攻防世界crypto高手题的工业协议分析2

原创

沐一 · 林 于 2021-09-08 21:58:07 发布 75 收藏 1

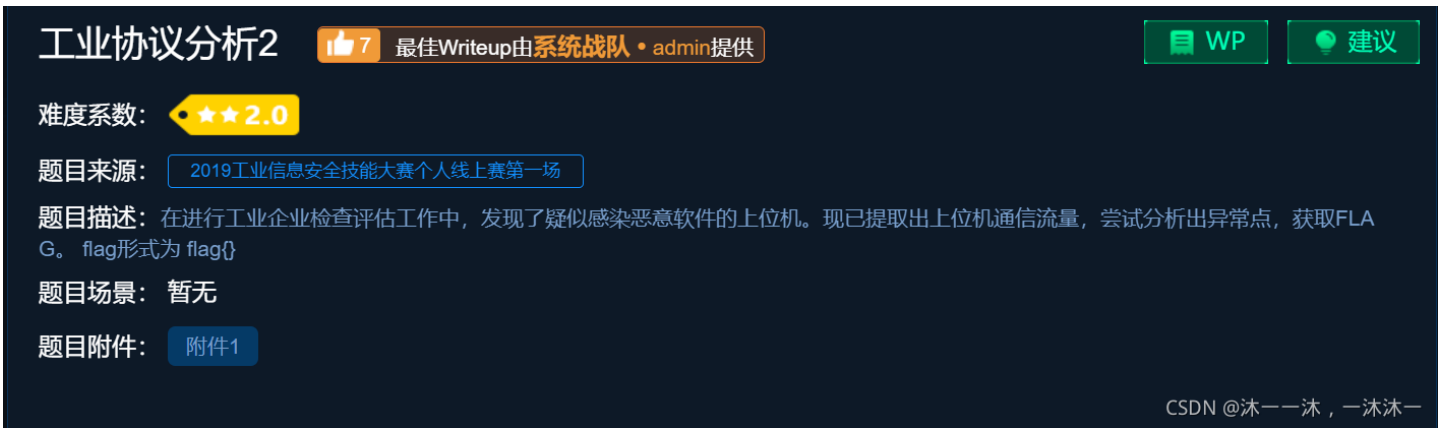
分类专栏： CTF 密码学 文章标签： ctf

本文链接：https://blog.csdn.net/xiao__1bai/article/details/120189759

攻防世界crypto高手题之工业协议分析2

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的工业协议分析2



下载附件，是一个pcapng流量文件：

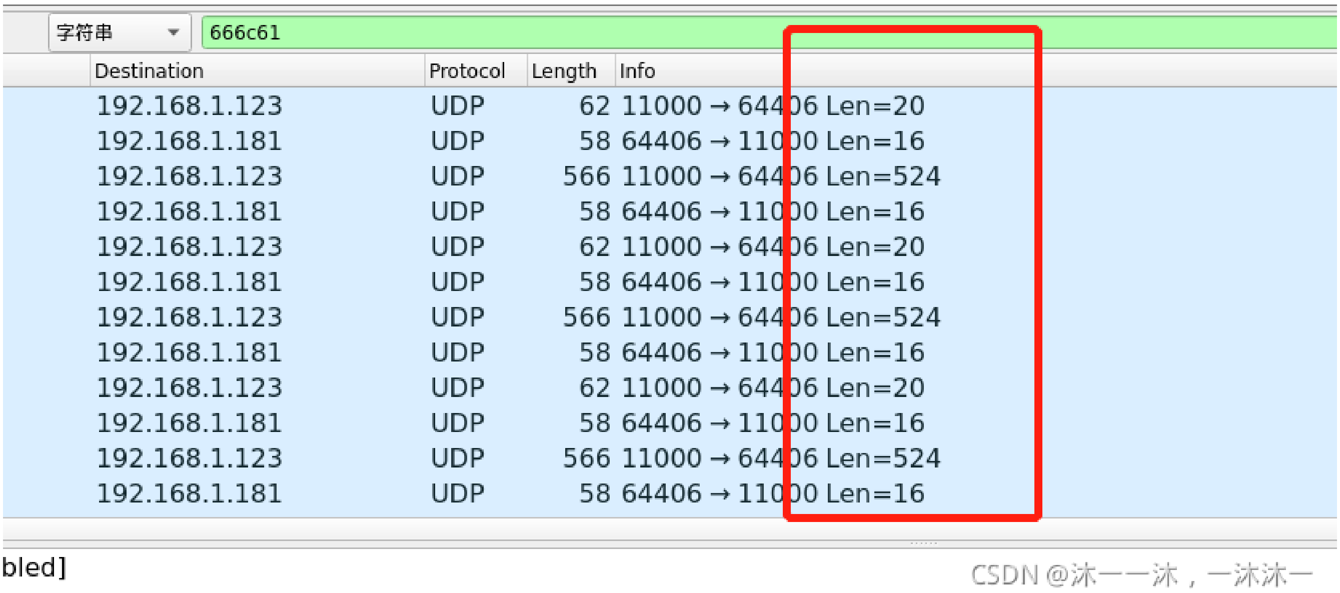
.

.

