# PCAP File Repairing

EN | ZH

## PCAP 文件结构

一般来说, 对于 `PCAP` 文件格式考察较少，且通常都能借助于现成的工具如 `pcapfix` 直接修复，这里大致介绍下几个常见的块，详细可以翻看 Here。

- Tools
  - PcapFix Online
  - PcapFix

一般文件结构

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Block Type                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Block Total Length                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                          Block Body                           /
/          /* variable length, aligned to 32 bits */            /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Block Total Length                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

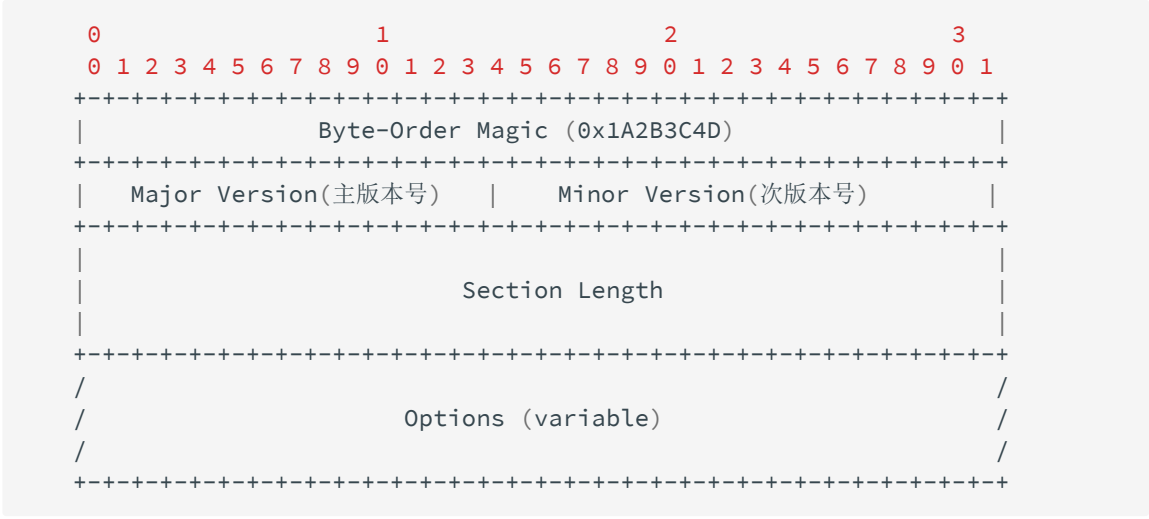
目前所定义的常见块类型有

1. Section Header Block: it defines the most important characteristics of the capture file.
2. Interface Description Block: it defines the most important characteristics of the interface(s) used for capturing traffic.
3. Packet Block: it contains a single captured packet, or a portion of it.
4. Simple Packet Block: it contains a single captured packet, or a portion of it, with only a minimal set of information about it.
5. Name Resolution Block: it defines the mapping from numeric addresses present in the packet dump and the canonical name counterpart.
6. Capture Statistics Block: it defines how to store some statistical data (e.g. packet dropped, etc) which can be useful to undestand the conditions in which the capture has been made.

# 常见块

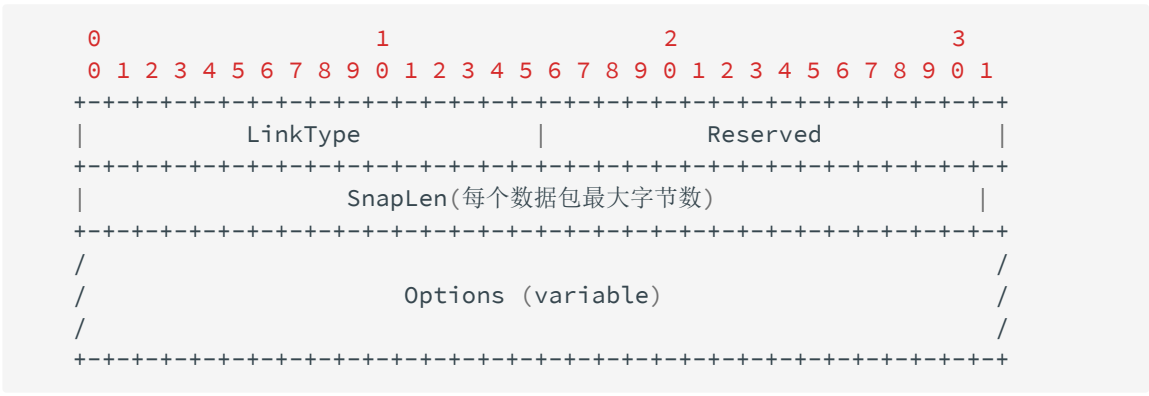
## Section Header BlocK(文件头)

必须存在, 意味着文件的开始

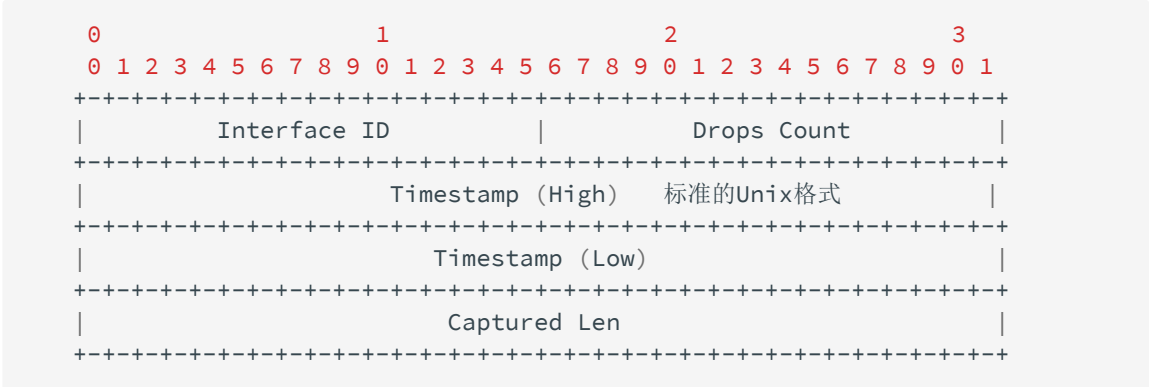



## Interface Description Block(接口描述)

必须存在, 描述接口特性




## Packet Block(数据块)



```
    |                          Packet Len                           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    /                          Packet Data                          /
    /          /* variable length, aligned to 32 bits */           /
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    /                       Options (variable)                      /
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

## 例题

> 题目：第一届 “百度杯” 信息安全攻防总决赛 线上选拔赛：find the flag
>
> WP：https://www.cnblogs.com/ECJTUACM-873284962/p/9884447.html

首先我们拿到这样一道流量包的题目，题目名称为 `find the flag` 。这里面给了很多提示信息，要我们去找到 `flag` 。

**第一步，搜索 `flag` 字样**

我们先去搜索看看流量包里面有没有 `flag` 。我们使用 `strings` 命令去找一下流量包，`Windows` 的朋友可以用 `notepad++` 的搜索功能去寻找。

搜索命令如下：

