WireShark 实验-IP

专业班级： 信息安全智息技术班　　**学号：** 21307130076　　**姓名：** 杨乙

【实验目的】

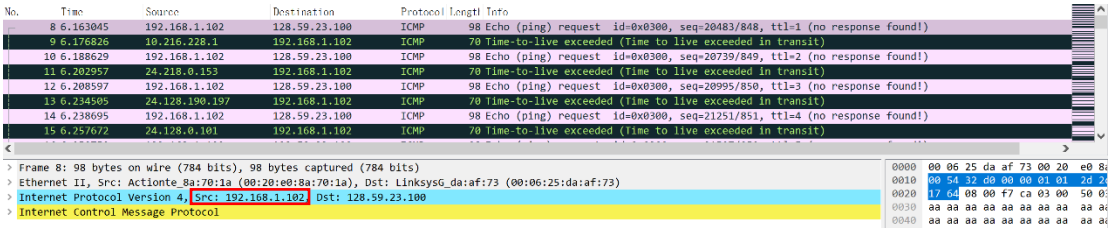
探索 IP 协议

【实验结果】

分析操作，回答问题。

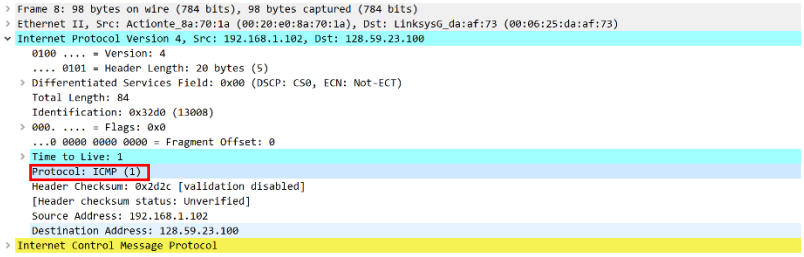
（本实验使用的数据包是网站上给出的数据包）

1. 选择发送的第一个 ICMP Echo Request 消息，然后在 packet details window 中展开数据包的 Internet 协议部分。您的 IP 地址是多少？



