fragment offset: 1480	
> Time to live: 1	
Protocol: ICMP (1)	
Header checksum: 0x0000 [validation disabled]	
[Header checksum status: Unverified]	
Source: 210.45.119.27	
Destination: 66.39.79.119	
> [2 IPv4 Fragments (1580 bytes): #1664(1480), #1665(100)]	
Internet Control Message Protocol	

其中的 fragment offset 非 0 这就说明这不是第一个;

✓ Flags: 0x00b9

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

..0. = More fragments: Not set

More fragments 说明没有更多的片段

13. What fields change in the IP header between the first and second fragment?

答: 改变的有 total length, flags, fragment offset.

14. How many fragments were created from the original datagram?

答

:

2899	55.160053	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=cb81) [Reassembled in #2901]
2900	55.160053	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cb81) [Reassembled in #2901]
2901	55.160053	210.45.119.27	66.39.79.119	ICMP	254 Echo (ping) request id=0x0002, seq=53451/52176, ttl=1 (no response found!)
2903	55.200160	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=cb82) [Reassembled in #2905]
2904	55.200169	210.45.119.27	66.39.79.119	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cb82) [Reassembled in #2905]
2905	55.200169	210.45.119.27	66.39.79.119	ICMP	254 Echo (ping) request id=0x0002, seq=53452/52432, ttl=2 (no response found!)

> Frame 2901: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0	
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)	
Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 240	
Identification: 0xcb81 (52097)	
Flags: 0x0172	
0... .. = Reserved bit: Not set	
.0.. .. = Don't fragment: Not set	
..0. = More fragments: Not set	
Fragment offset: 2960	
> Time to live: 1	
Protocol: ICMP (1)	
Header checksum: 0x0000 [validation disabled]	
[Header checksum status: Unverified]	
Source: 210.45.119.27	
Destination: 66.39.79.119	
> [3 IPv4 Fragments (3180 bytes): #2899(1480), #2900(1480), #2901(220)]	
Internet Control Message Protocol	

有 3 个.

15. What fields change in the IP header among the fragments?

答: 第一个和第二个的 more fragments 位是 1, 第三个是 0;

第一个和第二个 payload 为 1480, 第三个为 220

对于 ppt 中报文分片问题的计算，用第 14 题来做个说明：

2899	55.160053	210.45.119.27	66.39.79.119	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cb81) [reassembled in #2901]
2900	55.160053	210.45.119.27	66.39.79.119	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cb81) [reassembled in #2901]
2901	55.160053	210.45.119.27	66.39.79.119	ICMP	254	Echo (ping) request id=0x0002, seq=53451/52176, ttl=1 (no response found)
2903	55.280169	210.45.119.27	66.39.79.119	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=cb82) [reassembled in #2905]
2904	55.280169	210.45.119.27	66.39.79.119	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=cb82) [reassembled in #2905]
2905	55.280169	210.45.119.27	66.39.79.119	ICMP	254	Echo (ping) request id=0x0002, seq=53452/52432, ttl=2 (no response found)

```
> Frame 2901: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor 0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou 91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 210.45.119.27, Dst: 66.39.79.119
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total length: 240
    Identification: 0xcb81 (52097)
  > Flags: 0x0172
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    Fragment offset: 2960
  > Time to live: 1
  > Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 210.45.119.27
    Destination: 66.39.79.119
  > [3 IPv4 Fragments (3180 bytes): #2899(1480), #2900(1480), #2901(220)]
> Internet Control Message Protocol
```

> Differentiated Services Field: 0x

Total Length: 1500

Identification: 0xcb81 (52097)

1500 除开 20 字节还有 1480. 第三个的要求是 3200, 那么只能容纳两个 1480 的分片, 这样 $1480 \times 2 = 2960$. $3200 - 2960 = 240$, 这是加入了 20 字节报头的, 除开后便是 220, 所以范围是 0-1479, 1480-2959, 2960-3179.

六. 实验总结

本次实验观察了 ip 数据报的结构, 进一步加深了对 ip 数据报的理解, 以及分片问题的求解, 对于理解网络层这一章来说还是有很好的作用.