```
strings findtheflag.cap | grep flag
```

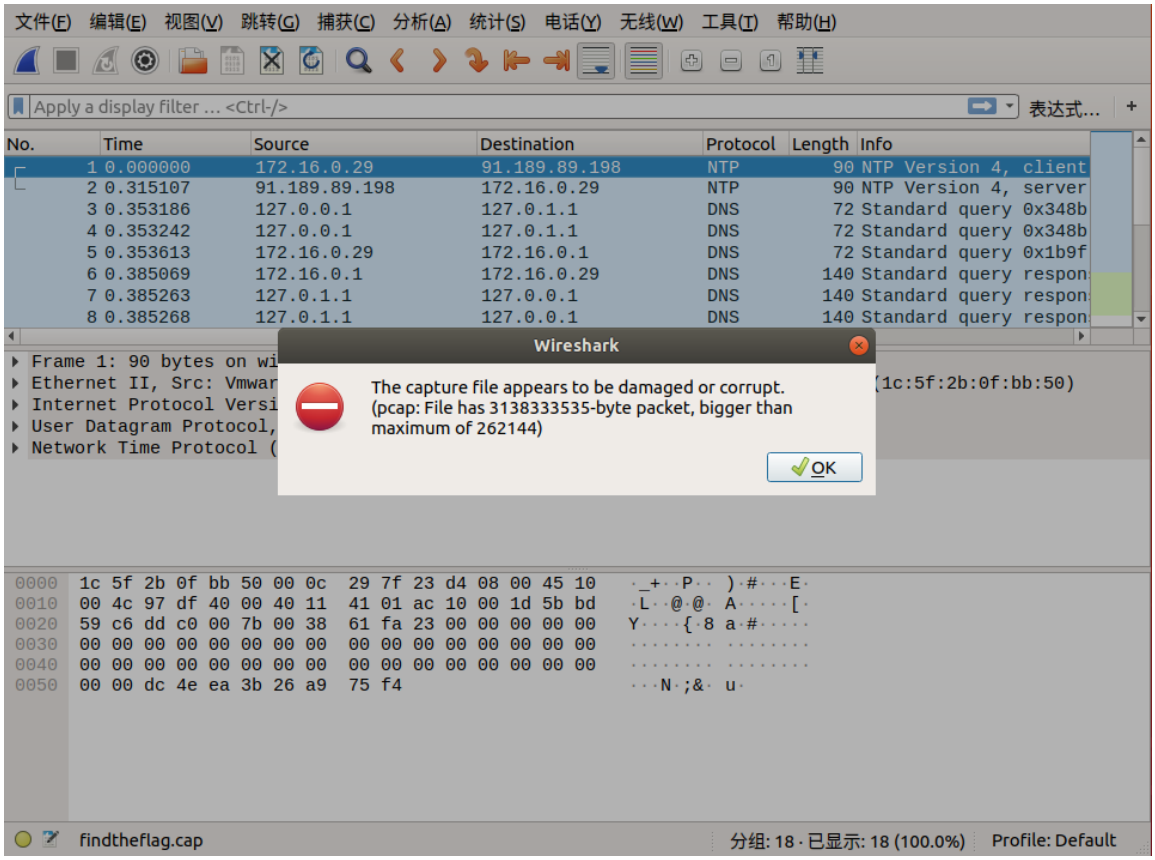
搜索结果如下：

