.misc

原创

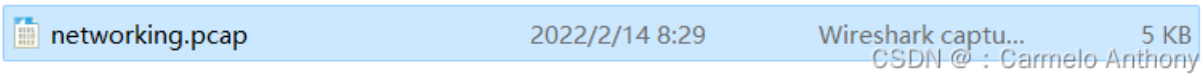
：Carmelo Anthony 于 2022-02-14 09:17:11 发布 2918 收藏 1
文章标签： 网络 网络协议 安全 wireshark

telnet

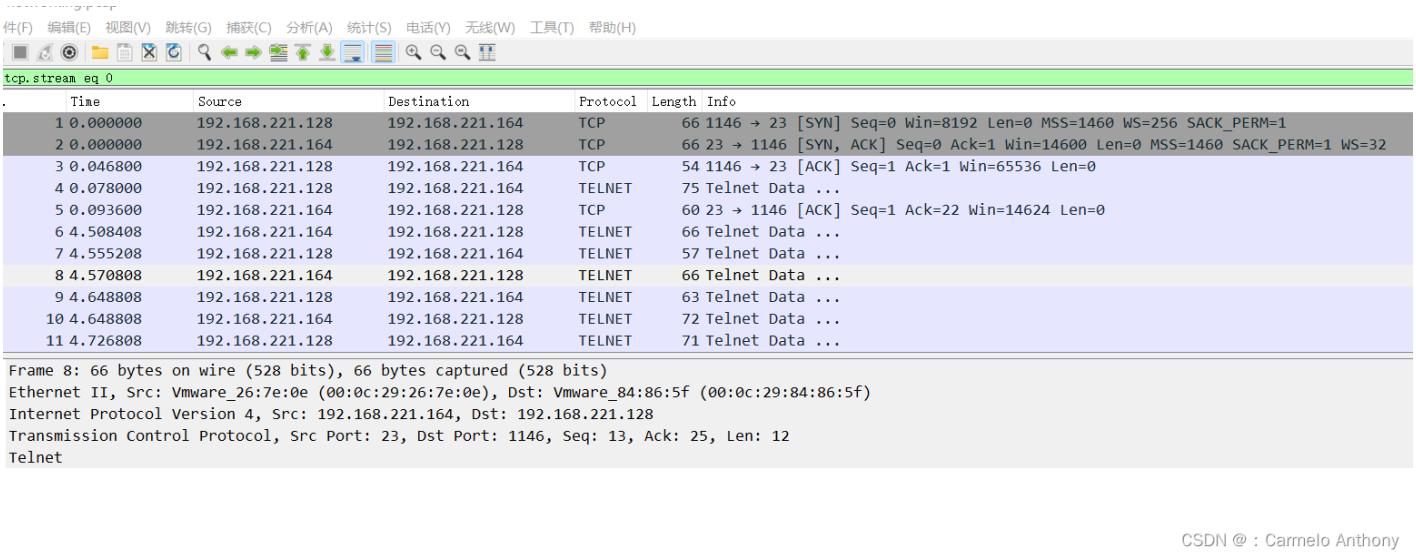
A

下载文件 解压压缩包 可以看到 是一个pcap结尾的文件

pcap文件为wireshark配置脚本文件 所以选择wireshark打开



得到数据流

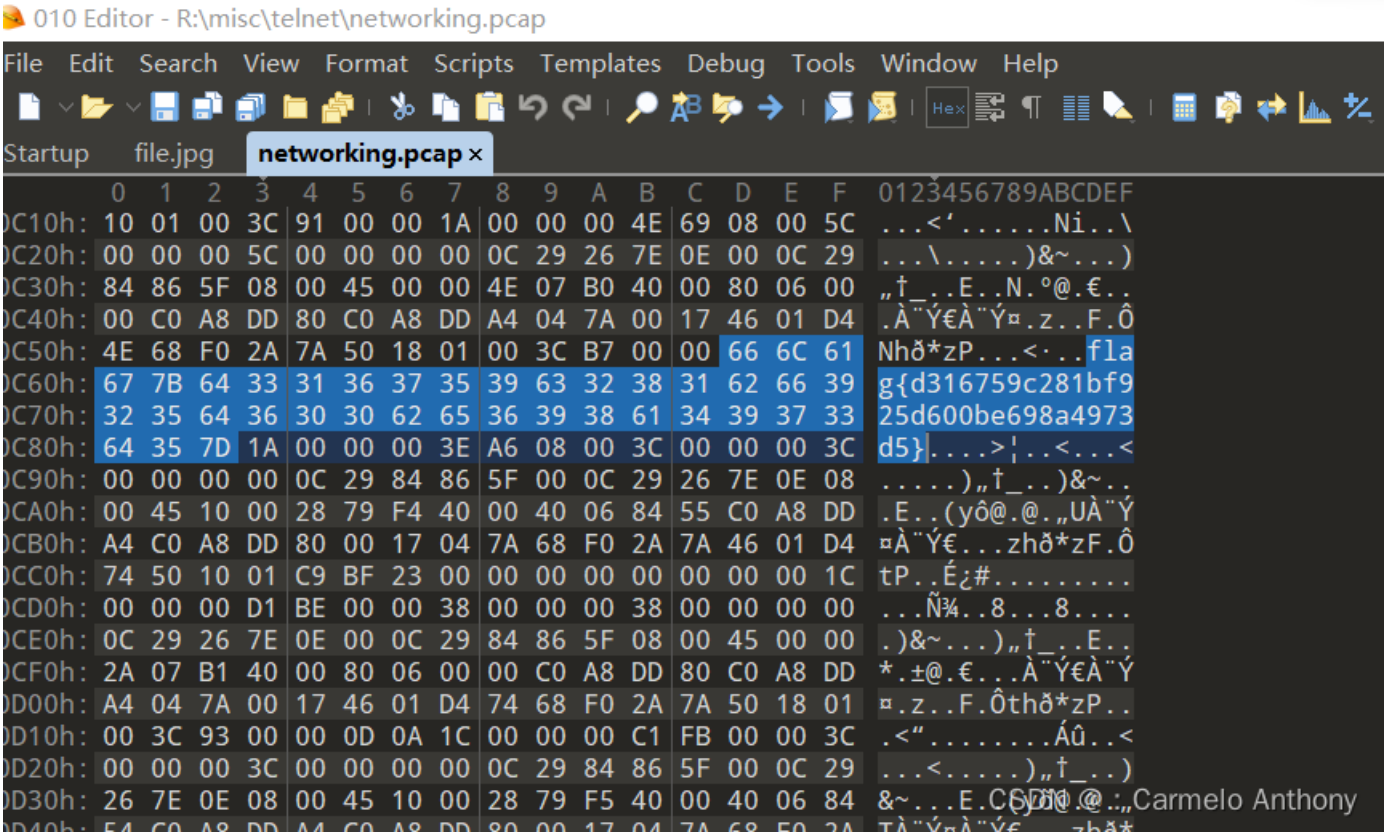


可以观察 没什么异样 然后我们选择一个telnet协议 追踪下tcp信息流

这里存在 flag

B

直接用010editor打开文件



也可以发掘flag

ping

下载文件 解压后发现 也是一个pcap文件

所以 尝试使用wireshark打开

捕获追踪流 但是 行不通

ping.pcap

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

应用显示过滤器 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2	1.083222	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3	2.164155	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4	3.243027	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5	4.328050	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6	5.438891	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7	6.532304	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
8	7.617469	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response found!)
9	8.698257	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response found!)
10	9.788550	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response found!)
11	10.879034	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response found!)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x178c [correct]
    [Checksum Status: Good]
    Identifier (BE): 31337 (0x7a69)
    Identifier (LE): 27002 (0x697a)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
  v Data (1400 bytes)
      Data: 660a0000000000000000000000000000000000000000000…

0020  50 01 08 00 17 8c 7a 69  00 00 66 0a 00 00 00 00   P·····zi ··f·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```


