
实验六 IP

张舒恒 PB19030888

实验目的

1. 了解 IP 协议和IP数据报
2. 了解 ICMP 协议，TTL 的作用了解 TCP 的拥塞控制算法
3. 了解 IP 数据报的字段的意义
4. 研究 IP 数据的分片方法

实验环境

pc一台，win10操作系统，wireshark工具， pingplotter工具， 浏览器

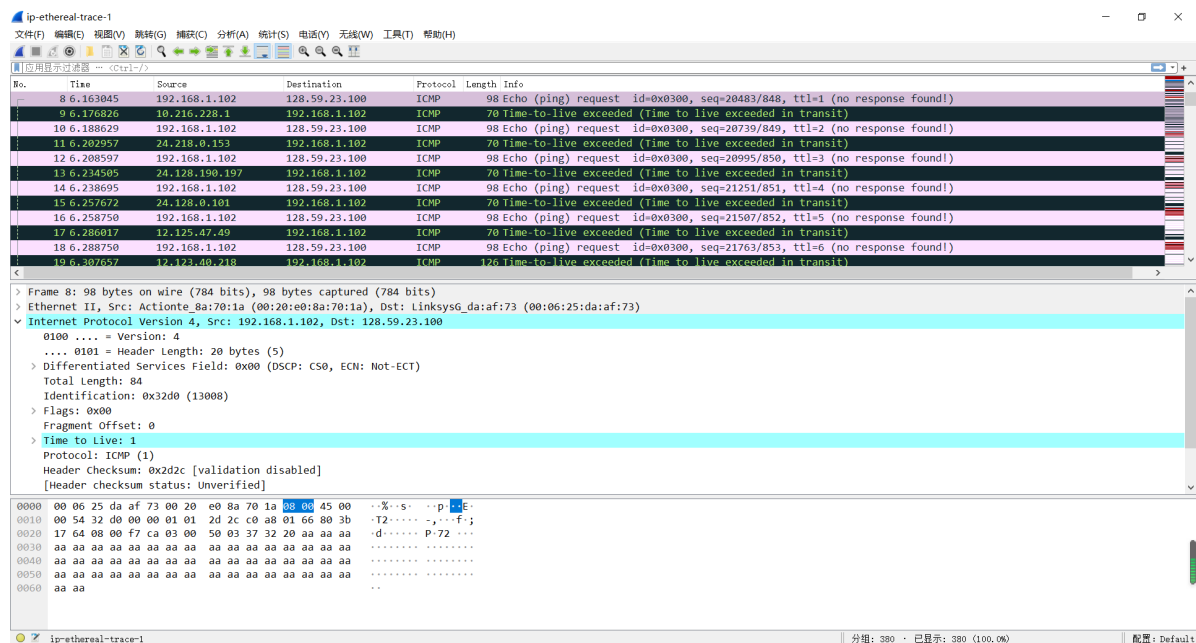
实验步骤

1. 下载 pingplotter工具， 安装并选择专业版14天试用。
2. 打开pingplotter， 通过选择菜单项 Edit-> Options-> Packet Options 然后填写 Packet Size 字段，将包大小设置为56字节
3. 启动 Wireshark 并开始数据包捕获（Capture-> Start），然后在 Wireshark 数据包捕获选项屏幕上按 OK
4. 打开 pingplotter 并在“要跟踪的地址窗口”中输入目标目标的名称。在“要跟踪的次数”字段中输入 3，这样就不会收集太多数据。选择菜单项编辑 ->高级选项 ->数据包选项，然后在数据包大小字段中输入值 56，然后按确定(这里我在第一次下载安装时已经完成)。然后按 Trace 按钮。
5. 通过选择编辑 ->高级选项 ->数据包选项并在数据包大小字段中输入值 2000，然后按确定，发送一组长度较长的数据报。然后按“继续”按钮。
6. 通过选择编辑 ->高级选项 ->数据包选项并在数据包大小字段中输入值 3500，然后按确定，发送一组长度较长的数据报。然后按“继续”按钮。
7. 停止 Wireshark 数据包捕获

问题回答

这里我用的都是作者的抓包结果，特此声明。

- 1.作者计算机IP地址：192.168.1.102



2.上层协议字段的值是 1

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x32d0 (13008)
> Flags: 0x00
Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2d2c [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

3.IP 头文件20字节, IP 报总长度84字节, 则IP 数据长度是64字节

```
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: 84
```