```
#( 10/29/18@ 7:12下午 )( python@Sakura ):~/桌面
   strings findtheflag.cap | grep flag
_#\GET /AS/Suggestions?pt=page.home&mkt=zh-cn&qry=where%20is%20my%20flag&cp=16&c
vid=D479002D4AB1402EB764D8AD1A031F72 HTTP/1.1
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
where is the flag?
```

我们发现搜出了一大堆的东西，我们通过管道去过滤出 `flag` 信息，似乎没有发现我们所需要找的答案。

**第二步，流量包修复**

我们用 `wireshark` 打开这个流量包

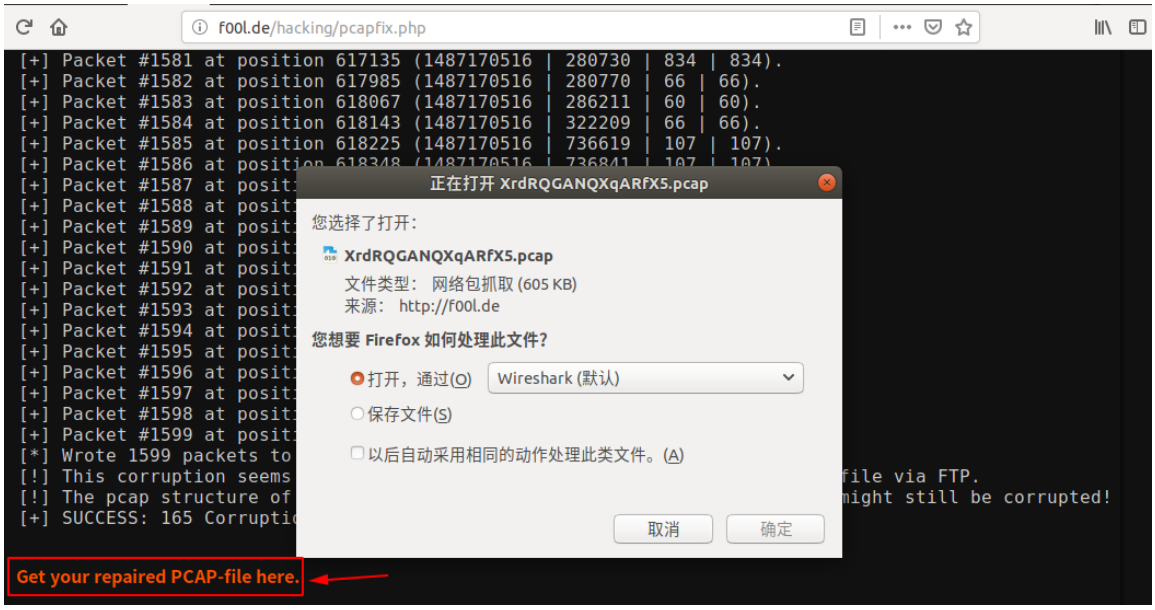



我们发现这个流量包出现了异常现象，我们可以修复一下这个流量包。

这里我们用到一个在线工具：http://f00l.de/hacking/pcapfix.php

这个工具可以帮助我们快速地将其流量包修复为 `pcap` 包。

我们对其进行在线修复。

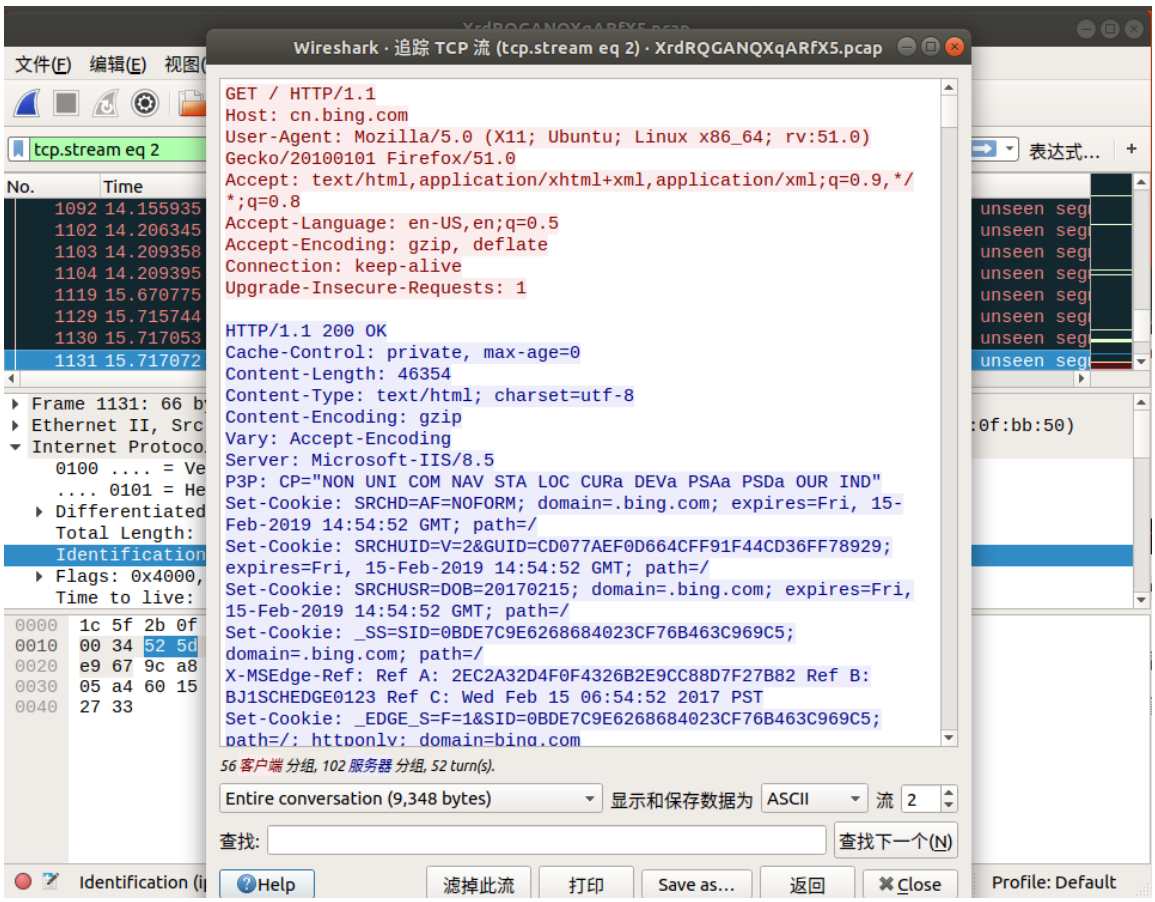



修复完毕后点击 `Get your repaired PCAP-file here.` 即可下载流量包，然后我们用 `wireshark` 打开。

既然还是要找 `flag` ，我们可以先看看这个流量包。

**第三步，追踪 TCP 流**

我们追踪一下 TCP 流，看看有没有什么突破？



我们通过追踪 `TCP` 流，可以看到一些版本信息， `cookie` 等等，我们还是发现了一些很有意思的东西。

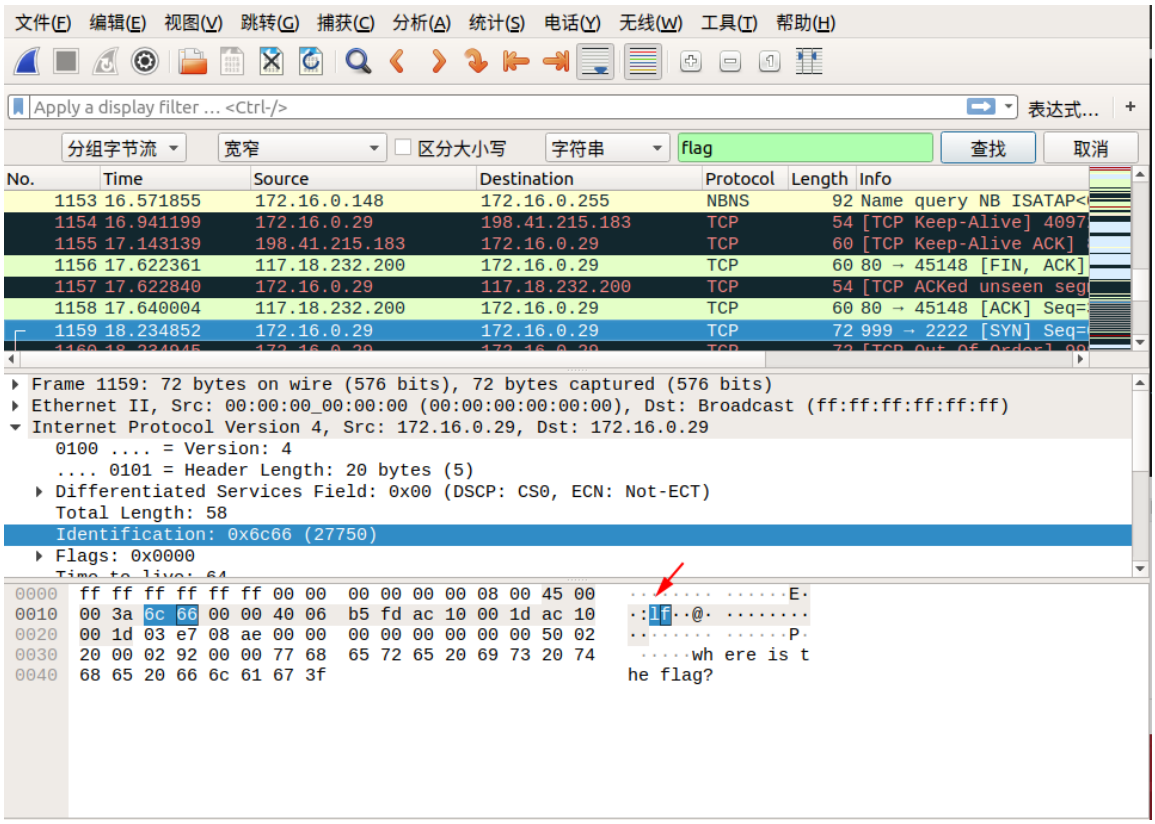
从 `tcp.stream eq 29` 到 `tcp.stream eq 41` 只显示了 `where is the flag?` 这个字样，难道这是出题人在告诉我们 `flag` 在这里嘛?

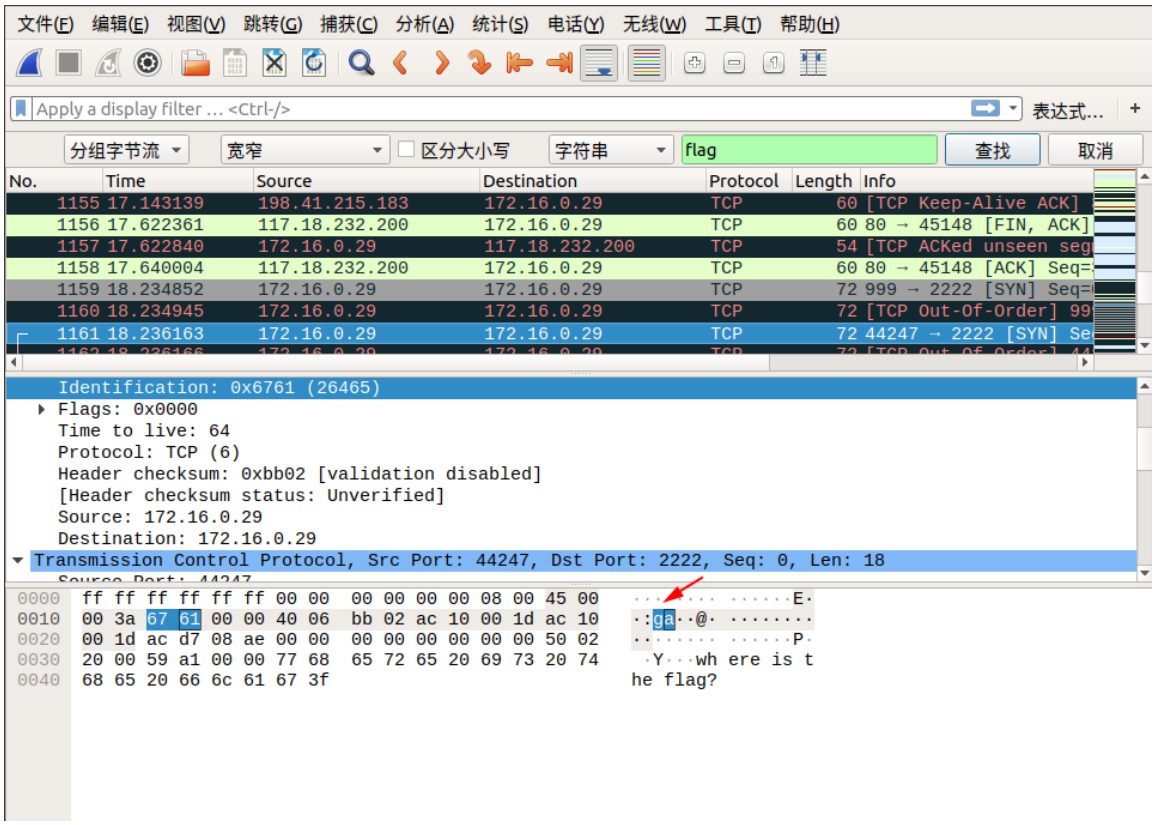
**第四步，查找分组字节流**

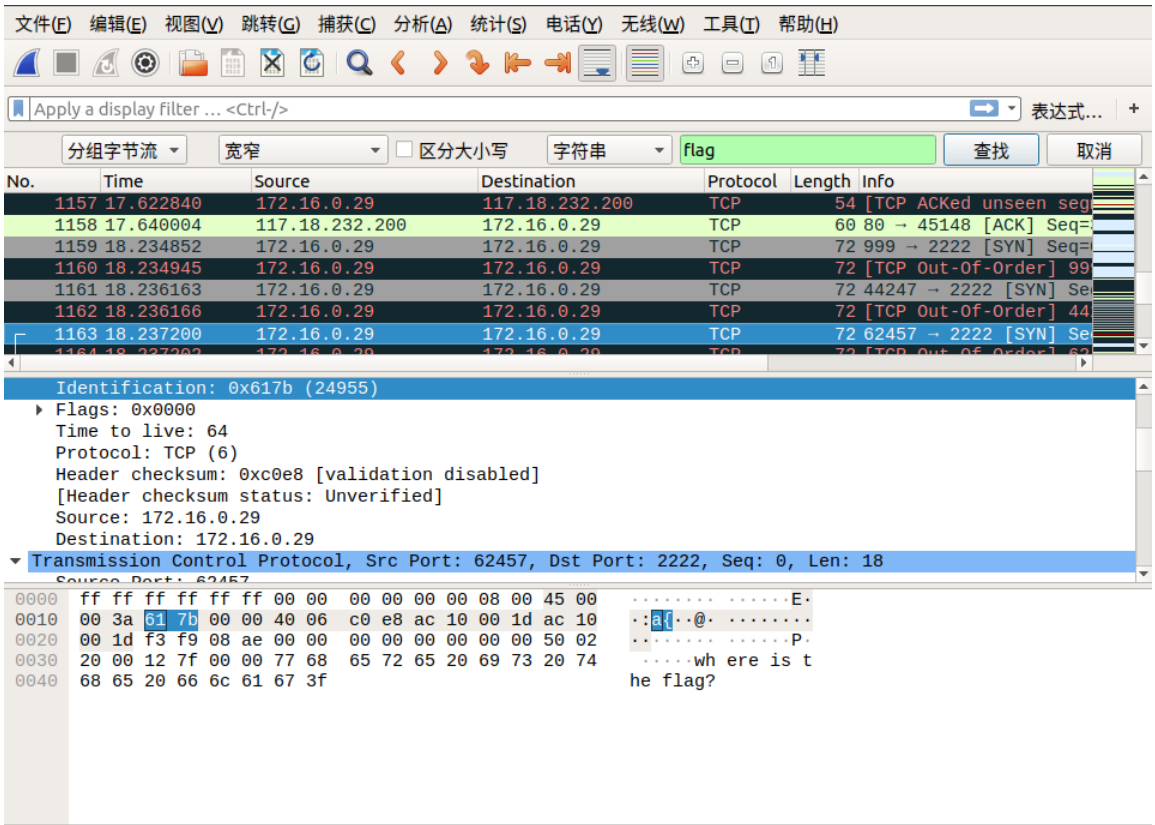
我们追踪到 `tcp.stream eq 29` 的时候，在 `Identification` 信息中看到了 `flag` 中的 `lf` 字样，我们可以继续追踪下一个流，在 `tcp.stream eq 30` 的 `Identification` 信息中看到了 `flag` 中的 `ga` 字样，我们发现将两个包中 `Identification` 信息对应的字段从右至左组合，恰好就是 `flag` ！于是我们可以大胆地猜测， `flag` 肯定是藏在这里面。

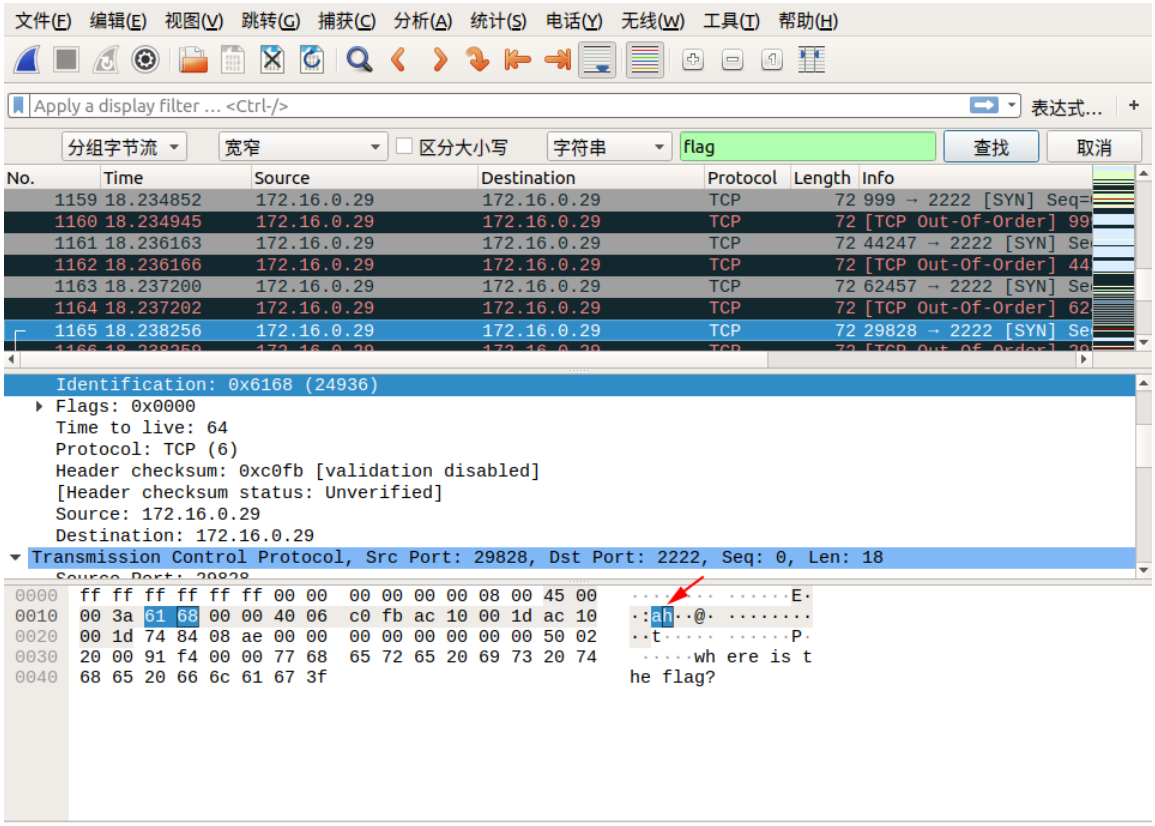
我们直接通过搜索 -> 字符串搜索 -> 分组字节流 -> 搜索关键字 `flag` 即可，按照同样的方式连接后面相连数据包的 `Identification` 信息对应的字段，即可找到最终的 flag!

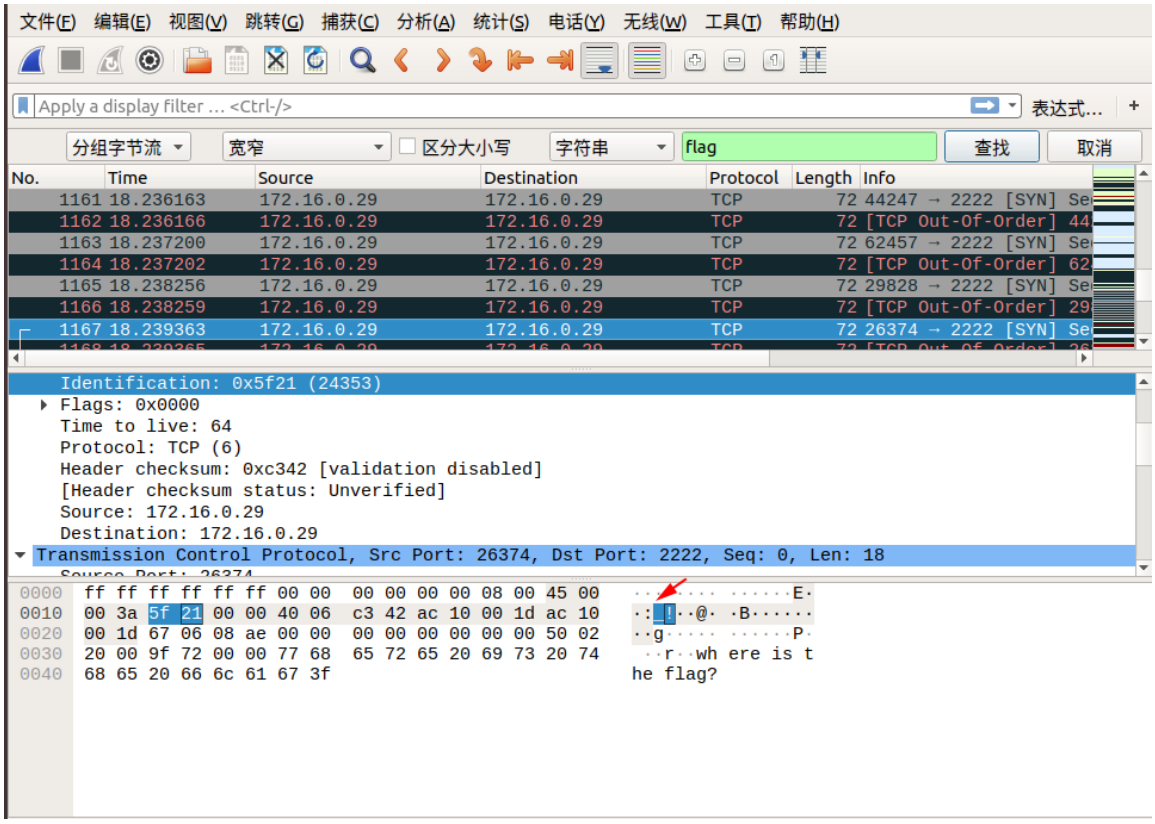
下面是搜索的截图：

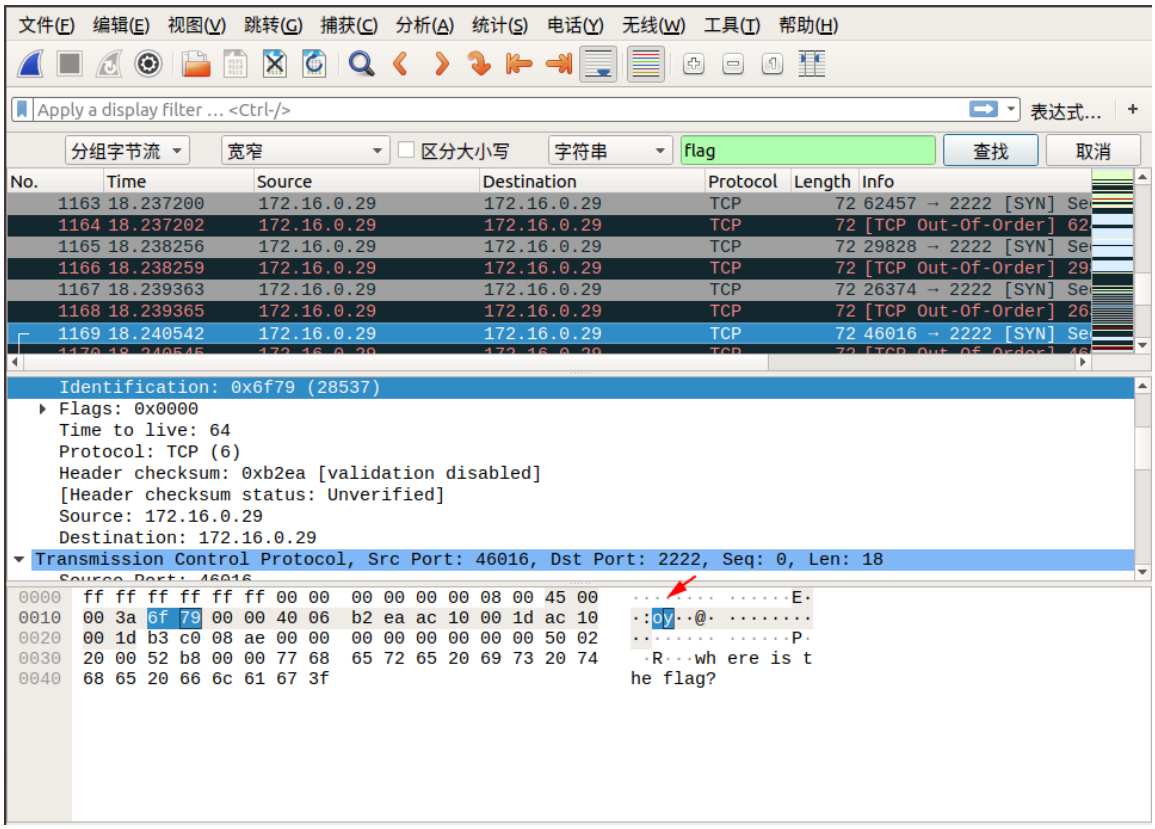


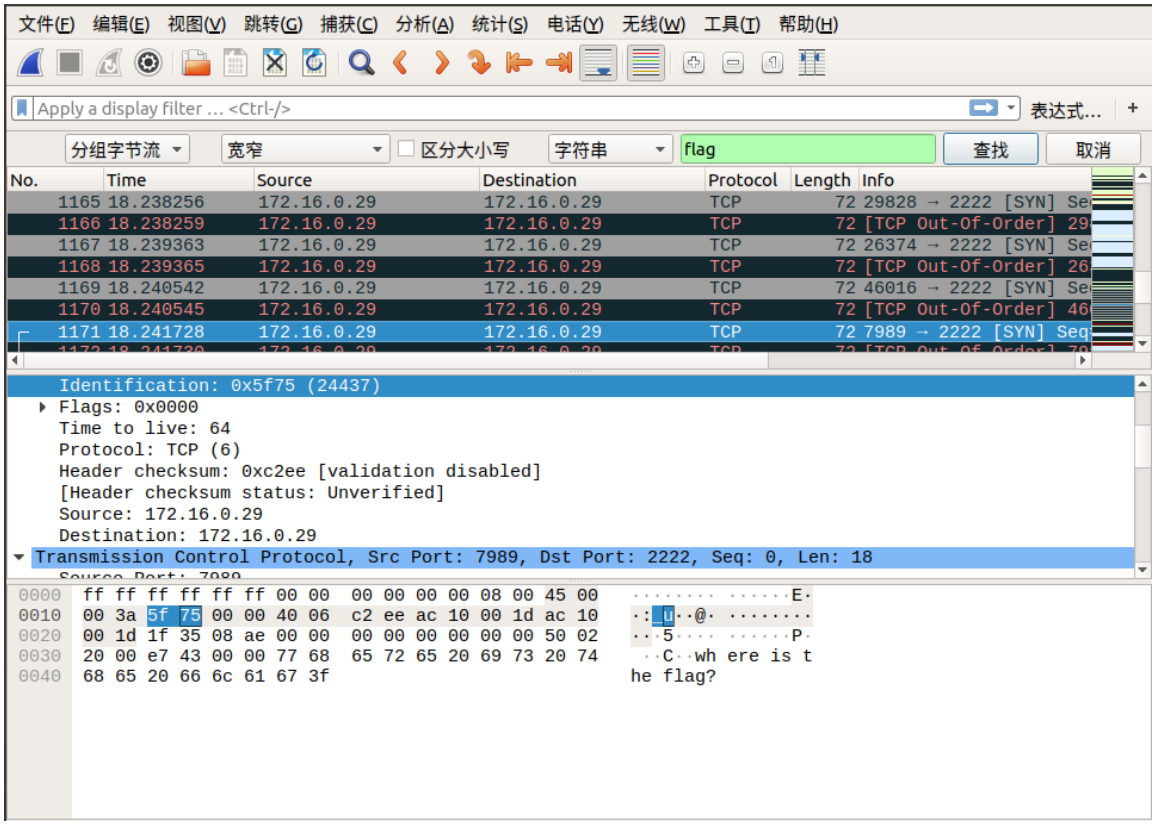

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1155 17.143139 198.41.215.183 172.16.0.29 TCP 60 [TCP Keep-Alive ACK]
1156 17.622361 117.18.232.200 172.16.0.29 TCP 60 80 → 45148 [FIN, ACK]
1157 17.622840 172.16.0.29 117.18.232.200 TCP 54 [TCP ACKed unseen seg
1158 17.640004 117.18.232.200 172.16.0.29 TCP 60 80 → 45148 [ACK] Seq=
1159 18.234852 172.16.0.29 172.16.0.29 TCP 72 999 → 2222 [SYN] Seq=
