



南开大学
Nankai University

《计算机网络》实验报告

(2022~2023 学年第一学期)

实验名称：IP与ICMP分析

学 院：软件学院

姓 名：郁万祥

学 号：2013852

指导老师：张圣林

2022 年 11 月 22

实验名称 (实验 2:IP与ICMP分析)

1 实验目的

IP 和 ICMP 协议是 TCP/IP 协议簇中的网络层协议，在网络寻址定位、数据分组转发和路由选择等任务中发挥了重要作用。本实验要求熟练使用 Wireshark 软件，观察 IP 数据报的基本结构，分析数据报的分片；掌握基于 ICMP 协议的 ping 和 tracert 命令其工作原理。

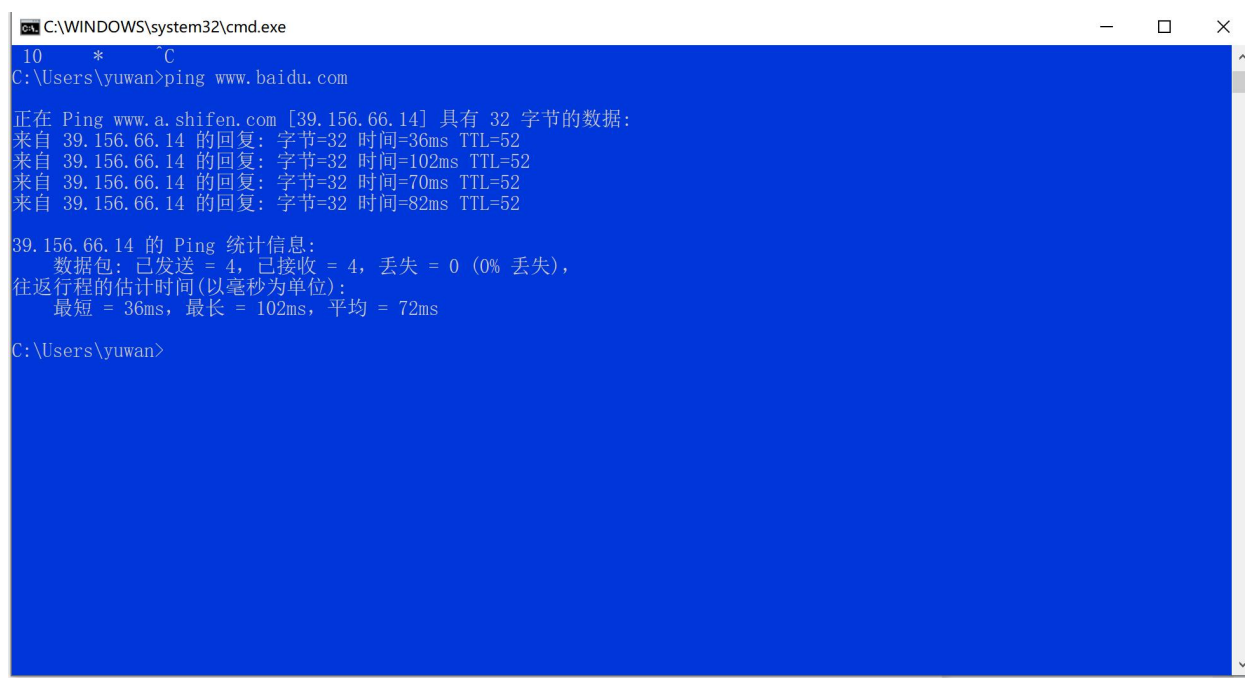
2 实验条件

装有 Wireshark 软件的 PC 机一台，处于局域网环境

3 实验报告内容及原理

1、实行ping命令（以ping www.baidu.com为例），解释任意一个IP数据报的首部。

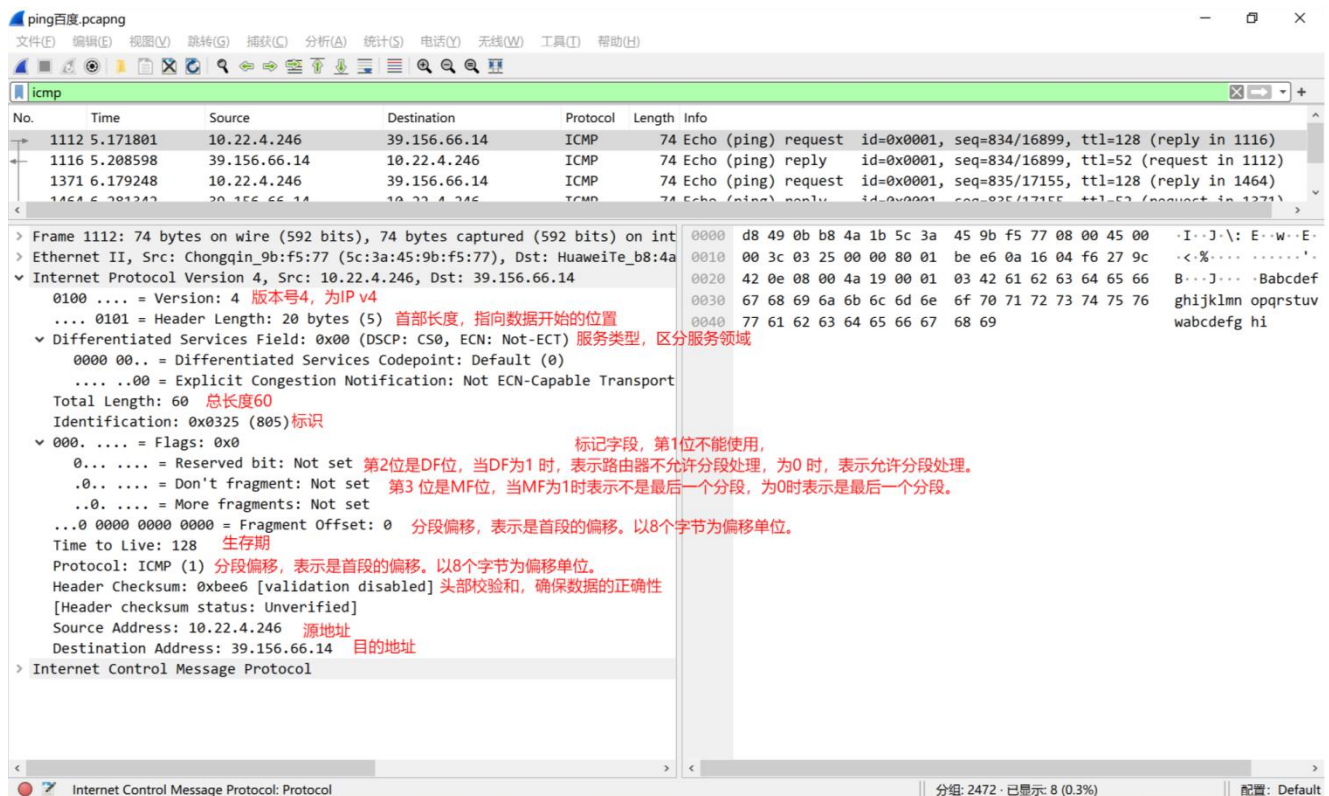
