

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 报文

学 号：PE20060014

姓 名：王晨

专 业：计算机科学与技术

指导老师：张信明

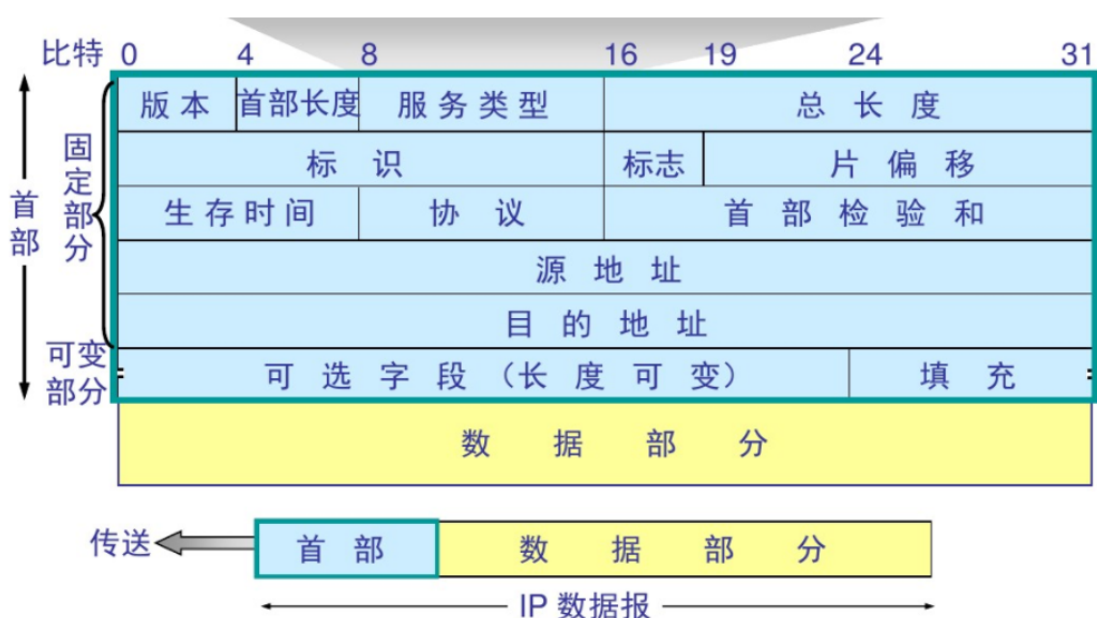
中国科学技术大学计算机学院

2020 年 12 月 6 日

一、实验目的

1. 捕获观察并分析 IP 数据报的结构，理解 IP 的细节。
2. 掌握 traceroute 的使用。
3. 回答 pdf 中的 question 部分的问题。

二、实验原理



MTU: Maximum Transmit Unit, 最大传输单元, 即物理接口 (数据链路层) 提供其上层 (通常是 IP 层) 最大一次传输数据的大小; 以普遍使用的以太网接口为例, 缺省 MTU=1500 Byte, 这是以太网接口对 IP 层的约束, 如果 IP 层有 ≤ 1500 byte 需要发送, 只需要一个 IP 包就可以完成发送任务; 如果 IP 层有 > 1500 byte 数据需要发送, 需要分片才能完成发送, 这些分片有一个共同点, 即

标识：唯一的标识主机发送的每一份数据报。通常每发送一个报文，它的值加一。当 IP 报文长度超过传输网络的 MTU（最大传输单元）时必须分片，这个标识字段的值被复制到所有数据分片的标识字段中，使得这些分片在达到最终目的地时可以依照标识字段的内容重新组成原先的数据。

IP 数据报首部的 TTL(Time to live)表示数据报的生存时间, 每经过路由器转发一次, 就至少减少 1, 当减少到 0 的时候, 会被路由器丢弃, 并返回 ICMP 消息.

Traceroute 通过巧妙的设置 ttl, 通过一次次的重传, 与 ttl+1 来得到到目的地址的路径上的路由器的信息.