(这里积累第一个经验)

题目描述说已提取出上位机通信流量，尝试分析出异常点，获取FLAG。 flag形式为 flag{}，这其实就是一个暗示，flag就在通信流量中，至于哪里异常，查了资料，有的说UDP的长度有部分异常，要一个个点击查看。可是为什么我感觉UDP大的一堆，小

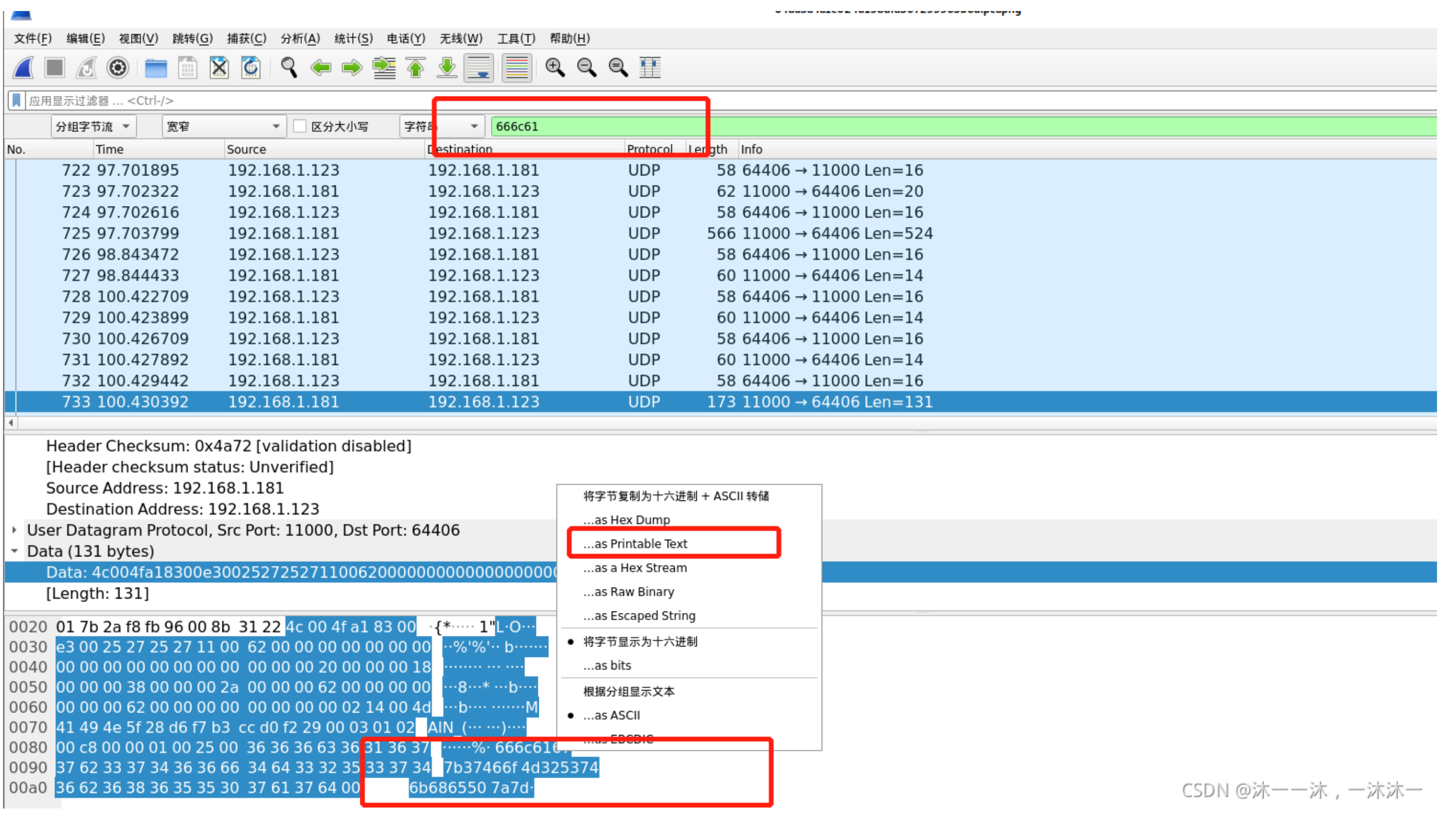
的也一堆，也不知道哪里异常：



.

.

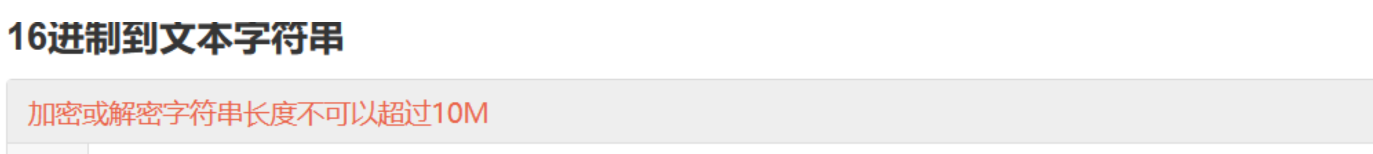
然后就是题目暗示说flag在异常流量中，那直接明文匹配查找不就行了？先搜索flag，无果，换十六进制666c6167试试，查到了，用as printable text 选项dump下来即可：



.

.

结果：



```
1  666c61677b37466f4d3253746b6865507a7d
```

16进制转字符 | 字符转16进制 | 测试用例 | 清空结果 | 复制结果


```
1  flag{7FoM2StkhePz}
```


.

.

总结：

> 1：
> (这里积累第一个经验) 题目描述说已提取出上位机通信流量，尝试分析出异常点，获取FLAG。 flag形式为 flag{}，这其实就是一个暗示，flag就在通信流量中，至于哪里异常，查了资料，有的说UDP的长度有部分异常，要一个个点击查看。可是为什么我感觉UDP大的一堆，小的也一堆，也不知道哪里异常。
> 然后就是题目暗示说flag在异常流量中，那直接明文匹配查找不就行了？先搜索flag，无果，换十六进制666c6167试试，查到了，用as printable text 选项dump下来即可。

解毕！敬礼！