4.找到IP头标志位的More fragments选项, 发现没有开启, 所以这个IP数据报没有被分段

```
Flags: 0x00
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment Offset: 0
```

5.标识符(Identification), 存活时间(Time to Live), IP 头校验和(Header Checksum)一直在变

```
Identification: 0x32d0 (13008)
> Flags: 0x00
  Fragment Offset: 0
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
```

```
Identification: 0x9d7c (40316)
> Flags: 0x00
  Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x6ca0 [validation disabled]
```

```
Identification: 0x32d1 (13009)
> Flags: 0x00
  Fragment Offset: 0
> Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x2c2b [validation disabled]
```

6. version, header length, Differentiated Service Field, Total Length, flags, fragment offset, protocol, source address, destination address字段都没有发生变化。

Version, header length, Differentiated Service Field, protocol, source address, destination address必定不变。因为使用的是IPv4所以Version必然不变。ICMP的header length固定20bytes必然不变。这里都是用ICMP服务, 所以Differentiated Service Field和protocol字段必然不变。源地址和目的地址也必然不变。

Identification、Time to Live、Header Checksum是必须变的。Identification是IP包的标识, 所以不同IP包必须有不同的ID, traceroute会递增修改TTL值所以必须变, Header Checksum是头的校验和也要变。

7. 每一个IP 数据报中的标识字段的值都不一样并且每次加1

```
Identification: 0x32d0 (13008)
> Flags: 0x00
  Fragment Offset: 0
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
```

```
Identification: 0x32d1 (13009)
> Flags: 0x00
  Fragment Offset: 0
> Time to Live: 2
  Protocol: ICMP (1)
  Header Checksum: 0x2c2b [validation disabled]
```

Identification: 0x32d2 (13010)

Flags: 0x00

Fragment Offset: 0

Time to Live: 3

Protocol: ICMP (1)

Header Checksum: 0x2b2a [validation disabled]

8. Identification: 40316

Time to Live: 255

Wireshark packet capture showing an ICMP Echo request. The packet details pane shows the following information:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x9d7c (40316)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 255
- Protocol: ICMP (1)
- Header Checksum: 0x6ca0 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.216.228.1
- Destination Address: 192.168.1.102

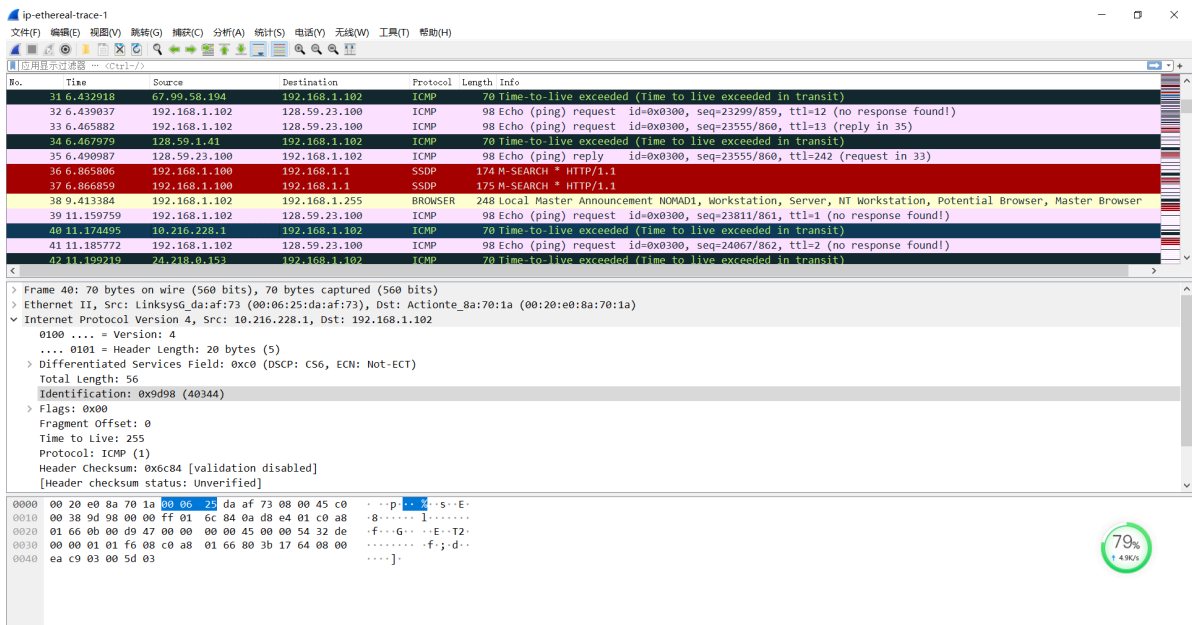
The packet bytes are displayed at the bottom of the packet details pane.