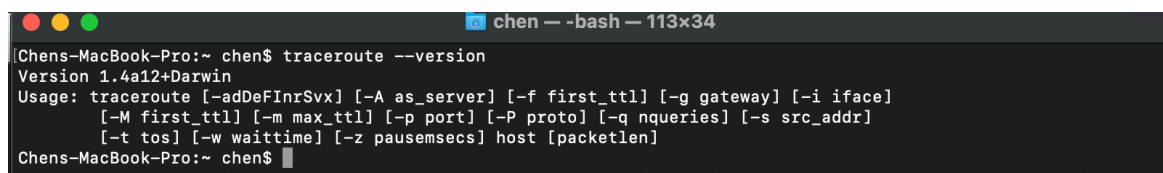
三、 实验条件

- 1、 硬件条件：Mac
- 2、 软件条件：Mac OS Big Sur 11.01

Chrome Web Browser

Wireshark 3.2.7

Traceroute version:

A screenshot of a macOS terminal window. The title bar shows 'chen' and the window size '113x34'. The terminal text shows the command 'traceroute --version' being executed, resulting in 'Version 1.4a12+Darwin'. Below this is the usage information for the traceroute command, listing various options like -A, -f, -g, -i, -M, -m, -p, -P, -q, -s, -t, -w, and -z.

```
chen -- -bash -- 113x34
[Chens-MacBook-Pro:~ chen$ traceroute --version
Version 1.4a12+Darwin
Usage: traceroute [-adDeFInrSvx] [-A as_server] [-f first_ttl] [-g gateway] [-i iface]
        [-M first_ttl] [-m max_ttl] [-p port] [-P proto] [-q nqueries] [-s src_addr]
        [-t tos] [-w waittime] [-z pausesecs] host [packetlen]
Chens-MacBook-Pro:~ chen$
```

四、 实验过程

1. Capturing packets from an execution of traceroute

用 wireshark 开启捕获, 用 traceroute 发送 3 个分别为 800 字节, 1600 字节, 3200 字节的包。

```
Chens-MacBook-Pro:~ chen$ traceroute gaia.cs.umass.edu
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 52 byte packets
 1  0.0.0.0 (0.0.0.0)  3.048 ms  3.869 ms  3.106 ms
 2  202.38.96.60 (202.38.96.60)  3.417 ms  3.589 ms  8.263 ms
 3  202.38.64.58 (202.38.64.58)  3.093 ms
```

```
Chens-MacBook-Pro:~ chen$ traceroute gaia.cs.umass.edu 1600
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 1600 byte packets
 1  0.0.0.0 (0.0.0.0)  10.518 ms  13.563 ms  3.245 ms
 2  * * *
 3  202.38.64.60 (202.38.64.60)  2.474 ms  2.214 ms  2.180 ms
```

```
Chens-MacBook-Pro:~ chen$ traceroute gaia.cs.umass.edu 3200
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 3200 byte packets
 1  0.0.0.0 (0.0.0.0)  4.385 ms  4.074 ms  4.806 ms
 2  * * *
 3  202.38.64.58 (202.38.64.58)  3.779 ms  3.551 ms  4.395 ms
```

2. A look at the captured trace

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?

IP address = 114.214.247.243

No.	Time	Source	Destination	Protocol	Length	Info
11	0.103766	222.192.186.4	114.214.247.243	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536, ttl=54 (reply in 12)
12	0.103823	114.214.247.243	222.192.186.4	ICMP	98	Echo (ping) reply id=0x0004, seq=6/1536, ttl=64 (request in 11)

```
Ethernet II, Src: Hangzhou_91721e2 (5c:0d:70:91:72:e2), Dst: Apple_31:30:57 (14:00:0a:31:30:57)
  Internet Protocol Version 4, Src: 222.192.186.4, Dst: 114.214.247.243
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

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

1, which means ICMP.

```
Fragment Offset: 0
Time to live: 54
Protocol: ICMP (1)
Header checksum: 0x358b [validation disa
```

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.

Header Length = 20Bytes,

Payload Length=84-20=64Bytes, as the total length=84Bytes.

```
Internet Protocol Version 4, Src: 222.192.186.4, Dst: 114.214.247.243
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
```

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

没有被分片，因为 More fragments 位未被置为 1.