文件见 ping百度.pcapng



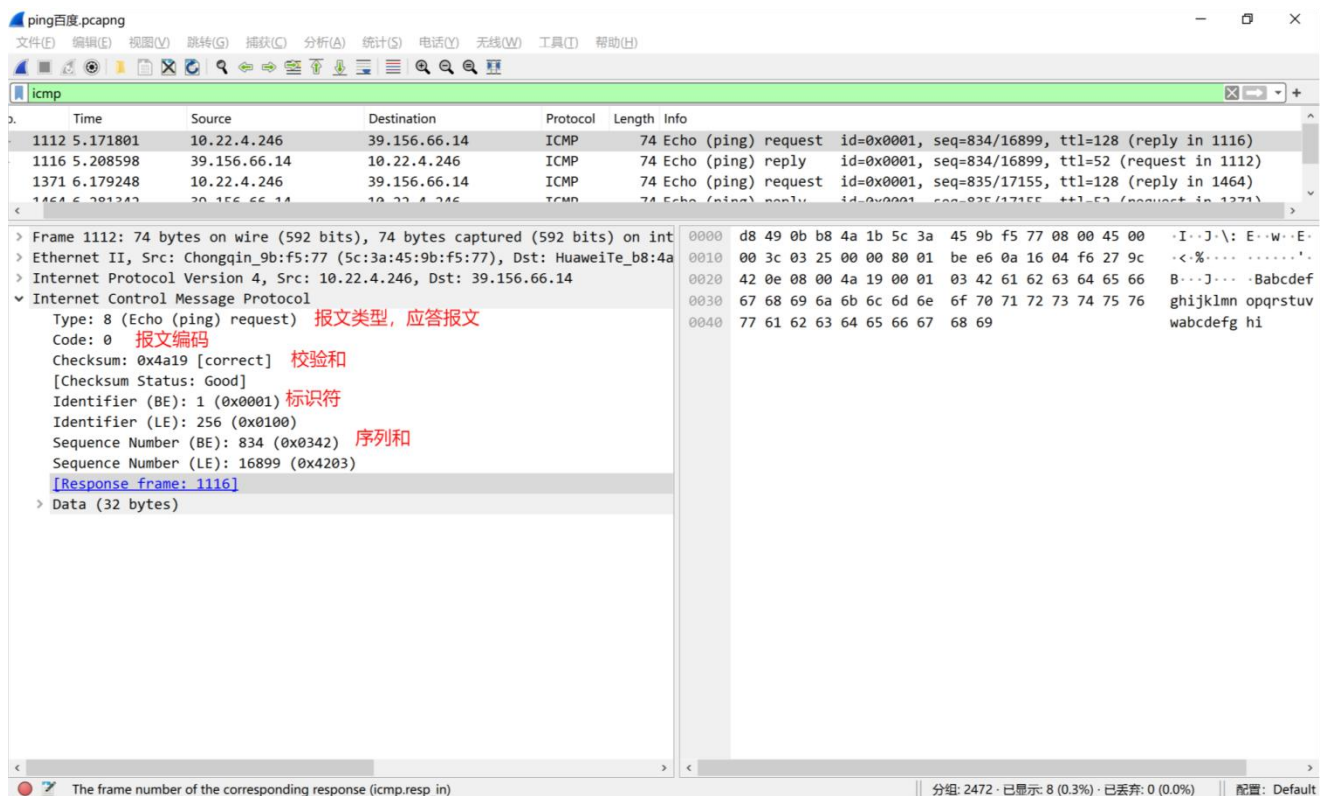
```
C:\WINDOWS\system32\cmd.exe
10 * ^C
C:\Users\yuwan>ping www.baidu.com

正在 Ping www.a.shifen.com [39.156.66.14] 具有 32 字节的数据:
来自 39.156.66.14 的回复: 字节=32 时间=36ms TTL=52
来自 39.156.66.14 的回复: 字节=32 时间=102ms TTL=52
来自 39.156.66.14 的回复: 字节=32 时间=70ms TTL=52
来自 39.156.66.14 的回复: 字节=32 时间=82ms TTL=52

39.156.66.14 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 = 36ms, 最长 = 102ms, 平均 = 72ms
C:\Users\yuwan>
```