1160 18.234945 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 99
1161 18.236163 172.16.0.29 172.16.0.29 TCP 72 44247 → 2222 [SYN] Se
Identification: 0x6761 (26465)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xbb02 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 44247, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00 ..... .....E.
0010 00 3a 67 61 00 00 40 06 bb 02 ac 10 00 1d ac 10 .:ga..@. ........
0020 00 1d ac d7 08 ae 00 00 00 00 00 00 00 00 50 02 ..... .....P.
0030 20 00 59 a1 00 00 77 68 65 72 65 20 69 73 20 74 .Y...wh ere is t
0040 68 65 20 66 6c 61 67 3f he flag?

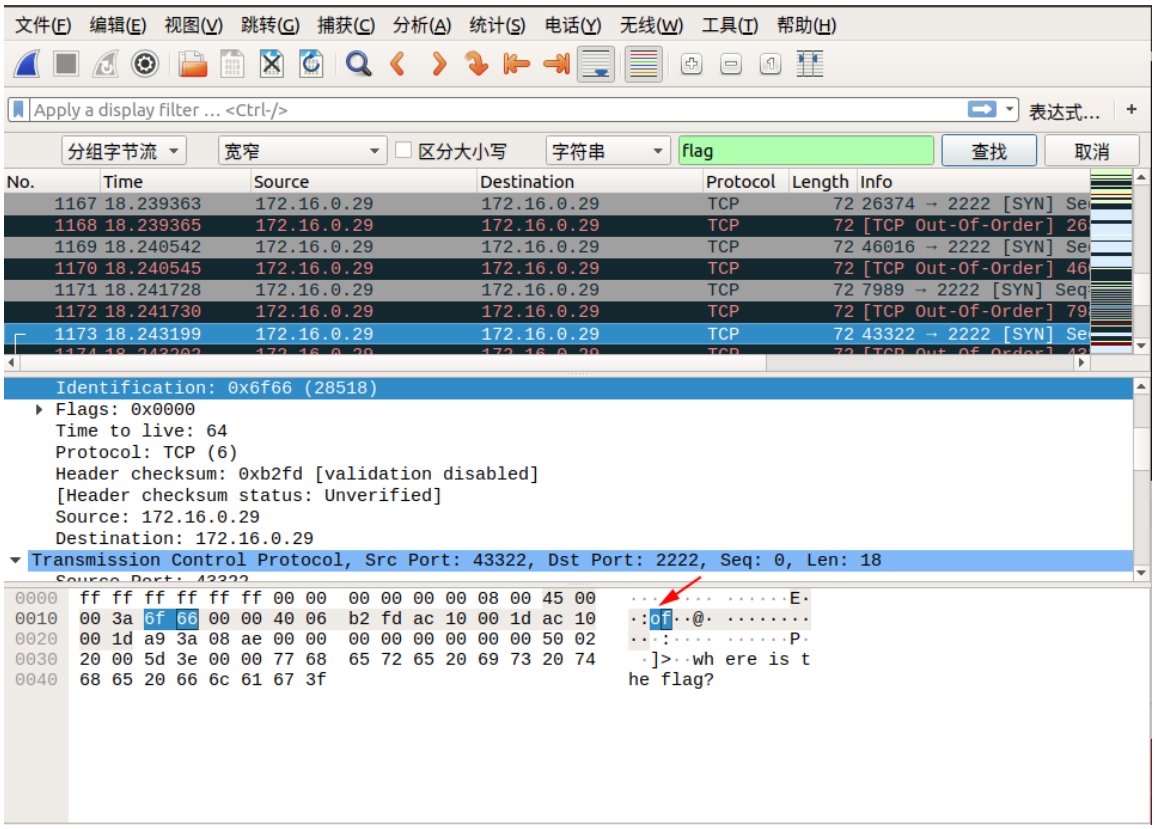

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1157 17.622840 172.16.0.29 117.18.232.200 TCP 54 [TCP ACKed unseen seg
1158 17.640004 117.18.232.200 172.16.0.29 TCP 60 80 → 45148 [ACK] Seq=
1159 18.234852 172.16.0.29 172.16.0.29 TCP 72 999 → 2222 [SYN] Seq=
1160 18.234945 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 99
1161 18.236163 172.16.0.29 172.16.0.29 TCP 72 44247 → 2222 [SYN] Se
1162 18.236166 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 44
1163 18.237200 172.16.0.29 172.16.0.29 TCP 72 62457 → 2222 [SYN] Se
Identification: 0x617b (24955)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xc0e8 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 62457, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00 ..... .....E.
0010 00 3a 61 7b 00 00 40 06 c0 e8 ac 10 00 1d ac 10 .:a{..@. ........
0020 00 1d f3 f9 08 ae 00 00 00 00 00 00 00 00 50 02 ..... .....P.
0030 20 00 12 7f 00 00 77 68 65 72 65 20 69 73 20 74 .....wh ere is t
0040 68 65 20 66 6c 61 67 3f he flag?

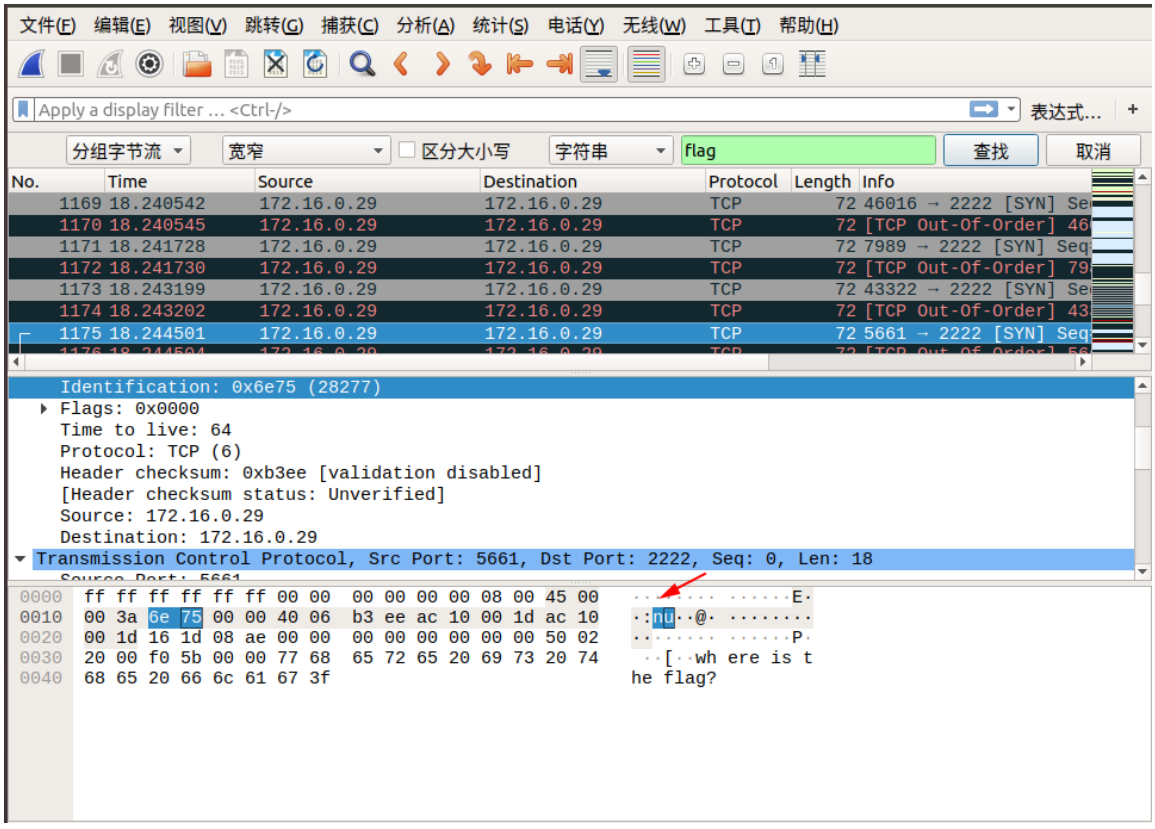

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1159 18.234852 172.16.0.29 172.16.0.29 TCP 72 999 → 2222 [SYN] Seq=
1160 18.234945 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 99
1161 18.236163 172.16.0.29 172.16.0.29 TCP 72 44247 → 2222 [SYN] Se