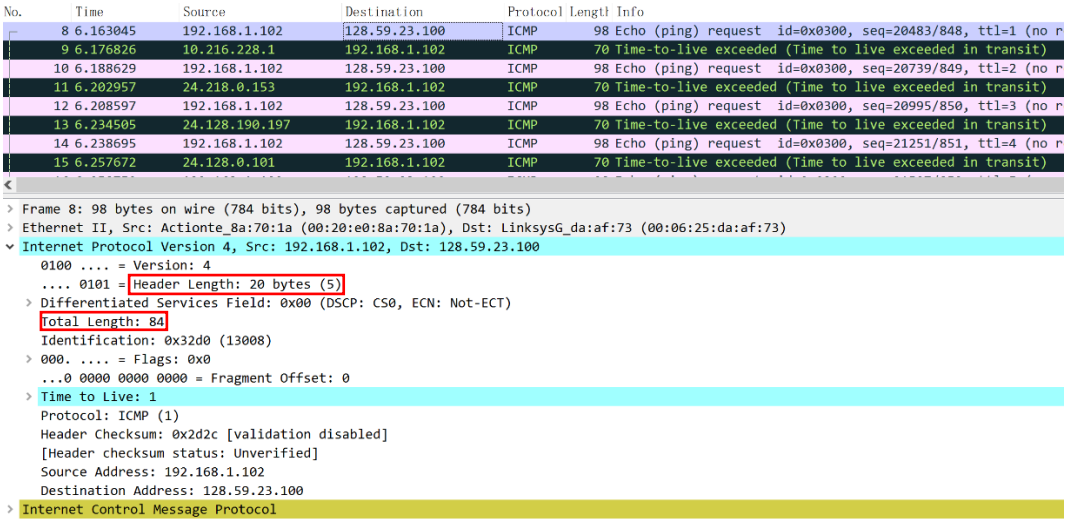
如图，我的 IP 地址为 192.168.1.102

2. 在 IP header 中，上层协议字段的值是多少？



上层协议字段的值为 1

3. IP header 有多少 bytes？IP datagram 的有效负载中有多少 bytes？说明如何确定 payload bytes 的数。

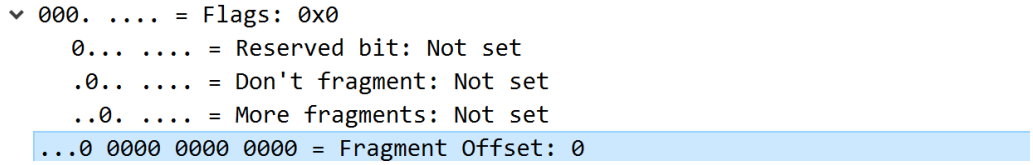


如图，IP header = 20 bytes，Total Length = 84 bytes

因此 IP datagram payload bytes = 84 - 20 = 64 bytes

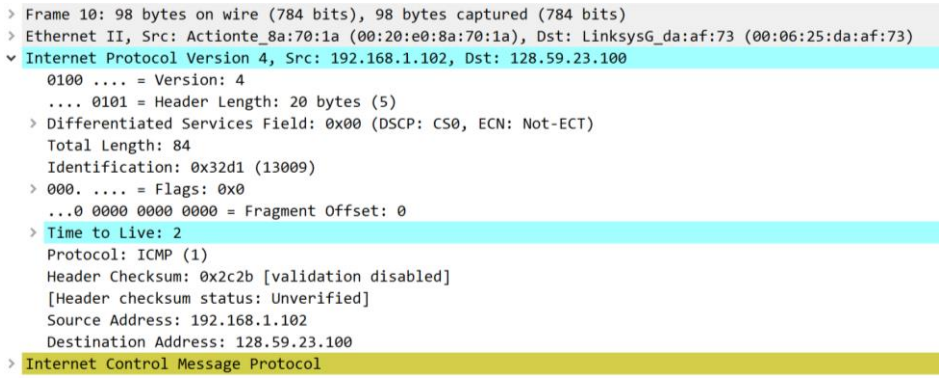
也可以直接查看 icmp 的字节数

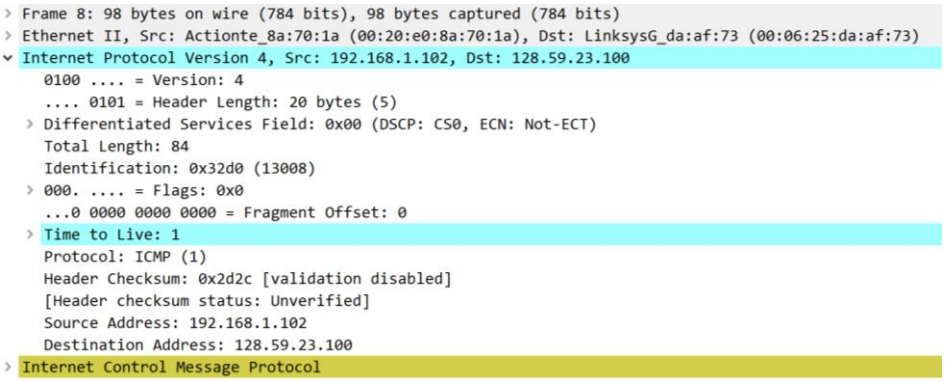
4. 此 IP 数据报是否已被分段(fragmented)？解释您如何确定数据报是否已被分段(fragmented)。



没有分段。因为 Fragments Offset 为 0。且 More fragments 值为 Not set，表示未设置分段

5. 在您发送的这一系列 ICMP 消息中，IP 数据报中的哪些字段一直改变?





通过对比两个不同的 ICMP 消息，发现 IP 数据报中一直改变的字段有：
TTL、Identification、Header Checksum
因为每一跳导致 TTL 减 1，因此 TTL 会改变；
Identification 用于唯一标志一个报文的所有分片，因为未进行分片，所以一直改变；
首部有字段改变，导致 Header Checksum 改变

6. 哪些字段保持不变? 哪个字段必须保持不变? 哪些字段必须更改? 为什么?