```
Flags: 0x4000, Don't fragment
  0... .... = Reserved bit: Not set
  .1.. .... = Don't fragment: Set
  ..0. .... = More fragments: Not set
Fragment offset: 0
```

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?

TTL, checksum, Identification in the Header always change.

No.	Time	Source	Destination	Protocol	Length	Time
83	1.760168	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	1.764619	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
87	1.767758	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	1.771867	202.38.96.60	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
91	1.784578	202.38.96.60	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
93	1.787921	202.38.96.60	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
97	1.793705	202.38.64.58	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
99	1.797111	202.38.64.58	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
101	1.799443	202.38.64.60	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
103	1.804259	218.45.224.252	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
105	1.808482	218.45.224.252	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
107	1.812749	218.45.224.252	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
109	6.828948	101.4.115.13	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
482	6.835116	101.4.115.13	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
484	6.842373	101.4.115.185	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
486	6.847730	101.4.115.185	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
488	6.851859	101.4.115.185	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
Total Length: 56						
Identification: 0x6dee (28142)						
Flags: 0x0000						
0... .. = Reserved bit: Not set						
.0... .. = Don't fragment: Not set						
..0... .. = More fragments: Not set						
Fragment offset: 0						
Time to live: 255						
Protocol: ICMP (1)						
Header checksum: 0xc3bc [validation disabled]						
[Header checksum status: Unverified]						
Source: 0.0.0.0						
Destination: 114.214.247.243						
Internet Control Message Protocol						
Times: 44 (Time to live exceeded)						

No.	Time	Source	Destination	Protocol	Length	Time
83	1.760168	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	1.764619	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
87	1.767758	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	1.771867	202.38.96.60	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
93	1.784578	202.38.96.60	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	1.787921	202.38.96.60	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
97	1.793705	202.38.64.58	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
99	1.797111	202.38.64.58	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
101	1.799443	202.38.64.60	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
103	1.804259	218.45.224.252	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
105	1.808482	218.45.224.252	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
107	1.812749	218.45.224.252	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
480	6.828948	101.4.115.13	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
482	6.835116	101.4.115.13	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
484	6.842373	101.4.115.185	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
486	6.847730	101.4.115.185	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
488	6.851859	101.4.115.185	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
Total Length: 56						
Identification: 0xc52b (58475)						
Flags: 0x0000						
0... .. = Reserved bit: Not set						
.0... .. = Don't fragment: Not set						
..0... .. = More fragments: Not set						
Fragment offset: 0						
Time to live: 254						
Protocol: ICMP (1)						
Header checksum: 0xc62c [validation disabled]						
[Header checksum status: Unverified]						
Source: 202.38.96.60						
Destination: 114.214.247.243						
Internet Control Message Protocol						
Times: 44 (Time to live exceeded)						

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

Version, header length, Differentiated Services Field, flags, fragment offset, protocol, source ip address, destination ip address.

必须不变的有:

Version=ipv4, protocol=icmp

header length, 因为 version 和 protocol 不变

Differentiated Services Field, 因为 version 和 protocol 不变

source ip address, destination ip address 在同一段 TTL 中是不变的。

必须变的有: TTL, traceroute 会改变 TTL; Identification, 不同 IP 数据报之间有不同 id; Header checksum, 因为 header 每次都不同。

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

每次 id 会比前一个增加 1.

- What is the value in the Identification field and the TTL field?

Identification= 0x55c5 (21957), ttl=255

No.	Time	Source	Destination	Protocol	Length	Info
11	0.103766	222.192.186.4	114.214.247.243	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536, ttl=54 (reply in 12)
12	0.103823	114.214.247.243	222.192.186.4	ICMP	98	Echo (ping) reply id=0x0004, seq=6/1536, ttl=64 (request in 11)
53	1.025718	222.192.186.4	114.214.247.243	ICMP	98	Echo (ping) request id=0x0004, seq=7/1792, ttl=54 (reply in 54)
54	1.025759	114.214.247.243	222.192.186.4	ICMP	98	Echo (ping) reply id=0x0004, seq=7/1792, ttl=64 (request in 53)
92	2.013091	222.192.186.4	114.214.247.243	ICMP	98	Echo (ping) request id=0x0004, seq=8/2048, ttl=54 (reply in 93)
93	2.013132	114.214.247.243	222.192.186.4	ICMP	98	Echo (ping) reply id=0x0004, seq=8/2048, ttl=64 (request in 92)
165	3.077134	222.192.186.4	114.214.247.243	ICMP	98	Echo (ping) request id=0x0004, seq=9/2304, ttl=54 (reply in 166)
166	3.077215	114.214.247.243	222.192.186.4	ICMP	98	Echo (ping) reply id=0x0004, seq=9/2304, ttl=64 (request in 165)
204	3.799991	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
206	3.808618	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
208	3.812008	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	3.815196	202.38.96.68	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	3.819841	202.38.96.68	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
214	3.822927	202.38.96.68	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
216	3.825211	202.38.64.68	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
218	3.839111	202.38.64.58	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
220	3.842472	202.38.64.58	114.214.247.243	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)