1162 18.236166 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 44
1163 18.237200 172.16.0.29 172.16.0.29 TCP 72 62457 → 2222 [SYN] Se
1164 18.237202 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 62
1165 18.238256 172.16.0.29 172.16.0.29 TCP 72 29828 → 2222 [SYN] Se
Identification: 0x6168 (24936)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xc0fb [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 29828, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 61 68 00 00 40 06 c0 fb ac 10 00 1d ac 10
0020 00 1d 74 84 08 ae 00 00 00 00 00 00 00 00 50 02
0030 20 00 91 f4 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
wh ere is t
he flag?

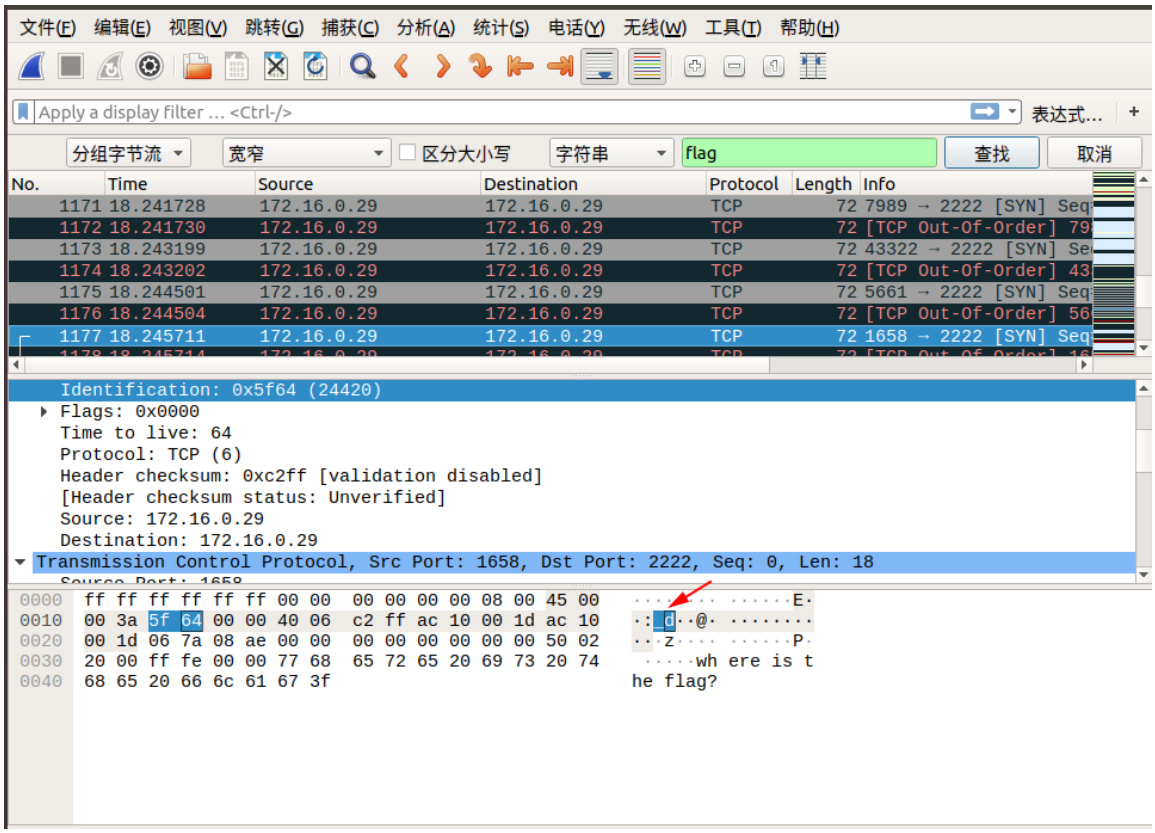

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1161 18.236163 172.16.0.29 172.16.0.29 TCP 72 44247 → 2222 [SYN] Se
1162 18.236166 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 44
1163 18.237200 172.16.0.29 172.16.0.29 TCP 72 62457 → 2222 [SYN] Se
1164 18.237202 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 62
1165 18.238256 172.16.0.29 172.16.0.29 TCP 72 29828 → 2222 [SYN] Se
1166 18.238259 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 29
1167 18.239363 172.16.0.29 172.16.0.29 TCP 72 26374 → 2222 [SYN] Se
Identification: 0x5f21 (24353)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xc342 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 26374, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 5f 21 00 00 40 06 c3 42 ac 10 00 1d ac 10
0020 00 1d 67 06 08 ae 00 00 00 00 00 00 00 00 50 02
0030 20 00 9f 72 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
wh ere is t
he flag?

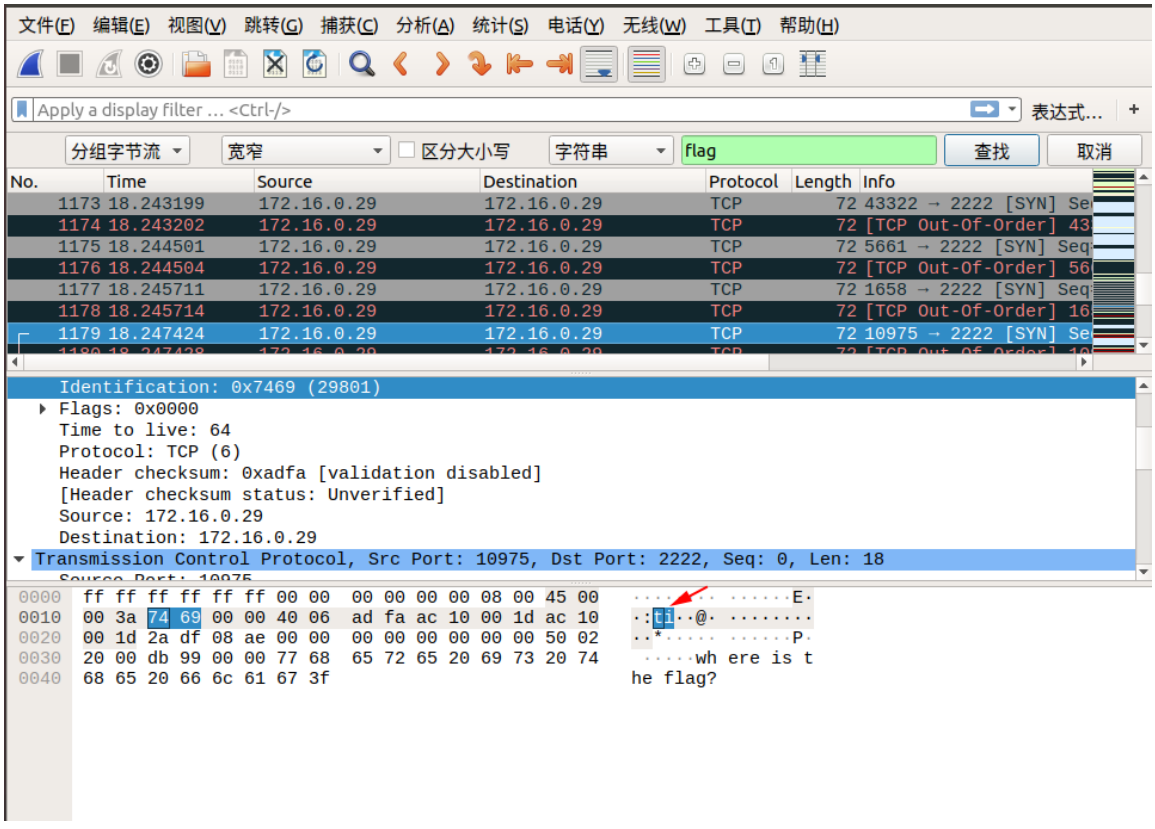

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1163 18.237200 172.16.0.29 172.16.0.29 TCP 72 62457 → 2222 [SYN] Se
1164 18.237202 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 62
1165 18.238256 172.16.0.29 172.16.0.29 TCP 72 29828 → 2222 [SYN] Se