保持不变：
1. Total Length：因为在一次 traceroute 中，首部长度固定，数据长度不变。因此 IP 数据报总长度不变
2. Source Address：报文的发送端固定
3. Destination Address：报文的接收端固定
4. Fragment Offset：指明了每个分片相对于原始报文开头的偏移量。因为未进行分片，所以保持不变
5. 标志：对于此字段，分片时最后一个片为 0，前边所有片为 1。因为未进行分片，所以保持不变
6. 选项：在一次 traceroute 中选项字段不变

必须保持不变：

1. Version：因为使用的都是 IPv4 协议，所以 Version 字段为 4
2. 首部长度：所有首部字段中，选项字段不变，其他字段长度固定，因此首部长度不变
3. 服务类型：因为不使用区分服务，所以此字段保持不变
4. 协议：都是 ICMP(1)

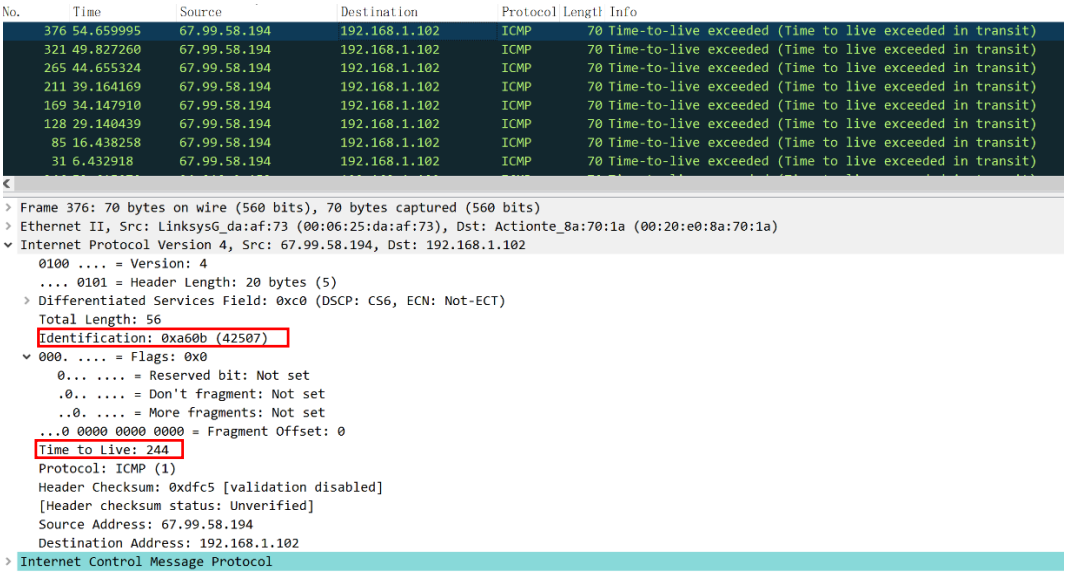
必须更改：

1. Identification：用来唯一地标识一个报文的所有分片，因为未进行分片，所以会改变
2. TTL：因为每一跳导致 TTL 减 1，因此 TTL 会改变
3. Header Checksum：首部有字段改变，导致 Header Checksum 改变
4. 数据：每次传输数据不同，因此改变

7. 描述您在 IP datagram 的 Identification field 中的值中所看到的下一步(数据包仍按来源地址排序)查找最近的(第一跳)路由器发送到您的计算机的一系列 ICMP TTL 超出的回复讯息。