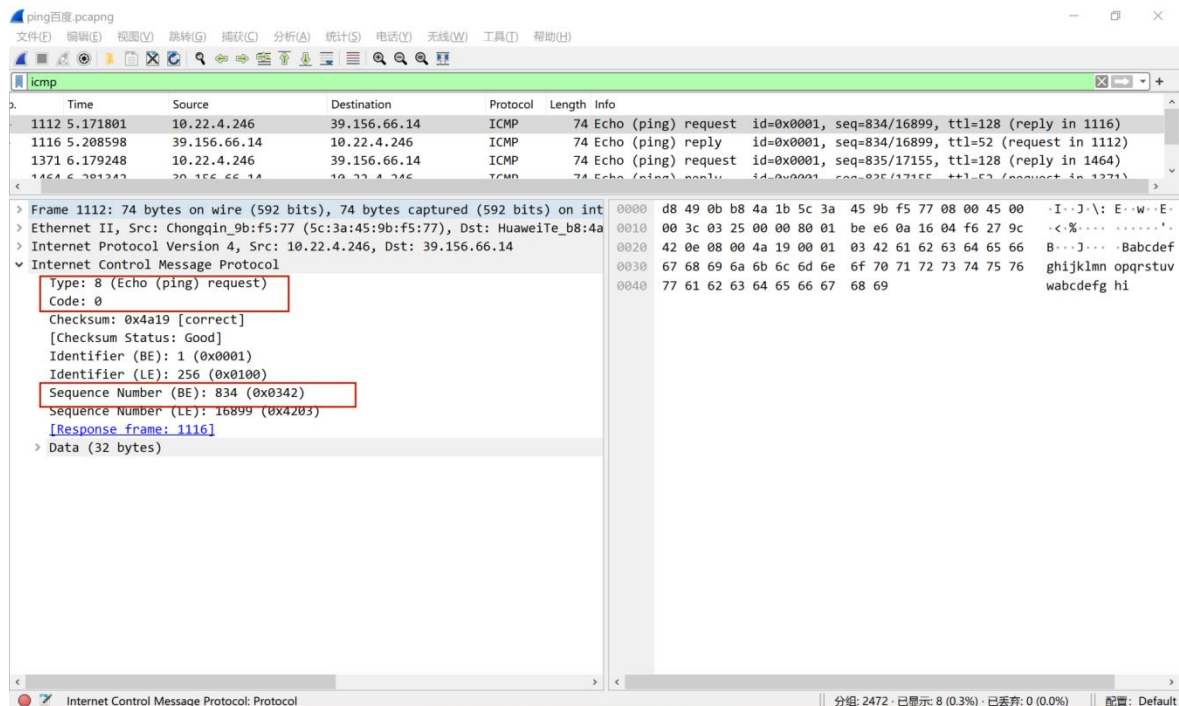


2、对上述ping命令中的任意一个ICMP协议进行分析。

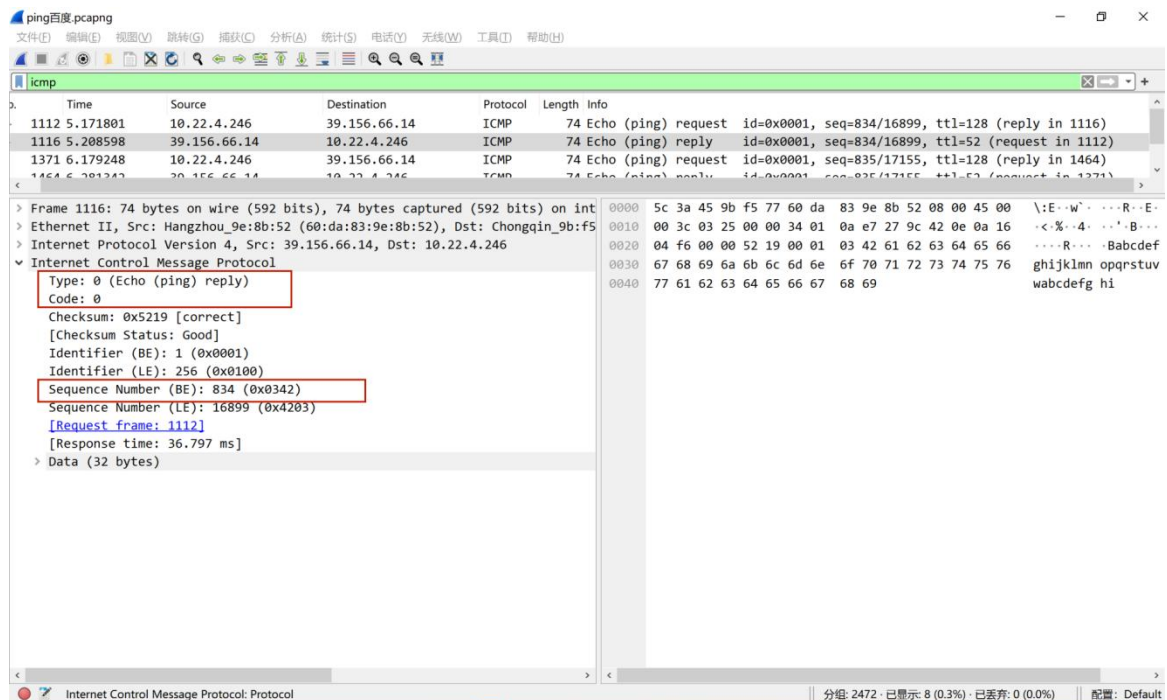


3、对上述ping命令得到的Echo请求帧和回应帧进行对比。

请求帧：



回应帧：



请求类型是8，代码是0，表示请求，回应类型是0，代码是0，表示应答。

回应和请求的Identifier (BE) 均834 (0x342)，说明该回应是响应的该请求。

IP头部字段Src和Dst相反，TTL也不同。

4、改变ping的长度参数（1000、2000、4000），（以ping sina.com.cn为例）解释IP数据包的分片情况。

```
C:\WINDOWS\system32\cmd.exe

C:\Users\yuwan>ping sina.com.cn -l 2000

正在 Ping sina.com.cn [49.7.37.133] 具有 2000 字节的数据:
来自 49.7.37.133 的回复: 字节=2000 时间=26ms TTL=49
来自 49.7.37.133 的回复: 字节=2000 时间=27ms TTL=49
来自 49.7.37.133 的回复: 字节=2000 时间=25ms TTL=49
来自 49.7.37.133 的回复: 字节=2000 时间=46ms TTL=49

49.7.37.133 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 = 25ms, 最长 = 46ms, 平均 = 31ms

C:\Users\yuwan>ping sina.com.cn -l 4000

正在 Ping sina.com.cn [49.7.37.133] 具有 4000 字节的数据:
来自 49.7.37.133 的回复: 字节=4000 时间=36ms TTL=49
来自 49.7.37.133 的回复: 字节=4000 时间=35ms TTL=49
来自 49.7.37.133 的回复: 字节=4000 时间=19ms TTL=49
来自 49.7.37.133 的回复: 字节=4000 时间=18ms TTL=49

49.7.37.133 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 = 18ms, 最长 = 36ms, 平均 = 27ms

C:\Users\yuwan>
```