1166 18.238259 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 29
1167 18.239363 172.16.0.29 172.16.0.29 TCP 72 26374 → 2222 [SYN] Se
1168 18.239365 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 26
1169 18.240542 172.16.0.29 172.16.0.29 TCP 72 46016 → 2222 [SYN] Se
Identification: 0x6f79 (28537)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xb2ea [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 46016, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 6f 79 00 00 40 06 b2 ea ac 10 00 1d ac 10
0020 00 1d b3 c0 08 ae 00 00 00 00 00 00 50 02
0030 20 00 52 b8 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
he flag?

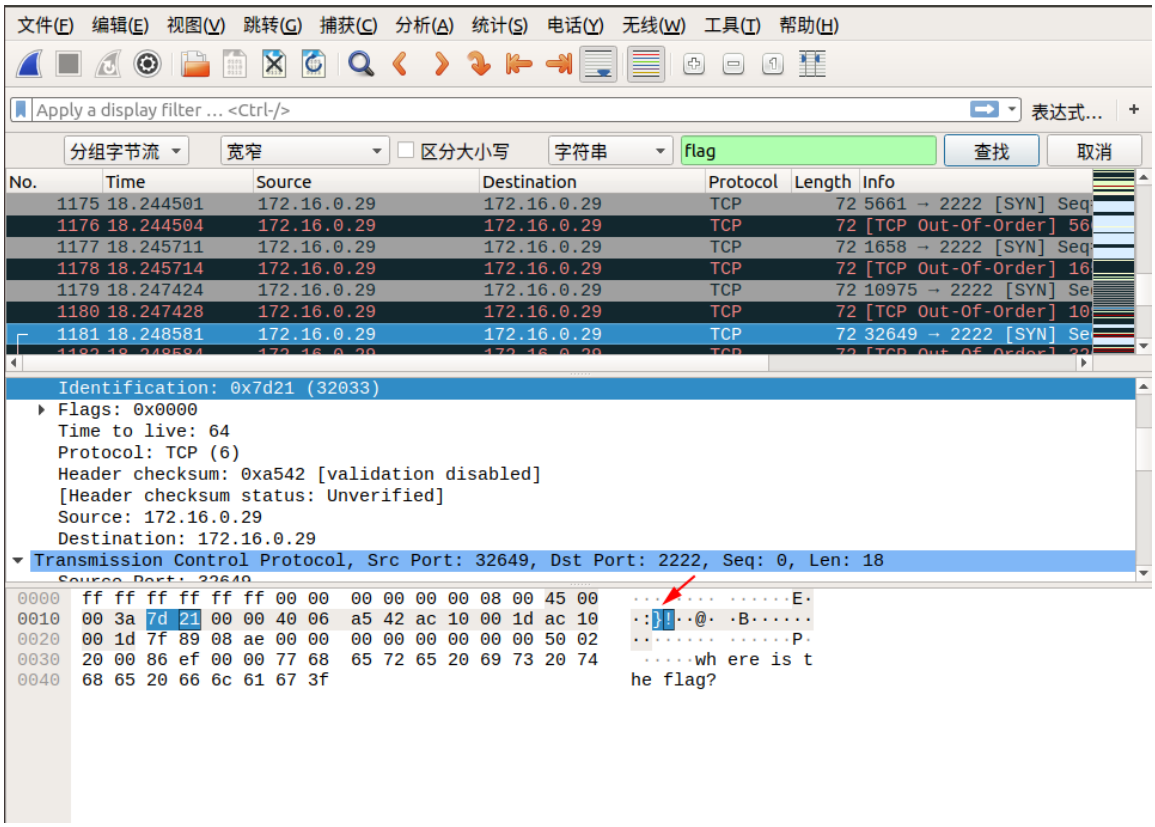

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1165 18.238256 172.16.0.29 172.16.0.29 TCP 72 29828 → 2222 [SYN] Se
1166 18.238259 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 29
1167 18.239363 172.16.0.29 172.16.0.29 TCP 72 26374 → 2222 [SYN] Se
1168 18.239365 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 26
1169 18.240542 172.16.0.29 172.16.0.29 TCP 72 46016 → 2222 [SYN] Se
1170 18.240545 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 46
1171 18.241728 172.16.0.29 172.16.0.29 TCP 72 7989 → 2222 [SYN] Seq
Identification: 0x5f75 (24437)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xc2ee [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 7989, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 5f 75 00 00 40 06 c2 ee ac 10 00 1d ac 10
0020 00 1d 1f 35 08 ae 00 00 00 00 00 00 50 02
0030 20 00 e7 43 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
he flag?


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)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1167 18.239363 172.16.0.29 172.16.0.29 TCP 72 26374 → 2222 [SYN] Se
1168 18.239365 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 26
1169 18.240542 172.16.0.29 172.16.0.29 TCP 72 46016 → 2222 [SYN] Se
1170 18.240545 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 46