9. ID 字段改变, TTL 字段不变。每个路由器都有一个固定的TTL, 所以最近的路由器回复的所有TTL exceeded的TTL值不变。ID是IP包的标识符, 所以不同IP包ID不一样

Wireshark packet capture showing an ICMP Echo request. The packet details pane shows the following information:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x9d7c (40316)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 255
- Protocol: ICMP (1)
- Header Checksum: 0x6ca0 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.216.228.1
- Destination Address: 192.168.1.102

The packet bytes are displayed at the bottom of the packet details pane.



10.该消息已碎片化为多个 IP 数据报，第一个数据报显示协议IPV4的IP分片，第二个数据报显示ICMP的PING剩下部分。

92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)

Destination Address: 128.59.23.100

▼ [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]

[\[Frame: 92, payload: 0-1479 \(1480 bytes\)\]](#)

[\[Frame: 93, payload: 1480-2007 \(528 bytes\)\]](#)

[Fragment count: 2]

11.通过 IP 数据头的标志位More fragments可以发现已经被分段，通过偏移量发现这是第一个片段，这个数据报有1500字节

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

Total Length: 1500

Identification: 0x32f9 (13049)

▼ Flags: 0x20, More fragments

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

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

..1. = More fragments: Set

Fragment Offset: 0

12.通过 IP 数据头的标志位More fragments可以发现后面没有更多的分段，通过偏移量发现这不是第一个片段

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

Total Length: 548

Identification: 0x32f9 (13049)

▼ Flags: 0x00

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

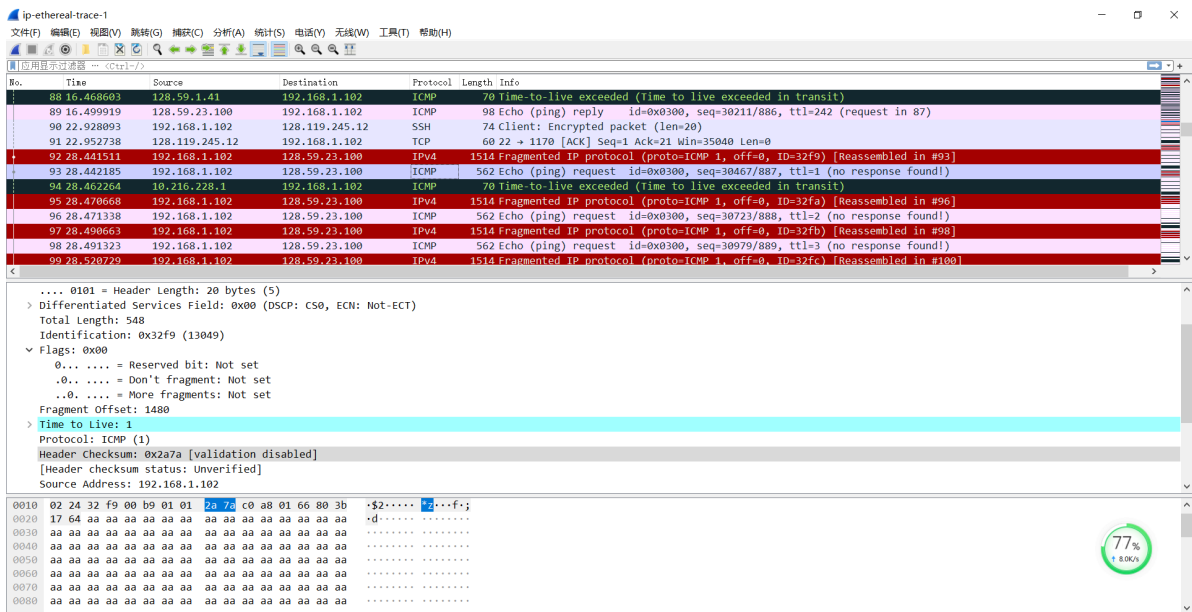
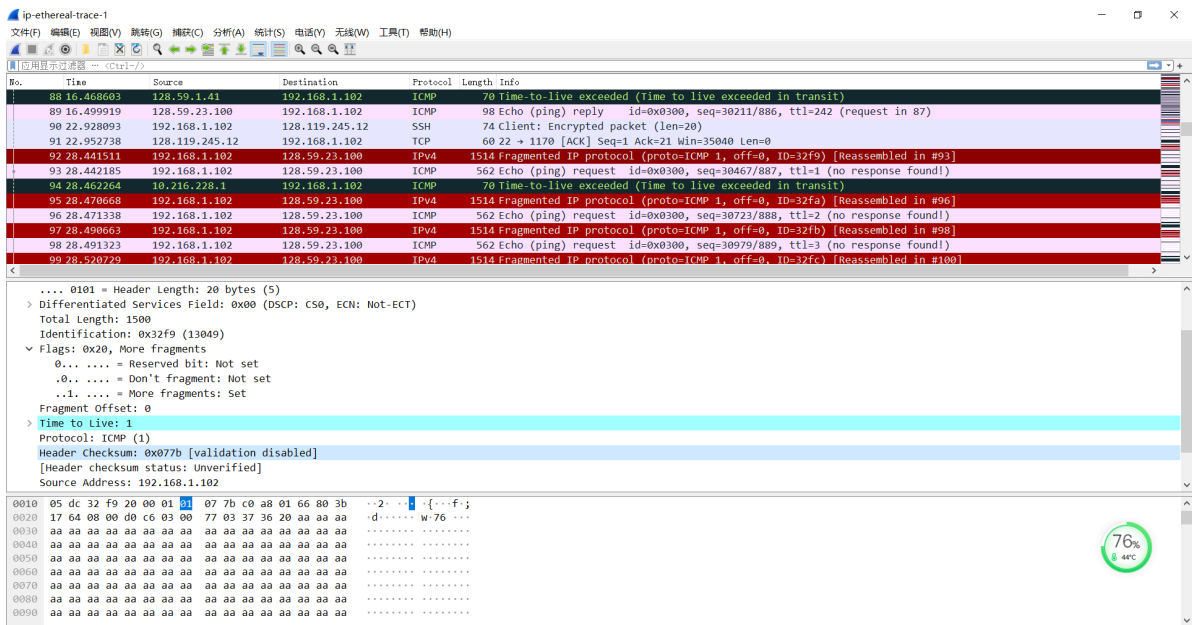
.0... .. = Don't fragment: Not set