文件见 ping新浪1000.pcapng、ping新浪2000.pcapng、ping新浪4000.pcapng

①Ping sina.com.cn -l 1000

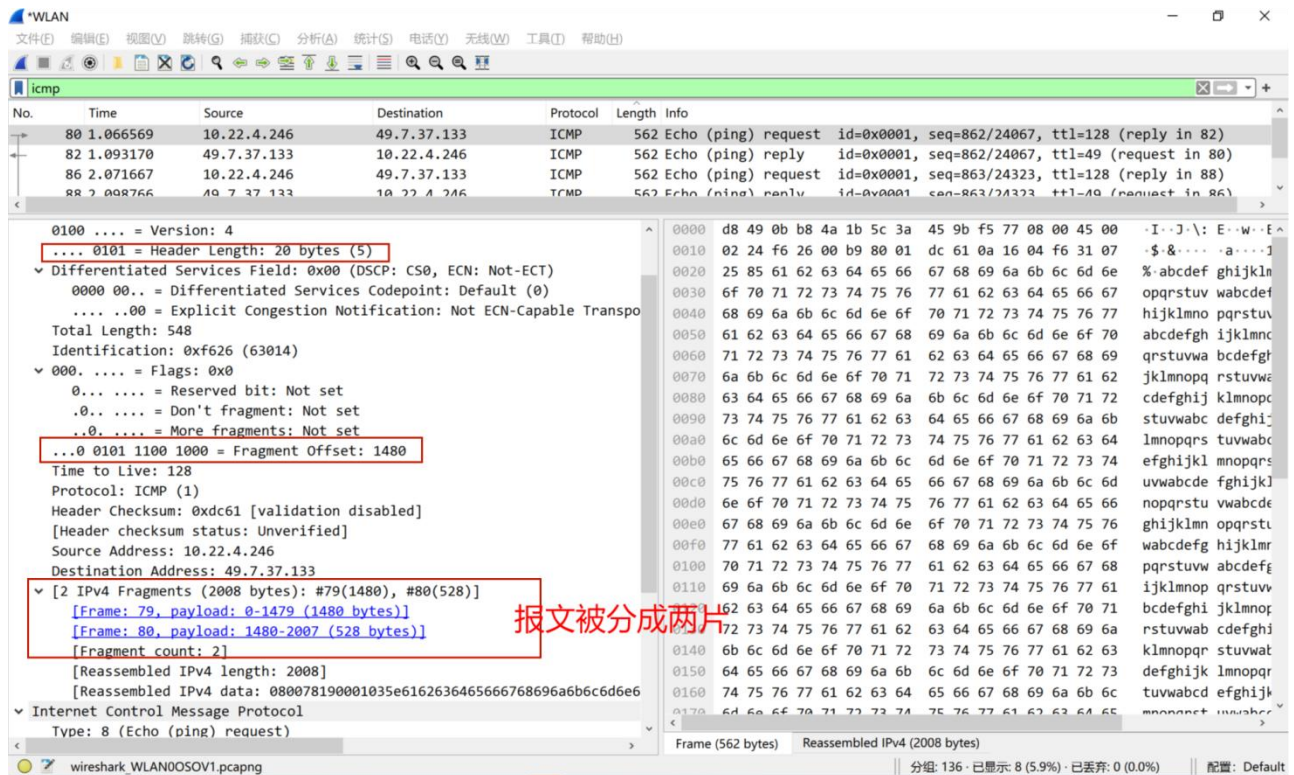
The image shows a Wireshark packet capture analysis of a ping command with length 1000. The packet list shows several ICMP Echo (ping) request and reply packets. The packet details pane shows the structure of an ICMP Echo request, including the header and data field. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	1.252564	10.22.4.246	49.7.37.133	ICMP	1042	Echo (ping) request id=0x0001, seq=850/20995, ttl=128 (reply in 10)
10	1.283389	49.7.37.133	10.22.4.246	ICMP	1042	Echo (ping) reply id=0x0001, seq=850/20995, ttl=49 (request in 9)
14	2.259142	10.22.4.246	49.7.37.133	ICMP	1042	Echo (ping) request id=0x0001, seq=851/21251, ttl=128 (reply in 15)
15	2.290341	49.7.37.133	10.22.4.246	ICMP	1042	Echo (ping) reply id=0x0001, seq=851/21251, ttl=49 (request in 14)
19	3.264460	10.22.4.246	49.7.37.133	ICMP	1042	Echo (ping) request id=0x0001, seq=852/21507, ttl=128 (reply in 20)
20	3.280646	49.7.37.133	10.22.4.246	ICMP	1042	Echo (ping) reply id=0x0001, seq=852/21507, ttl=49 (request in 19)
27	4.270298	10.22.4.246	49.7.37.133	ICMP	1042	Echo (ping) request id=0x0001, seq=853/21763, ttl=128 (reply in 28)
28	4.299521	49.7.37.133	10.22.4.246	ICMP	1042	Echo (ping) reply id=0x0001, seq=853/21763, ttl=49 (request in 27)

Frame 9: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on 0
> Ethernet II, Src: Chongqin_9b:f5:77 (5c:3a:45:9b:f5:77), Dst: HuaweiTe_b8:
Internet Protocol Version 4, Src: 10.22.4.246, Dst: 49.7.37.133
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 Transpo
Total Length: 1028
Identification: 0xf61a (63002)
000. = Flags: 0x0
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0xdb46 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.22.4.246
Destination Address: 49.7.37.133

