xctf攻防世界 CRYPTO高手进阶区 工业协议分析2

原创

l8947943 于 2022-02-10 19:51:49 发布 10778 收藏 1

分类专栏： 攻防世界crypto之路 文章标签： 安全 crypto

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/l8947943/article/details/122868060

版权

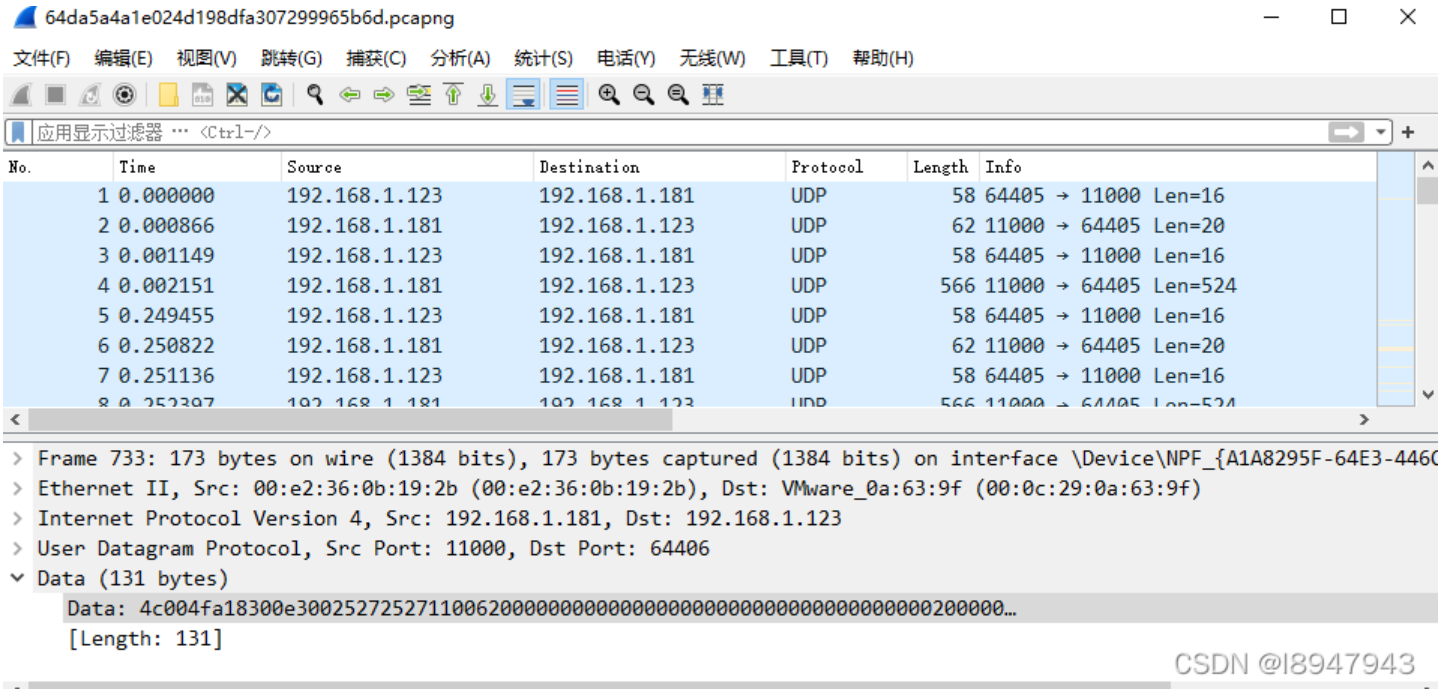
攻防世界crypto之路 专栏收录该内容

26 篇文章 0 订阅

订阅专栏

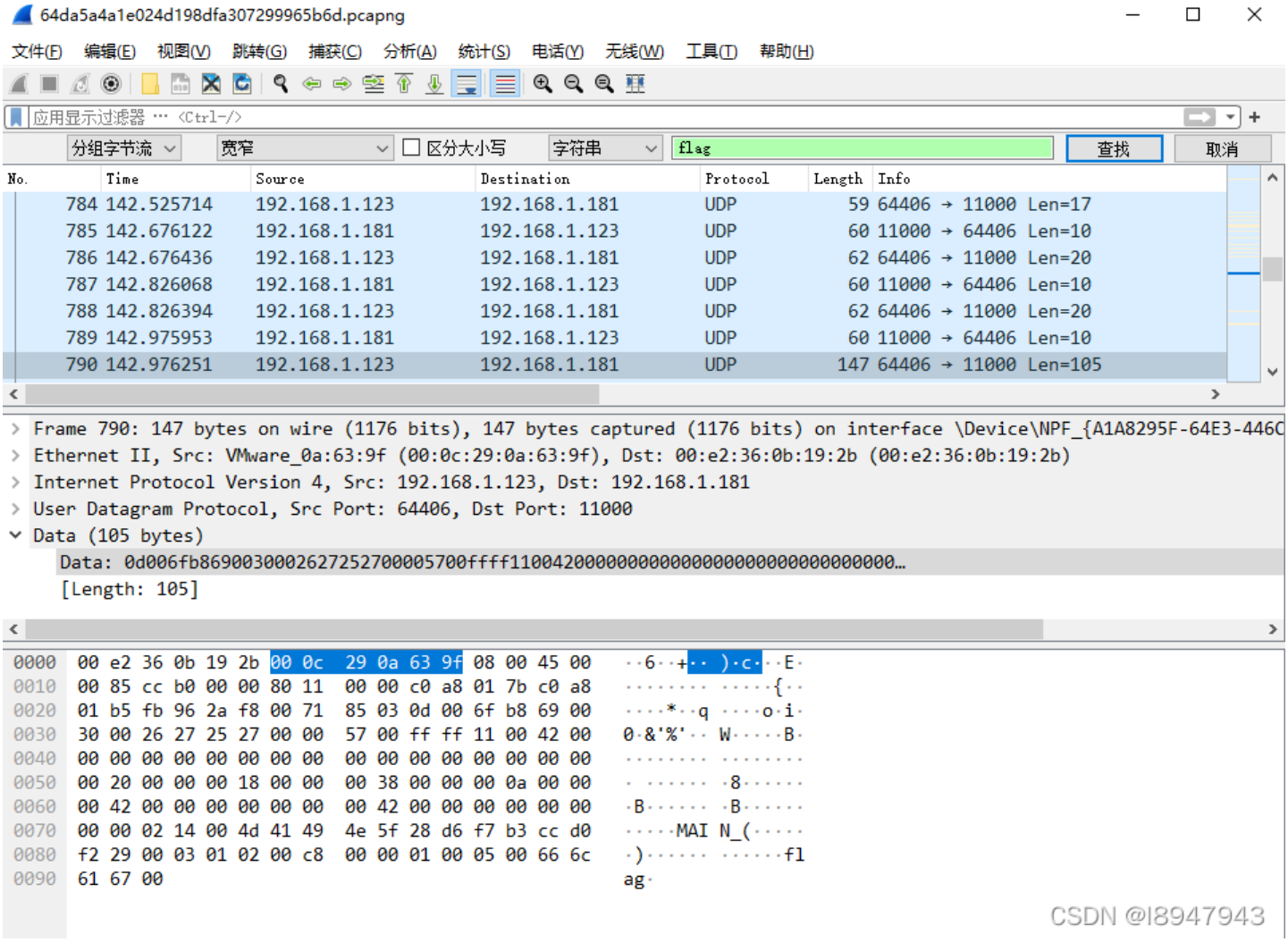
1. 进入环境，下载附件

题目给的是一个pacpng的流量包文件，我们使用wireshark打开：



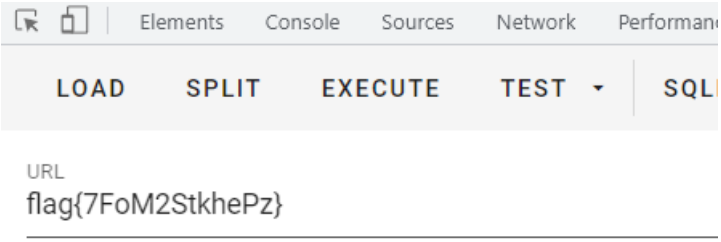
2. 问题分析

题目提示 flag形式为 flag{}，那么我们在流量包的分组字节流中搜索flag，还真有，如图：



右键追踪流，并在追踪流中找到具体的flag位置：

发现flag的同时还有奇怪的字符666c61677b37466f4d3253746b6865507a7d，尝试16进制解码：

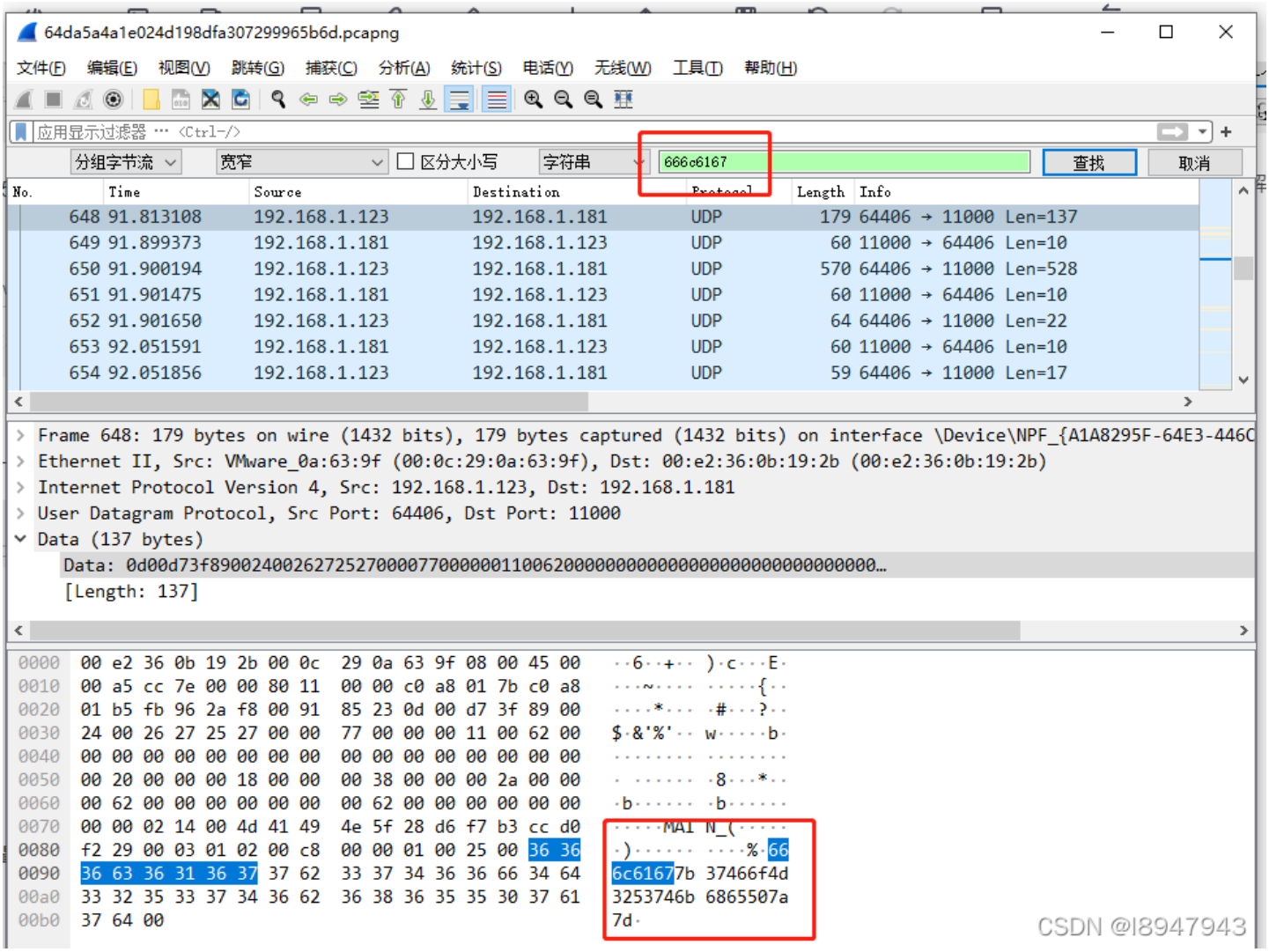


最终答案为：`flag{7FoM2StkhePz}`

3. 逆向思路

flag的16进制编码为`666c6167`

因此在分组字节流中搜索666c6167，定位到搜寻字符，也可以得到最终答案，如图：


64da5a4a1e024d198dfa307299965b6d.pcapng
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-/>