应用显示过滤器 … <Ctrl-/>

o.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2	1.083222	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3	2.164155	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4	3.243027	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5	4.328050	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6	5.438891	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7	6.532304	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
8	7.617469	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response found!)
9	8.698257	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response found!)
10	9.788550	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response found!)
11	10.879034	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response found!)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0e8c [correct]
    [Checksum Status: Good]
    Identifier (BE): 32105 (0x7d69)
    Identifier (LE): 27005 (0x697d)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
  v Data (1400 bytes)
      Data: 6c0a0000000000000000000000000000000000000000000…

0020  50 01 08 00 0e 8c 7d 69  00 00 6c 0a 00 00 00 00   P·····}i ··l·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

ping.pcap

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

应用显示过滤器 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2	1.083222	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3	2.164155	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4	3.243027	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5	4.328050	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6	5.438891	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7	6.532304	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
8	7.617469	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response found!)
9	8.698257	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response found!)
10	9.788550	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response found!)
11	10.879034	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response found!)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x168c [correct]
    [Checksum Status: Good]
    Identifier (BE): 32873 (0x8069)
    Identifier (LE): 27008 (0x6980)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
  v Data (1400 bytes)
      Data: 610a0000000000000000000000000000000000000000000000…

0020  50 01 08 00 16 8c 80 69  00 00 61 0a 00 00 00 00   P·····i ··a·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```


ping.pcap

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

应用显示过滤器 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2	1.083222	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3	2.164155	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4	3.243027	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5	4.328050	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6	5.438891	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7	6.532304	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
8	7.617469	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response found!)
9	8.698257	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response found!)
10	9.788550	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response found!)
11	10.879034	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response found!)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0d8c [correct]
    [Checksum Status: Good]
    Identifier (BE): 33641 (0x8369)
    Identifier (LE): 27011 (0x6983)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
  v Data (1400 bytes)
      Data: 670a0000000000000000000000000000000000000000000000…

0020  50 01 08 00 0d 8c 83 69  00 00 67 0a 00 00 00 00   P·····i ··g·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```


依次点击 查看数据包 有趣的事情发生了 下面的ascii码逐一变化 f l a g 组合起来就是我们要寻找的 flag

应用显示过滤器 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2	1.083222	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3	2.164155	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4	3.243027	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5	4.328050	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6	5.438891	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7	6.532304	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
8	7.617469	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response found!)
9	8.698257	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response found!)
10	9.788550	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response found!)
11	10.879034	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response found!)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf68b [correct]
    [Checksum Status: Good]
    Identifier (BE): 34409 (0x8669)
    Identifier (LE): 27014 (0x6986)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
  v Data (1400 bytes)
      Data: 7b0a0000000000000000000000000000000000000000…

0020  50 01 08 00 f6 8b 86 69  00 00 7b 0a 00 00 00 00   P·····i ··{·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```


ping.pcap

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

应用显示过滤器 … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response fou
2	1.083222	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response fou
3	2.164155	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response fou
4	3.243027	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response fou
5	4.328050	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response fou
6	5.438891	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response fou
7	6.532304	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response fou
8	7.617469	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9069, seq=0/0, ttl=64 (no response fou
9	8.698257	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9369, seq=0/0, ttl=64 (no response fou
10	9.788550	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9669, seq=0/0, ttl=64 (no response fou
11	10.879034	192.168.80.129	192.168.80.1	ICMP	1442	Echo (ping) request id=0x9969, seq=0/0, ttl=64 (no response fou

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0a8c [correct]
    [Checksum Status: Good]
    Identifier (BE): 35177 (0x8969)
    Identifier (LE): 27017 (0x6989)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
  > [No response seen]
  v Data (1400 bytes)
      Data: 640a0000000000000000000000000000000000000000…

0020  50 01 08 00 0a 8c 89 69  00 00 64 0a 00 00 00 00   P·····i ··d·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```


探索下去 凑齐flag

flag{dc76a1eee6e3822877ed627e0a04ab4a}

小结：

A wireshark的pcap文件