因为ping下来的都是长度为1000的数据，而以太网中的MTU为1500，所以不存在分片。

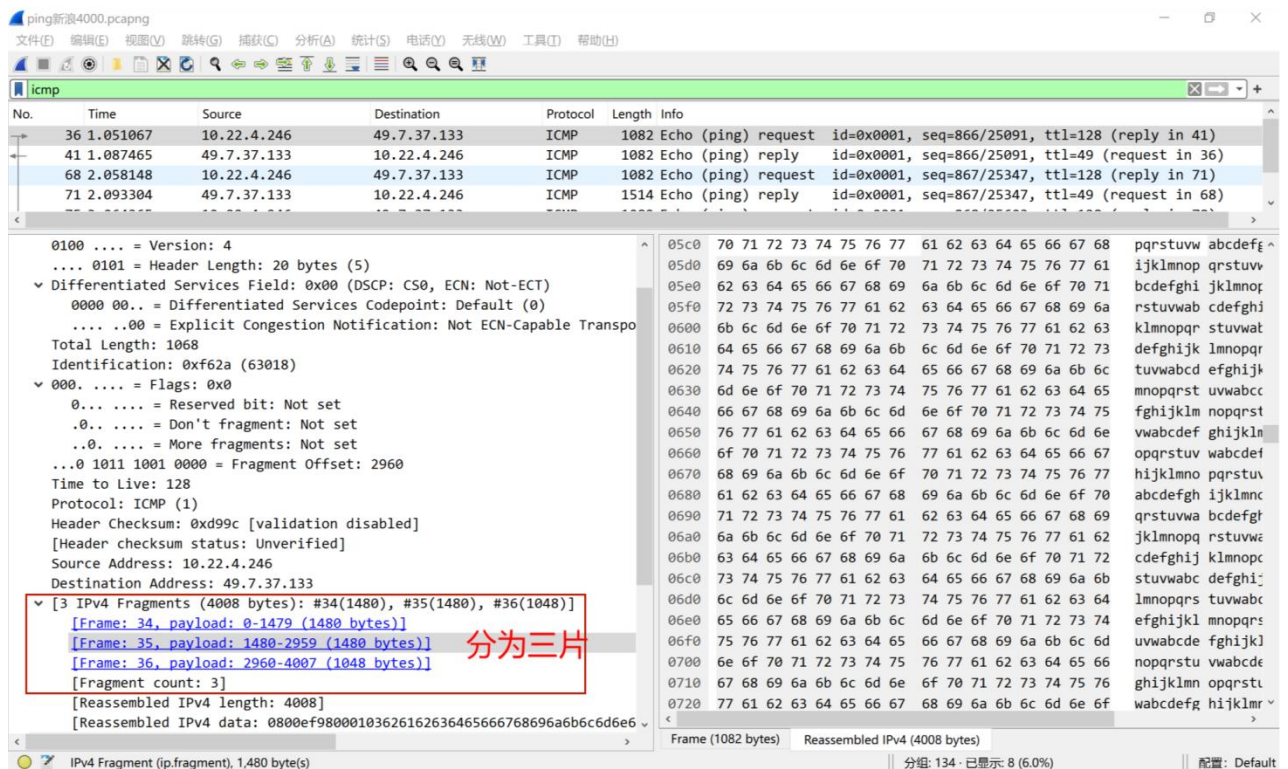
②Ping sina.com.cn -l 2000



MTU计算：我们可以看到，此时分片为2，而分片偏移为1480，再加上头部长度为20，所以说第二段的报文头部所在位置为1501，也就是第一片报文长度为1500，也就是MTU。