1171 18.241728 172.16.0.29 172.16.0.29 TCP 72 7989 → 2222 [SYN] Seq
1172 18.241730 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 79
1173 18.243199 172.16.0.29 172.16.0.29 TCP 72 43322 → 2222 [SYN] Se
Identification: 0x6f66 (28518)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xb2fd [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 43322, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 6f 66 00 00 40 06 b2 fd ac 10 00 1d ac 10
0020 00 1d a9 3a 08 ae 00 00 00 00 00 00 00 00 50 02
0030 20 00 5d 3e 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
wh ere is t
he flag?


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)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1169 18.240542 172.16.0.29 172.16.0.29 TCP 72 46016 → 2222 [SYN] Se
1170 18.240545 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 46
1171 18.241728 172.16.0.29 172.16.0.29 TCP 72 7989 → 2222 [SYN] Seq
1172 18.241730 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 79
1173 18.243199 172.16.0.29 172.16.0.29 TCP 72 43322 → 2222 [SYN] Se
1174 18.243202 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 43
1175 18.244501 172.16.0.29 172.16.0.29 TCP 72 5661 → 2222 [SYN] Seq
Identification: 0x6e75 (28277)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xb3ee [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 5661, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 6e 75 00 00 40 06 b3 ee ac 10 00 1d ac 10
0020 00 1d 16 1d 08 ae 00 00 00 00 00 00 00 00 50 02
0030 20 00 f0 5b 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
wh ere is t
he flag?


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)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1171 18.241728 172.16.0.29 172.16.0.29 TCP 72 7989 → 2222 [SYN] Seq
1172 18.241730 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 79
1173 18.243199 172.16.0.29 172.16.0.29 TCP 72 43322 → 2222 [SYN] Se
1174 18.243202 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 43
