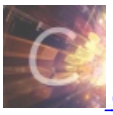
【XCTF 攻防世界】MISC 杂项 高手进阶区 就在其中

原创

Kal1 于 2020-08-13 17:38:17 发布 675 收藏 1

分类专栏： CTF刷题 杂项 文章标签： 安全 openssl 加密解密

本文链接：https://blog.csdn.net/weixin_45844670/article/details/107985213



题目链接：https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4925&page=2

下载链接得到一个流量包

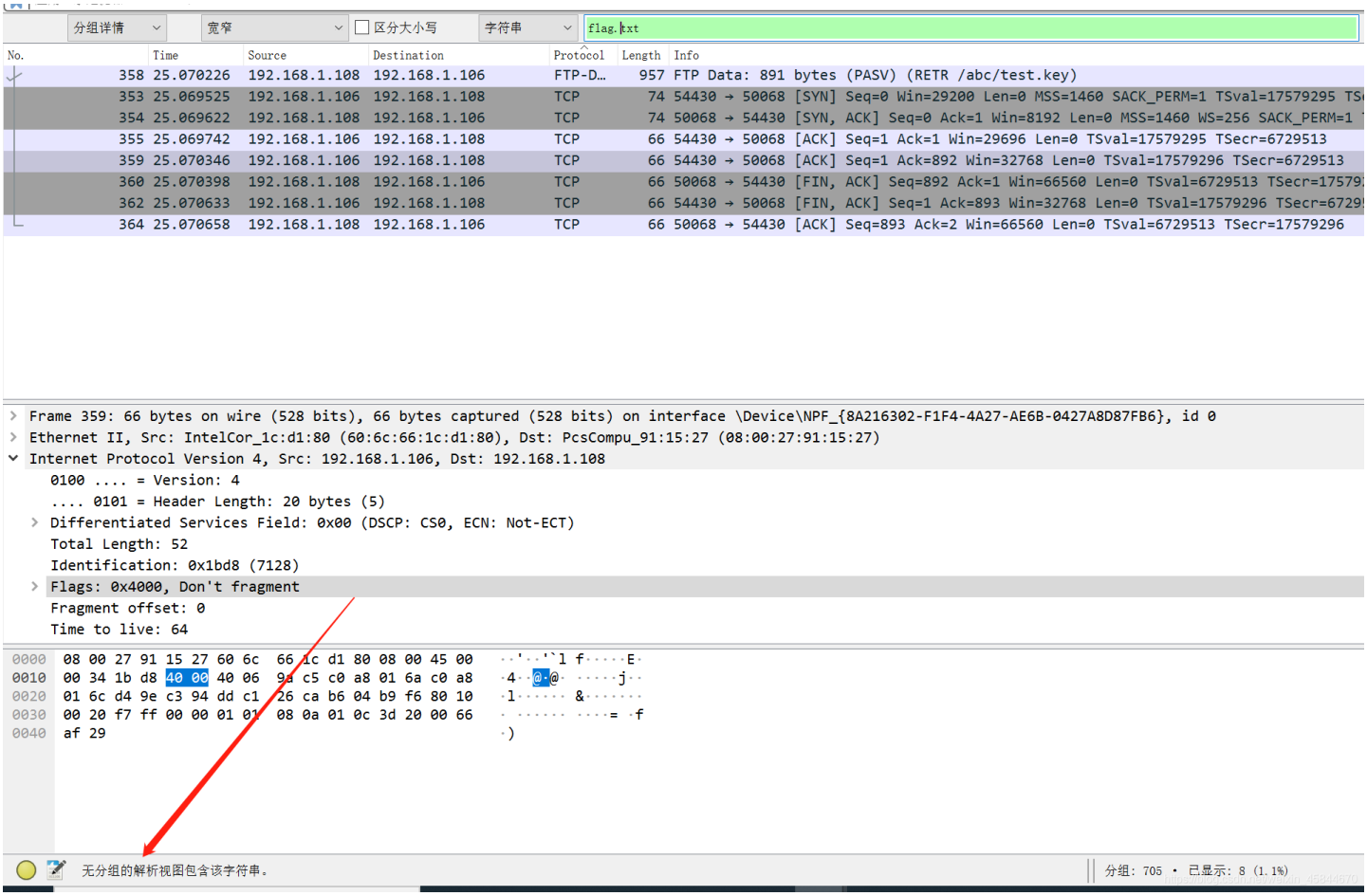
刚开始想用解压软件看看有没有什么隐藏文件，结果发现只有一个key.txt

但是用了好多编码方法都不对

于是打算用流量包看看

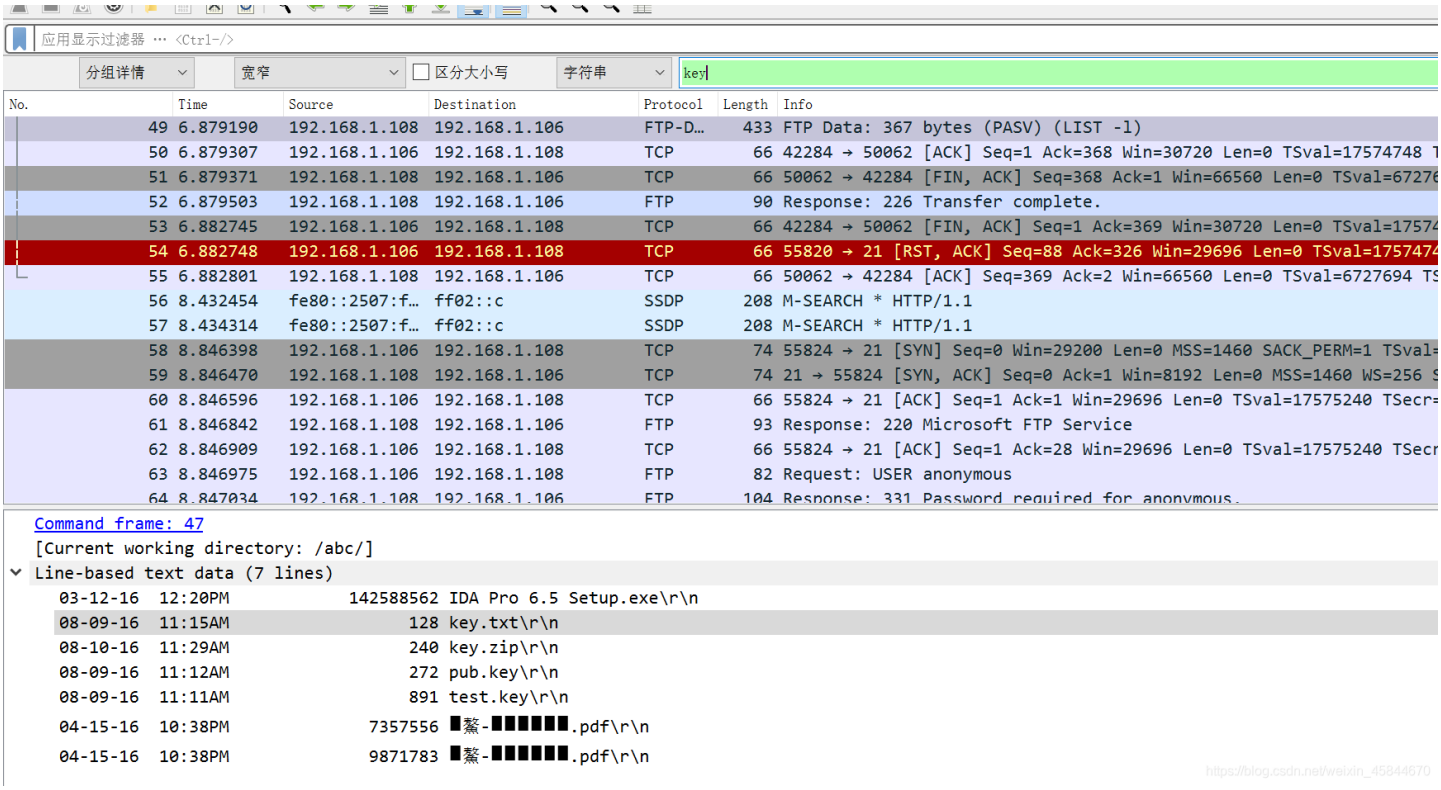
□□沙?□嫸f懵q鳇?:\檑□38　摸砌?月籍釦豳?轷覿□ 酵h~M牀d謢□闢□U€S　苺猎□□燉醜-□狣忏?叔则趁C??场3?漊虚m