分组字节流 宽窄 区分大小写 字符串 666c6167 查找 取消
No. Time Source Destination Protocol Length Info
648 91.813108 192.168.1.123 192.168.1.181 UDP 179 64406 → 11000 Len=137
649 91.899373 192.168.1.181 192.168.1.123 UDP 60 11000 → 64406 Len=10
650 91.900194 192.168.1.123 192.168.1.181 UDP 570 64406 → 11000 Len=528
651 91.901475 192.168.1.181 192.168.1.123 UDP 60 11000 → 64406 Len=10
652 91.901650 192.168.1.123 192.168.1.181 UDP 64 64406 → 11000 Len=22
653 92.051591 192.168.1.181 192.168.1.123 UDP 60 11000 → 64406 Len=10
654 92.051856 192.168.1.123 192.168.1.181 UDP 59 64406 → 11000 Len=17
Frame 648: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{A1A8295F-64E3-446C
Ethernet II, Src: VMware_0a:63:9f (00:0c:29:0a:63:9f), Dst: 00:e2:36:0b:19:2b (00:e2:36:0b:19:2b)
Internet Protocol Version 4, Src: 192.168.1.123, Dst: 192.168.1.181
User Datagram Protocol, Src Port: 64406, Dst Port: 11000
Data (137 bytes)
Data: 0d00d73f890024002627252700007700000011006200000000000000000000000000000000…
[Length: 137]
0000 00 e2 36 0b 19 2b 00 0c 29 0a 63 9f 08 00 45 00
0010 00 a5 cc 7e 00 00 80 11 00 00 c0 a8 01 7b c0 a8
0020 01 b5 fb 96 2a f8 00 91 85 23 0d 00 d7 3f 89 00
0030 24 00 26 27 25 27 00 00 77 00 00 00 11 00 62 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 20 00 00 00 18 00 00 00 38 00 00 00 2a 00 00
0060 00 62 00 00 00 00 00 00 00 62 00 00 00 00 00 00
0070 00 00 02 14 00 4d 41 49 4e 5f 28 d6 f7 b3 cc d0
0080 f2 29 00 03 01 02 00 c8 00 00 01 00 25 00 36 36
0090 36 63 36 31 36 37 37 62 33 37 34 36 36 66 34 64
00a0 33 32 35 33 37 34 36 62 36 38 36 35 35 30 37 61
00b0 37 64 00
6c61677b 37466f4d
3253746b 6865507a
7d
CSDN @l8947943