此时ping到的是数据长度为2000的数据报文，然而MTU为1500，所以需要将每一条ICMP报文分成两片。

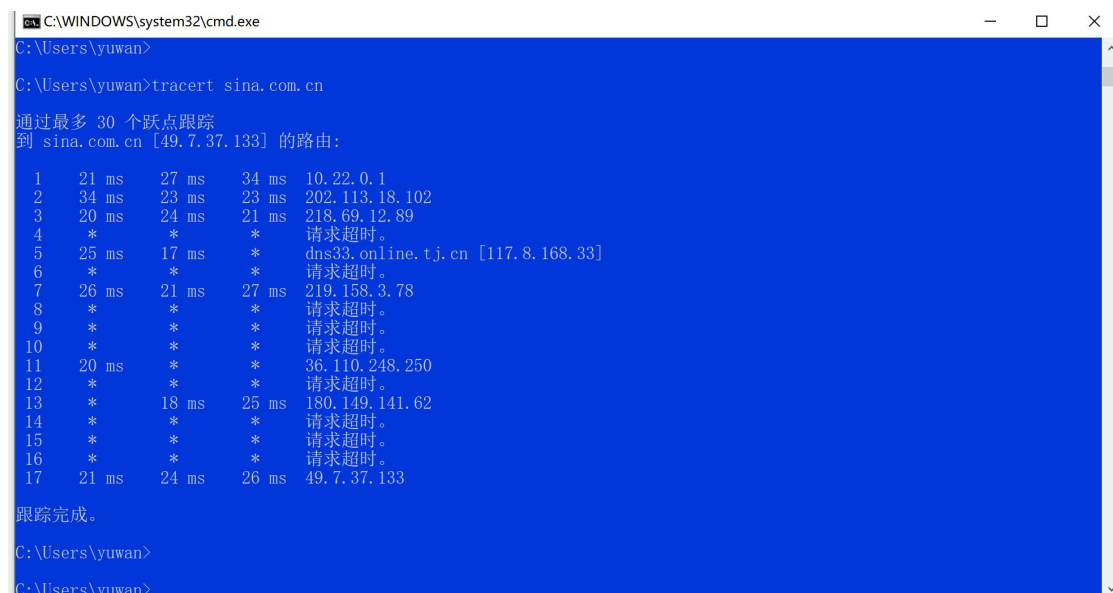
③Ping sina.com.cn -l 4000

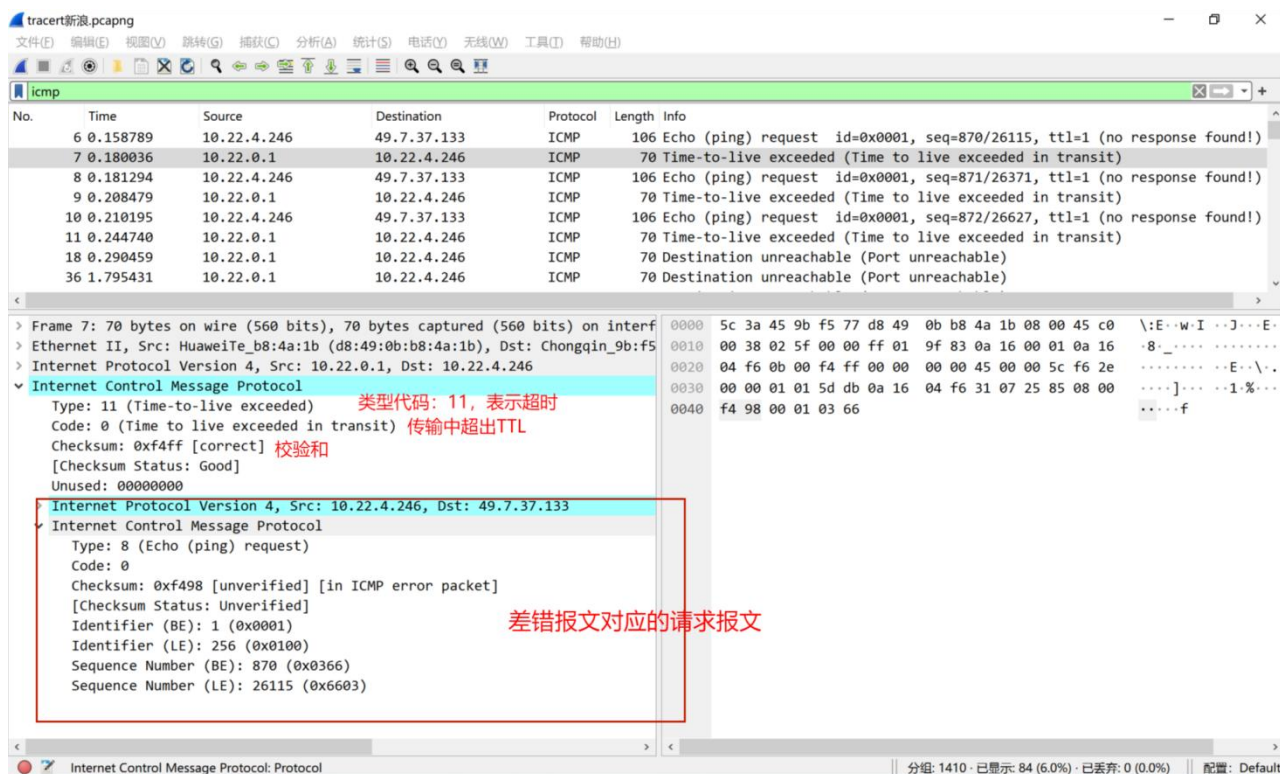


此时ping到的是数据长度为4000的数据报文，然而MTU为1500，所以需要将每一条ICMP报文分成三片。

5、实时tracert命令（以tracert sina.com.cn为例），解释任意一个ICMP差错报文的结构。

文件见tracert新浪.pcapng。





6、描述tracert工作过程

Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

首先, tracert 送出一个 TTL 是 1 的 IP 数据包到目的地, 当路径上的第一个路由器收到这个数据包时, 它将 TTL 减 1。此时, TTL 变为 0, 所以该路由器会将此数据包丢掉, 并送回一个「ICMP time exceeded」消息 (包括发 IP 包的源地址, IP 包的所有内容及路由器的 IP 地址),

tracert 收到这个消息后, 便知道这个路由器存在于这个路径上, 接着 tracert 再送出另一个 TTL 是 2 的数据包, 发现第 2 个路由器.....

tracert 每次将送出的数据包的 TTL 加 1 来发现另一个路由器, 这个重复的动作一直持续到某个数据包抵达目的地。当数据包到达目的地后, 该主机则不会送回 ICMP time exceeded 消息, 一旦到达目的地, 由于 racert 通过 UDP 数据包向不常见端口 (30000 以上) 发送数据包, 因此会收到「ICMP port unreachable」消息, 故可判断到达目的地。