1175 18.244501 172.16.0.29 172.16.0.29 TCP 72 5661 → 2222 [SYN] Seq
1176 18.244504 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 56
1177 18.245711 172.16.0.29 172.16.0.29 TCP 72 1658 → 2222 [SYN] Seq
Identification: 0x5f64 (24420)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xc2ff [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 1658, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 5f 64 00 00 40 06 c2 ff ac 10 00 1d ac 10
0020 00 1d 06 7a 08 ae 00 00 00 00 00 00 00 50 02
0030 20 00 ff fe 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
he flag?


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)
Apply a display filter ... <Ctrl-/>
表达式...
分组字节流
宽窄
区分大小写
字符串
flag
查找
取消
No. Time Source Destination Protocol Length Info
1173 18.243199 172.16.0.29 172.16.0.29 TCP 72 43322 → 2222 [SYN] Se
1174 18.243202 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 43
1175 18.244501 172.16.0.29 172.16.0.29 TCP 72 5661 → 2222 [SYN] Seq
1176 18.244504 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 56
1177 18.245711 172.16.0.29 172.16.0.29 TCP 72 1658 → 2222 [SYN] Seq
1178 18.245714 172.16.0.29 172.16.0.29 TCP 72 [TCP Out-Of-Order] 16
1179 18.247424 172.16.0.29 172.16.0.29 TCP 72 10975 → 2222 [SYN] Se
Identification: 0x7469 (29801)
Flags: 0x0000
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xadfa [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.29
Destination: 172.16.0.29
Transmission Control Protocol, Src Port: 10975, Dst Port: 2222, Seq: 0, Len: 18
0000 ff ff ff ff ff ff 00 00 00 00 00 00 08 00 45 00
0010 00 3a 74 69 00 00 40 06 ad fa ac 10 00 1d ac 10
0020 00 1d 2a df 08 ae 00 00 00 00 00 00 00 50 02
0030 20 00 db 99 00 00 77 68 65 72 65 20 69 73 20 74
0040 68 65 20 66 6c 61 67 3f
he flag?




所以最终的 `flag` 为：**flag{aha!_you_found_it!}**

## 参考文献


- http://www.tcpdump.org/pcap/pcap.html
- https://zhuanlan.zhihu.com/p/27470338
- https://www.cnblogs.com/ECJTUACM-873284962/p/9884447.html


## 评论