```

0x00 .... = version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x55c5 (21957)
> Flags: 0x0000
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0xf335 [validation disabled]

```

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

id 变化, 因为 id 相同表示 ip 包是同一个大包的 fragment, 这里的 id 需要独立. ttl 不变. 因为在同一段时间内, 电脑的第一跳路由是不变的, 其 ttl 的初始值已经是 255 了, 默认不会改变.

Fragmentation

Sort the packet listing according to time again by clicking on the *Time* column.

- Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 1600. Has that message been fragmented across more than one IP datagram?

1600 时, 可以看到被分成了 2 片。

No.	Time	Source	Destination	Protocol	Length	Info
17	0.285341	36.155.244.189	114.214.247.243	TCP	237	14000 → 58095 [PSH, ACK] Seq=1 Ack=1 Win=63 Len=183
18	0.285728	114.214.247.243	36.155.244.189	TCP	54	58095 → 14000 [ACK] Seq=1 Ack=184 Win=4096 Len=0
149	3.349786	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c376) [Reassembled in #150]
150	3.349787	114.214.247.243	128.119.245.12	UDP	134	50037 → 33435 Len=1572
151	3.359172	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	3.359430	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c377) [Reassembled in #153]
153	3.359431	114.214.247.243	128.119.245.12	UDP	134	50037 → 33436 Len=1572
154	3.361915	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
155	3.362144	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c378) [Reassembled in #156]
156	3.362146	114.214.247.243	128.119.245.12	UDP	134	50037 → 33437 Len=1572
157	3.365315	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	3.365531	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c379) [Reassembled in #159]
159	3.365533	114.214.247.243	128.119.245.12	UDP	134	50037 → 33438 Len=1572
160	3.368589	202.38.96.60	114.214.247.243	IPv4	70	Fragmented IP protocol (proto=ICMP 1, off=0, ID=c379)
252	5.428499	122.51.187.118	114.214.247.243	TCP	74	54938 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1424 SACK_PERM=1 TSval=3413952928 TSecr=0
253	5.428677	114.214.247.243	122.51.187.118	TCP	78	22 → 54938 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 TSval=1322194219 TSecr=0
254	5.442255	122.51.187.118	114.214.247.243	TCP	66	54938 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3413952970 TSecr=1322194219

```

Flags: 0x0000
0... .. = Reserved bit: Not set
0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set
Fragment offset: 1480
> Time to live: 1
Protocol: UDP (17)
Header checksum: 0x14f8 [validation disabled]
[Header checksum status: Unverified]
Source: 114.214.247.243
Destination: 128.119.245.12
[ 2 IPv4 Fragments (1580 bytes): #149(1480), #150(100)]
[Frame: 149, payload: 0-1479 (1480 bytes)]
[Frame: 150, payload: 1480-1579 (100 bytes)]

```

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?

找到 frame149, 其中 flags 中的 More fragments 位被置为 1. 这里的 fragment offset 为 0, 整个 ip 包的长度为 1500 字节。

No.	Time	Source	Destination	Protocol	Length	Info
17	0.285341	36.155.244.189	114.214.247.243	TCP	237	14000 → 58095 [PSH, ACK] Seq=1 Ack=1 Win=63 Len=183
18	0.285728	114.214.247.243	36.155.244.189	TCP	54	58095 → 14000 [ACK] Seq=1 Ack=184 Win=4096 Len=0
149	3.349786	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c376) [Reassembled in #150]
150	3.349787	114.214.247.243	128.119.245.12	UDP	134	50037 → 33435 Len=1572
151	3.359172	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	3.359430	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c377) [Reassembled in #153]
153	3.359431	114.214.247.243	128.119.245.12	UDP	134	50037 → 33436 Len=1572
154	3.361915	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
155	3.362144	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c378) [Reassembled in #156]
156	3.362146	114.214.247.243	128.119.245.12	UDP	134	50037 → 33437 Len=1572
157	3.365315	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	3.365531	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c379) [Reassembled in #159]
159	3.365533	114.214.247.243	128.119.245.12	UDP	134	50037 → 33438 Len=1572
160	3.368589	202.38.96.60	114.214.247.243	IPv4	70	Fragmented IP protocol (proto=ICMP 1, off=0, ID=c379)
252	5.428499	122.51.187.118	114.214.247.243	TCP	74	54938 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1424 SACK_PERM=1 TSval=3413952928 TSecr=0
253	5.428677	114.214.247.243	122.51.187.118	TCP	78	22 → 54938 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 TSval=1322194219 TSecr=0
254	5.442255	122.51.187.118	114.214.247.243	TCP	66	54938 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3413952970 TSecr=1322194219