tracert 新浪.pcapng

文件(F) 编辑(E) 视图(V) 跳转(S) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

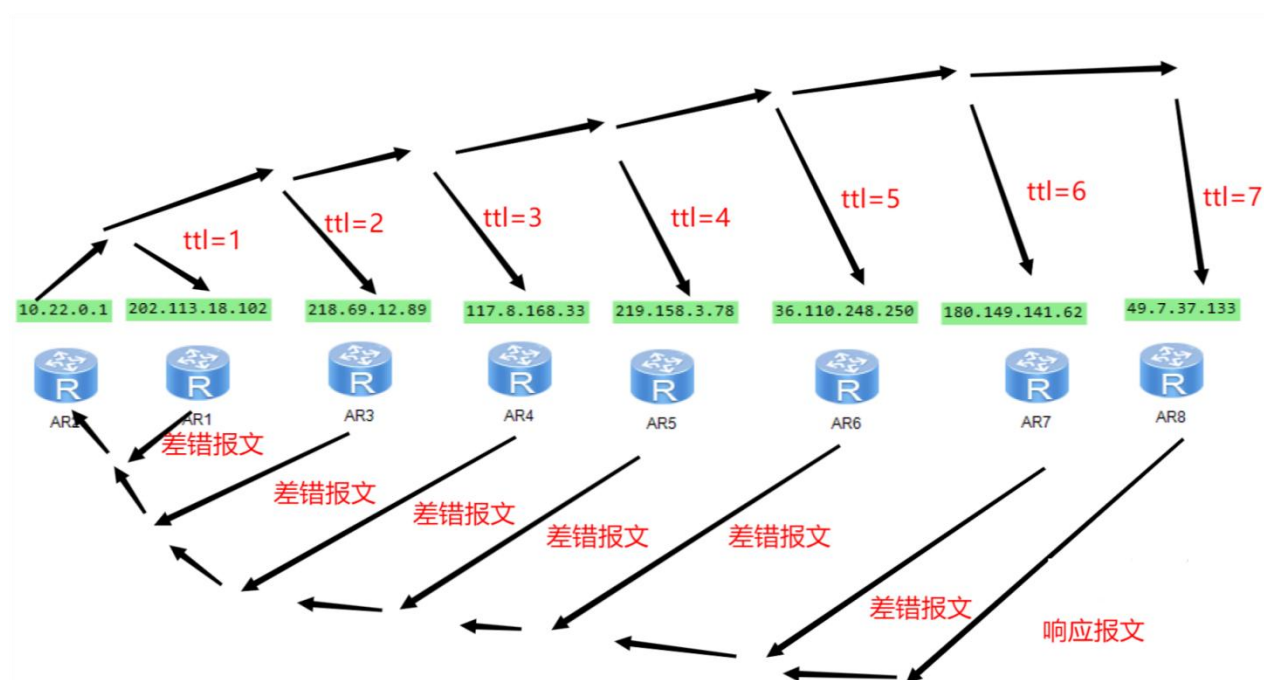
icmp

No.	Time	Source	Destination	Protocol	Length	Info
6	0.158789	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=870/26115, ttl=1 (no response found!)
7	0.180036	10.22.0.1	10.22.4.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
8	0.181294	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=871/26371, ttl=1 (no response found!)
9	0.208479	10.22.0.1	10.22.4.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	0.210195	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=872/26627, ttl=1 (no response found!)
11	0.244740	10.22.0.1	10.22.4.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	0.290459	10.22.0.1	10.22.4.246	ICMP	70	Destination unreachable (Port unreachable)
36	1.795431	10.22.0.1	10.22.4.246	ICMP	70	Destination unreachable (Port unreachable)
45	3.298566	10.22.0.1	10.22.4.246	ICMP	70	Destination unreachable (Port unreachable)
64	5.750141	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=873/26883, ttl=2 (no response found!)
65	5.784273	202.113.18.102	10.22.4.246	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
66	5.785962	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=874/27139, ttl=2 (no response found!)
67	5.808810	202.113.18.102	10.22.4.246	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
68	5.810161	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=875/27395, ttl=2 (no response found!)
69	5.833364	202.113.18.102	10.22.4.246	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
148	11.358360	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=876/27651, ttl=3 (no response found!)
149	11.378604	218.69.12.89	10.22.4.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
150	11.379899	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=877/27907, ttl=3 (no response found!)
151	11.404537	218.69.12.89	10.22.4.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
152	11.406044	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=878/28163, ttl=3 (no response found!)
153	11.427611	218.69.12.89	10.22.4.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
157	11.465931	218.69.12.89	10.22.4.246	ICMP	70	Destination unreachable (Port unreachable)
159	12.977066	218.69.12.89	10.22.4.246	ICMP	70	Destination unreachable (Port unreachable)
162	14.485603	218.69.12.89	10.22.4.246	ICMP	70	Destination unreachable (Port unreachable)
207	16.948610	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=879/28419, ttl=4 (no response found!)
223	20.468614	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=880/28675, ttl=4 (no response found!)
256	24.468571	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=881/28931, ttl=4 (no response found!)
287	28.470516	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=882/29187, ttl=5 (no response found!)
288	28.495452	117.8.168.33	10.22.4.246	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
289	28.496765	10.22.4.246	49.7.37.133	ICMP	106	Echo (ping) request id=0x0001, seq=883/29443, ttl=5 (no response found!)

Internet Control Message Protocol: Protocol

分组: 1410 · 已显示: 84 (6.0%) · 已丢弃: 0 (0.0%) 配置: Default

7、结合上述得到的ICMP报文记录画出数据交互示意。



4 实验结论及心得体会

1、经常ping命令会显示timeout：可能是网络问题，可以多ping几次，或者换几个ip地址进行ping命令。

2、分片的数据包不能够查看，将wireshark首选项里面关掉一个Ipv4的选项，才能显示所有帧的信息。