..0. = More fragments: Not set

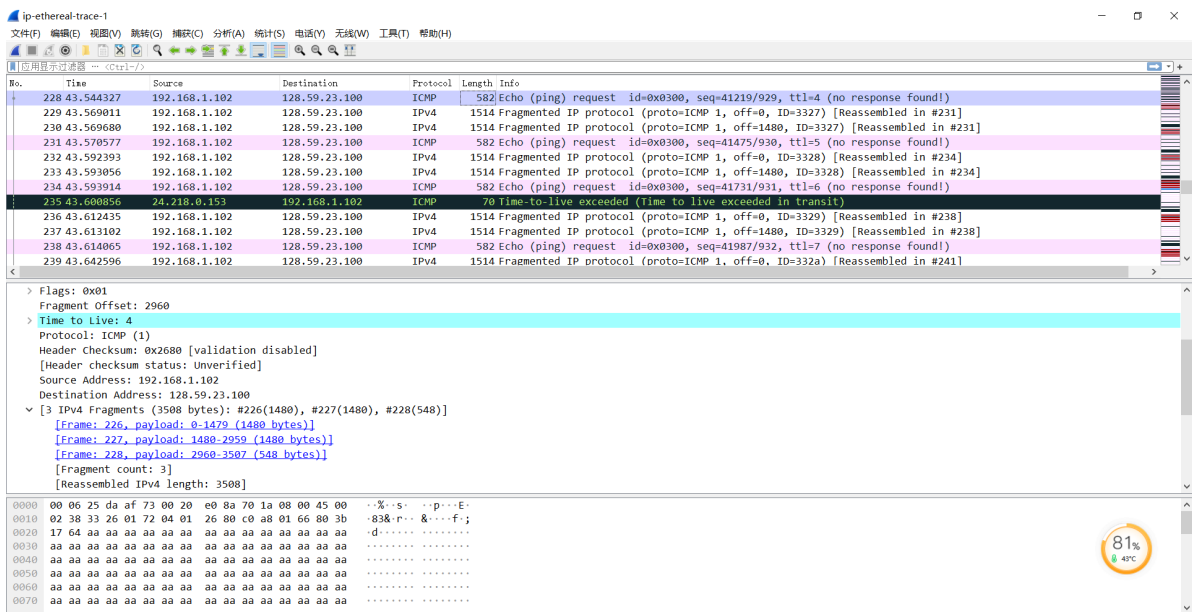
Fragment Offset: 1480

► Time to Live: 1

13.Total Length, More fragments, Fragment Offset, Header Checksum变了



14.创建了3个片段



15.Total Length, More fragments, Fragment Offset, Header Checksum变了

ip-ethereal-trace-1

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

应用显示过滤器: -- C:\n1- />

No.	Time	Source	Destination	Protocol	Length	Info
228	43.544327	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
229	43.569011	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3327) [Reassembled in #231]
230	43.569080	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3327) [Reassembled in #231]
231	43.570577	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41475/930, ttl=5 (no response found!)
232	43.592393	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3328) [Reassembled in #234]
233	43.593056	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3328) [Reassembled in #234]
234	43.593014	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41731/931, ttl=6 (no response found!)
235	43.600056	24.210.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (time to live exceeded in transit)
236	43.612435	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3329) [Reassembled in #238]
237	43.613102	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3329) [Reassembled in #238]
238	43.614065	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41987/932, ttl=7 (no response found!)
239	43.642596	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=332a) [Reassembled in #241]

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3327 (13095)
Flags: 0x20, More Fragments
0... = Reserved bit: Not set
0... = Don't fragment: Not set
..1. = More fragments: Set
Fragment Offset: 0
Time to Live: 5
Protocol: ICMP (1)
Header Checksum: 0x034d [validation disabled]
[Header checksum status: Unverified]

0010 05 dc 33 27 20 00 05 01 03 4d c0 a8 01 66 80 3b ..3'...M...f;
0020 17 64 08 00 a5 c3 03 00 a2 03 37 39 20 aa aa aa ..d.....79 ...
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0070 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0080 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0090 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

81%
± 4.8%

ip-ethereal-trace-1

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

应用显示过滤器: -- C:\n1- />

No.	Time	Source	Destination	Protocol	Length	Info
228	43.544327	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
229	43.569011	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3327) [Reassembled in #231]
230	43.569080	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3327) [Reassembled in #231]
231	43.570577	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41475/930, ttl=5 (no response found!)
232	43.592393	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3328) [Reassembled in #234]
233	43.593056	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3328) [Reassembled in #234]
234	43.593014	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41731/931, ttl=6 (no response found!)