搜索flag.txt，无果



分析流量包发现大部分都是ftp协议，猜测传输的文件中有和flag有关的信息

搜索刚才得到的key，看到



pub.key

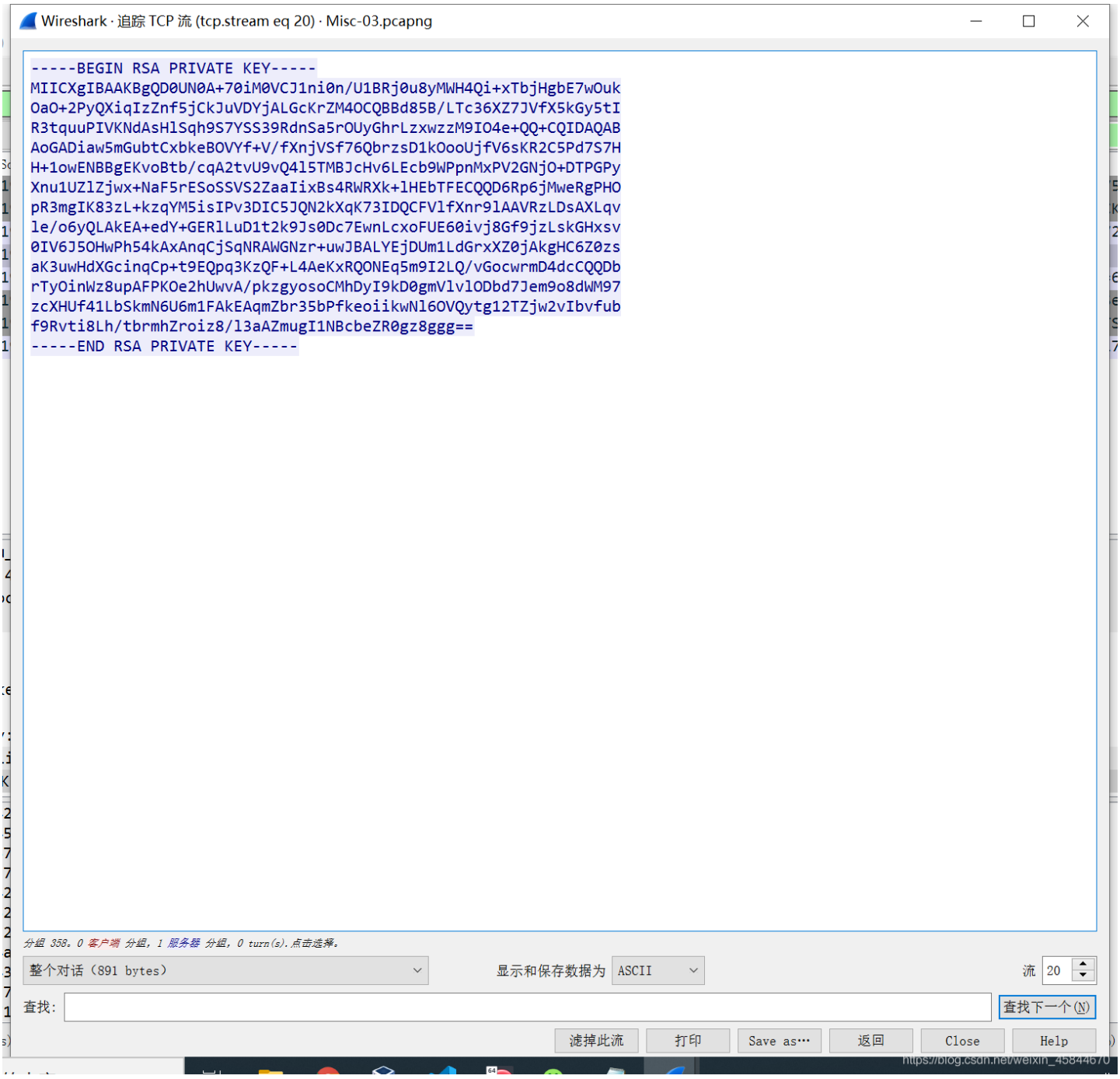
想到rsa加密

那么key.txt不能打开就有可能是因为加密过了

那我们来找一下私钥

搜索RSA或者PRIVATE这些关键字

然后追踪tcp流可以得到：

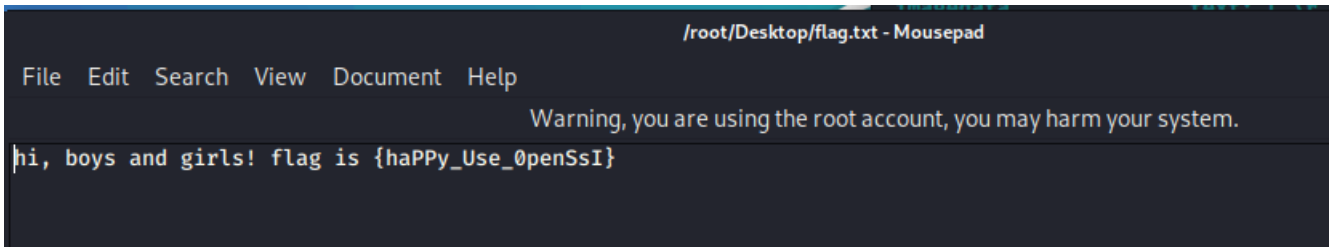


把上面的内容复制出来
存为rsa.key文件

放到kali的openssl进行解密

```
openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt
-in 为要解密的加密文档 -inkey 为密钥 -out 为输出文档
```

得到flag


/root/Desktop/flag.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
hi, boys and girls! flag is {haPPy_Use_0penSsI}