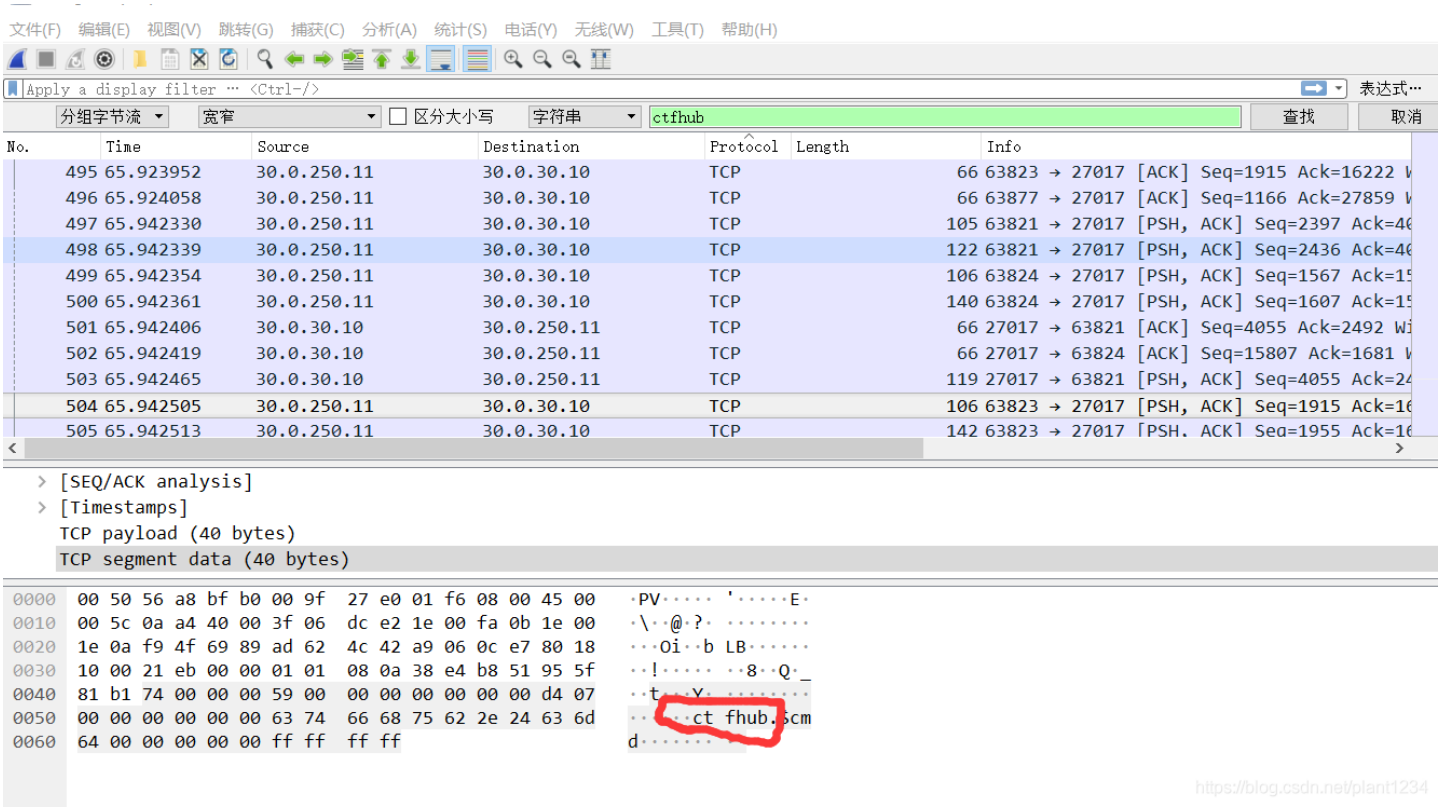
ctfhub MongoDB流量

原创

『铁躯电芯』 于 2021-06-06 14:23:13 发布 205 收藏

MongoDB流量：

知识点:wireshark过滤搜索功能
这题我们打开题目得到流量包，查找ctfhub得到很多有关的流量包
且不是要的答案：



于是我们增加精确用ctfhub{ 得到flag：

Wireshark · 分组 483 · mongodb.pcap

```
    [Calculated window size: 131072]
    [Window size scaling factor: 32]
    Checksum: 0x2958 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (160 bytes)
    TCP segment data (160 bytes)
```

```
0030  10 00 29 58 00 00 01 01  08 0a 38 e4 b8 33 95 5f   ··)X···· ··8··3·_
0040  57 1c a0 00 00 00 02 69  6e 73 65 72 74 00 05 00   W·····i nsert···
0050  00 00 66 6c 61 67 00 04  64 6f 63 75 6d 65 6e 74   ··flag·· document
0060  73 00 51 00 00 00 03 30  00 49 00 00 00 07 5f 69   s·Q····0 ·I····_i
0070  64 00 5e b3 c2 c4 9d af  59 23 62 e9 06 30 02 66   d·^·····  Y#b··0·f
0080  6c 61 67 00 29 00 00 00  63 74 66 68 75 62 7b 35   lag·)··· ctfhub{5
0090  66 32 38 34 65 63 63 32  37 39 64 32 63 62 64 31   f284ecc2 79d2cbd1
00a0  61 66 32 35 38 62 62 35  33 63 37 61 35 66 36 7d   af258bb5 3c7a5f6}
00b0  00 00 00 08 6f 72 64 65  72 65 64 00 01 03 6c 73   ····orde red···ls
00c0  69 64 00 1e 00 00 00 05  69 64 00 10 00 00 00 04   id····· id·····
00d0  08 0f a0 8f 6f fd 44 70  b6 40 39 1d 69 10 96 37   ····o·Dp ·@9·i··7
00e0  00 00                                             ··
```