235	43.600056	24.210.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (time to live exceeded in transit)
236	43.612435	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3329) [Reassembled in #238]
237	43.613102	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3329) [Reassembled in #238]
238	43.614065	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41987/932, ttl=7 (no response found!)
239	43.642596	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=332a) [Reassembled in #241]

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3327 (13095)
Flags: 0x20, More Fragments
0... = Reserved bit: Not set
0... = Don't fragment: Not set
..1. = More fragments: Set
Fragment Offset: 1480
Time to Live: 5
Protocol: ICMP (1)
Header Checksum: 0x0294 [validation disabled]
[Header checksum status: Unverified]

0010 05 dc 33 27 20 b9 05 01 02 94 c0 a8 01 66 80 3b ..3'...B...f;
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa ..d.....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0070 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0080 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0090 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

83%
± 4.8%

ip-ethereal-trace-1

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

应用显示过滤器: -- C:\n1- />

No.	Time	Source	Destination	Protocol	Length	Info
228	43.544327	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41219/929, ttl=4 (no response found!)
229	43.569011	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3327) [Reassembled in #231]
230	43.569080	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3327) [Reassembled in #231]
231	43.570577	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41475/930, ttl=5 (no response found!)
232	43.592393	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3328) [Reassembled in #234]
233	43.593056	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3328) [Reassembled in #234]
234	43.593014	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41731/931, ttl=6 (no response found!)
235	43.600056	24.210.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (time to live exceeded in transit)
236	43.612435	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3329) [Reassembled in #238]
237	43.613102	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3329) [Reassembled in #238]
238	43.614065	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=41987/932, ttl=7 (no response found!)
239	43.642596	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=332a) [Reassembled in #241]

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 568
Identification: 0x3327 (13095)
Flags: 0x01
0... = Reserved bit: Not set
0... = Don't fragment: Not set
0... = More fragments: Not set
Fragment Offset: 2960
Time to Live: 5
Protocol: ICMP (1)
Header Checksum: 0x257f [validation disabled]
[Header checksum status: Unverified]

0010 02 38 33 27 01 72 05 01 25 7f c0 a8 01 66 80 3b ..83'...B...f;
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa ..d.....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0070 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0080 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

83%
± 4.8%