这些回复讯息的 Identification 值各不相同。这一字段用来唯一地标识一个报文的所有分片，因为未进行分片，所以会改变

8. ID 字段和 TTL 字段的值是多少?



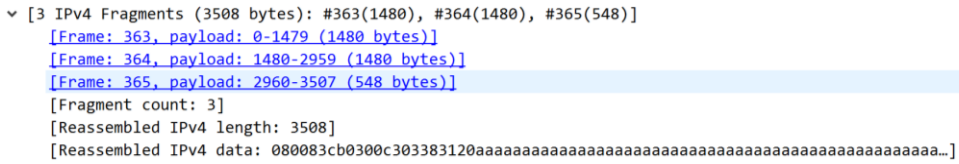
如图，ID 字段值为 0xa60b

TTL 字段值为 244

9. 对于第一跳路由器发送到您的计算机的所有 ICMP TTL 超出的回复，这些值是否保持不变？为什么？

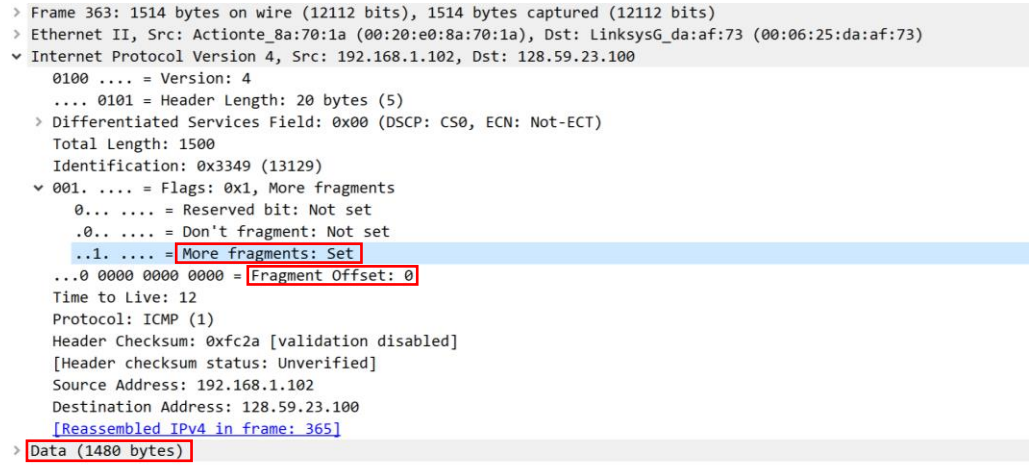
ID 字段改变，因为是不同的数据报
TTL 字段不变（都为 244）。因为 TTL 值都减一

10. 在将 pingplotter 中的数据包大小更改为 2000 后，查找计算机发送的第一个 ICMP Echo Request 消息。该消息是否已碎片化为多个 IP 数据报？



如图，该消息已碎片化为 3 个 IP 数据报

11. IP 数据报的第一个片段。IP 头中的哪些信息表明数据报已碎片化？IP 头中的哪些信息表明这是第一个片段还是后一个片段？这个 IP 数据报有多长？



More fragments 为 Set 表示数据段已碎片化
Fragment Offset 为 0 表明这是第一个片段
Data 字段长 1480 bytes，Header Length 为 20 bytes，IP 数据报长度为 1480 + 20 = 1500 bytes

12. 找到碎片 IP 数据报的第二个片段。IP 标头中的哪些信息表明这不是第一个数据报片段？是否还有更多的片段？你是如何知道的？

```
> Frame 364: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3349 (13129)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 12
    Protocol: ICMP (1)
    Header Checksum: 0xfb71 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 365]
> Data (1480 bytes)
```

Fragment Offset 非 0 表示不是第一个片段

```
v [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
    [Frame: 363, payload: 0-1479 (1480 bytes)]
    [Frame: 364, payload: 1480-2959 (1480 bytes)]
    [Frame: 365, payload: 2960-3507 (548 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3508]
    [Reassembled IPv4 data: 080083cb0300c303383120aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa…]
```

如图，还有更多的片段

13. 在第一个和第二个片段中，IP 标头中哪些字段发生了变化？

```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3349 (13129)
  v 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: 12
    Protocol: ICMP (1)
    Header Checksum: 0xfc2a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 365]
> Data (1480 bytes)
```

```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3349 (13129)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 12
    Protocol: ICMP (1)
    Header Checksum: 0xfb71 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 365]
> Data (1480 bytes)
```

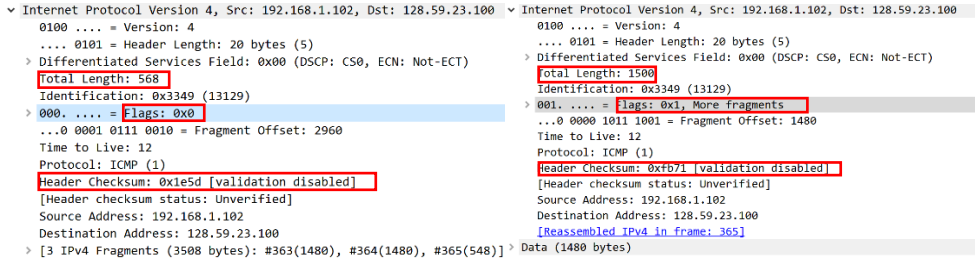
如图，Fragments Offset 和 Header Checksum 字段发生了变化

14. 从原始数据报创建了多少个片段？

```
v [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
    [Frame: 363, payload: 0-1479 (1480 bytes)]
    [Frame: 364, payload: 1480-2959 (1480 bytes)]
    [Frame: 365, payload: 2960-3507 (548 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3508]
    [Reassembled IPv4 data: 080083cb0300c303383120aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa…]
```

如图，创建了三个片段

15. 片段中 IP 头中的哪些字段发生了变化?



如图，Total Length 字段、Flags 字段（标志）、Header Checksum 字段发生了变化