```

Ethernet II, Src: Apple-3f:3b:57 (14:7d:da:3f:3b:57), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
Internet Protocol Version 4, Src: 114.214.247.243, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xc376 (50038)
Flags: 0x2000, More fragments
0... .. = Reserved bit: Not set
0... .. = Don't fragment: Not set
..1... .. = More fragments: Set
Fragment offset: 0
> Time to live: 1
Protocol: UDP (17)

```

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 the more fragments? How can you tell?

找到 frame150, 看到 fragment offset=1480, 不是第一个。

不能根据 more fragments 位判断是不是第一个, 因为最后一个 fragment 的 more fragments 位也是 0.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.205341	36.155.244.189	114.214.247.243	TCP	237	14000 → 58095 [PSH, ACK] Seq=1 Ack=1 Win=63 Len=183
18	0.205728	114.214.247.243	36.155.244.189	TCP	54	58095 → 14000 [ACK] Seq=1 Ack=184 Win=4096 Len=0
+	149	3.349786	114.214.247.243	128.119.245.12	IPv4	1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c376) [Reassembled in #150]
+ 150	3.349787	114.214.247.243	128.119.245.12	UDP	134	50037 → 33435 Len=1572
+ 151	3.359172	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	3.359430	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c377) [Reassembled in #153]
153	3.359431	114.214.247.243	128.119.245.12	UDP	134	50037 → 33436 Len=1572
154	3.361915	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
155	3.362144	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c378) [Reassembled in #156]
156	3.362146	114.214.247.243	128.119.245.12	UDP	134	50037 → 33437 Len=1572
157	3.365315	0.0.0.0	114.214.247.243	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	3.365531	114.214.247.243	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=c379) [Reassembled in #159]
159	3.365533	114.214.247.243	128.119.245.12	UDP	134	50037 → 33438 Len=1572
160	3.368589	202.38.96.60	114.214.247.243	IPv4	70	Fragmented IP protocol (proto=ICMP 1, off=0, ID=c379)
252	5.428499	122.51.187.118	114.214.247.243	TCP	74	54938 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1424 SACK_PERM=1 TSval=3413952928 TSecr=0
253	5.428677	114.214.247.243	122.51.187.118	TCP	78	22 → 54938 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 TSval=1322194219 TSecr=0
254	5.442255	122.51.187.118	114.214.247.243	TCP	66	54938 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3413952970 TSecr=1322194219

```

> Ethernet II, Src: Apple3f:b3:57 (14:7d:da:3f:b3:57), Dst: Hangzhou_91:72:e2 (Sciddd70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.247.243, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, EQN: ECT-ECT)
      Total Length: 120
      Identification: 0xc376 (50038)
    > Flags: 0x00b9
      0... .. = Reserved bit: Not set
      .0.. .. = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    > Fragment offset: 1400
    > Time to live: 1
    > Protocol: UDP [17]
    > Payload: UDP [17]
  
```

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

对这两个 fragment 来说, 变的有 Total length, flags, fragment offset, header checksum。

对于所有的第一个和第二个 fragment 来说, 肯定变的有 fragment offset, header checksum。

Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3200.

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

分成了 3 段 fragment.

[illegible]

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

header checksum, fragment offset.

第一个第二个的 more fragments 位是 1, 第三个是 0

第一个第二个的 total length 是 1500, 第三个是 240。

第一个第二个第三个的 fragment offset 分别为 0, 1480, 2960。

```
Total Length: 1500
Identification: 0xc3fb (50171)
Flags: 0x2000, More fragments
  0... .. = Reserved bit: Not set
  .0... .. = Don't fragment: Not set
  ..1... .. = More fragments: Set
Fragment offset: 0
> Time to live: 1
Protocol: UDP (17)
Header checksum: 0xefc7 [validation disabled]
[Header checksum status: Unverified]
Source: 114.214.247.243
Destination: 128.119.245.12
```

```
Total Length: 1500
Identification: 0xc3fb (50171)
Flags: 0x20b9, More fragments
  0... .. = Reserved bit: Not set
  .0... .. = Don't fragment: Not set
  ..1... .. = More fragments: Set
Fragment offset: 1480
> Time to live: 1
Protocol: UDP (17)
Header checksum: 0xef0e [validation disabled]
[Header checksum status: Unverified]
Source: 114.214.247.243
Destination: 128.119.245.12
```

```
Total Length: 240
Identification: 0xc3fb (50171)
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: UDP (17)
Header checksum: 0x1342 [validation disabled]
[Header checksum status: Unverified]
Source: 114.214.247.243
Destination: 128.119.245.12
```