xctf攻防世界 MISC高手进阶区 就在其中

原创

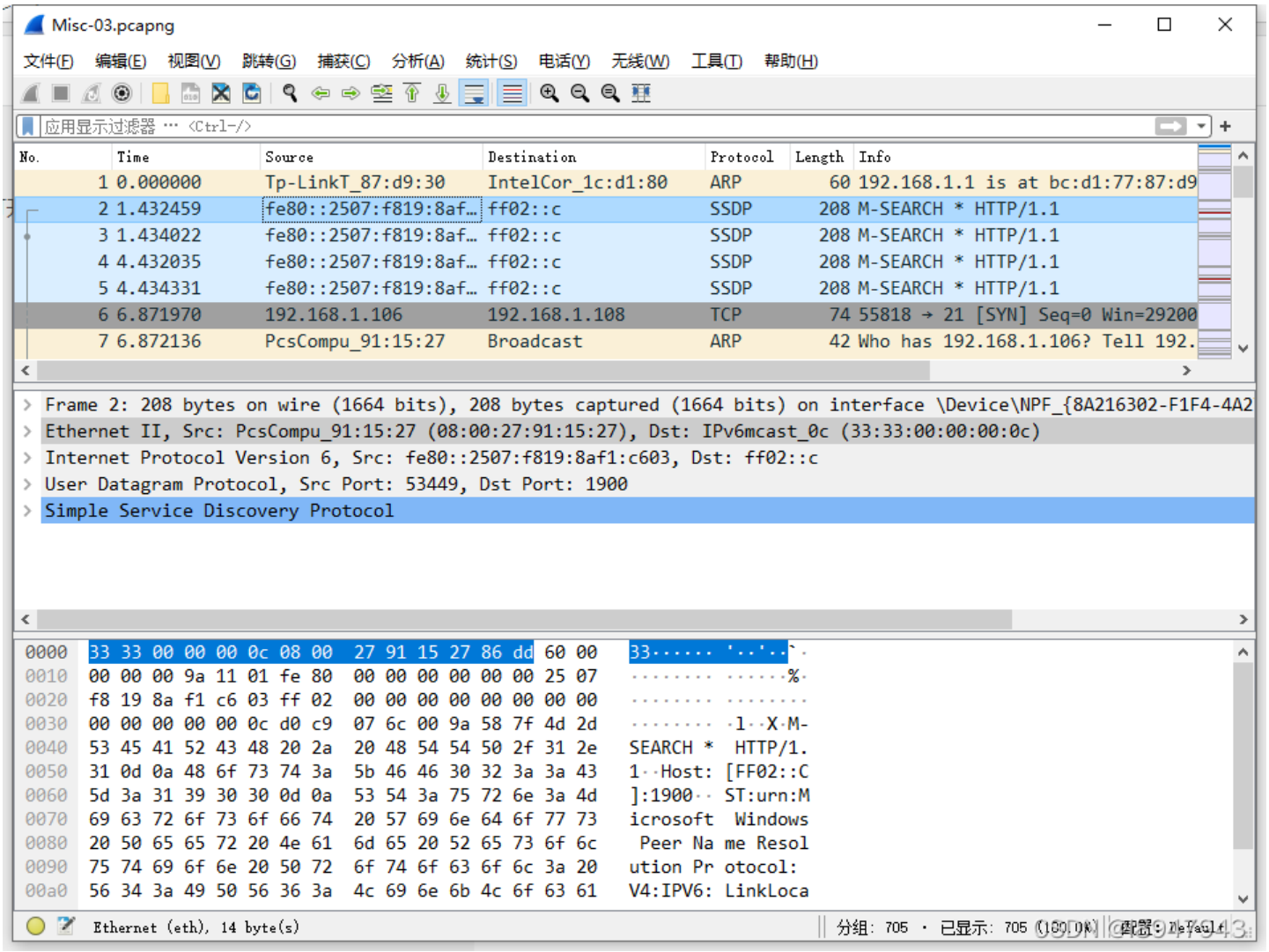
l8947943 于 2022-01-17 11:45:45 发布 6132 收藏

分类专栏： 攻防世界misc之路 文章标签： 安全 web安全

本文链接：https://blog.csdn.net/l8947943/article/details/122535932

1. 进入环境，下载附件

题目给出的是一个pcagpng流量包，果断使用wireshark打开，如图：

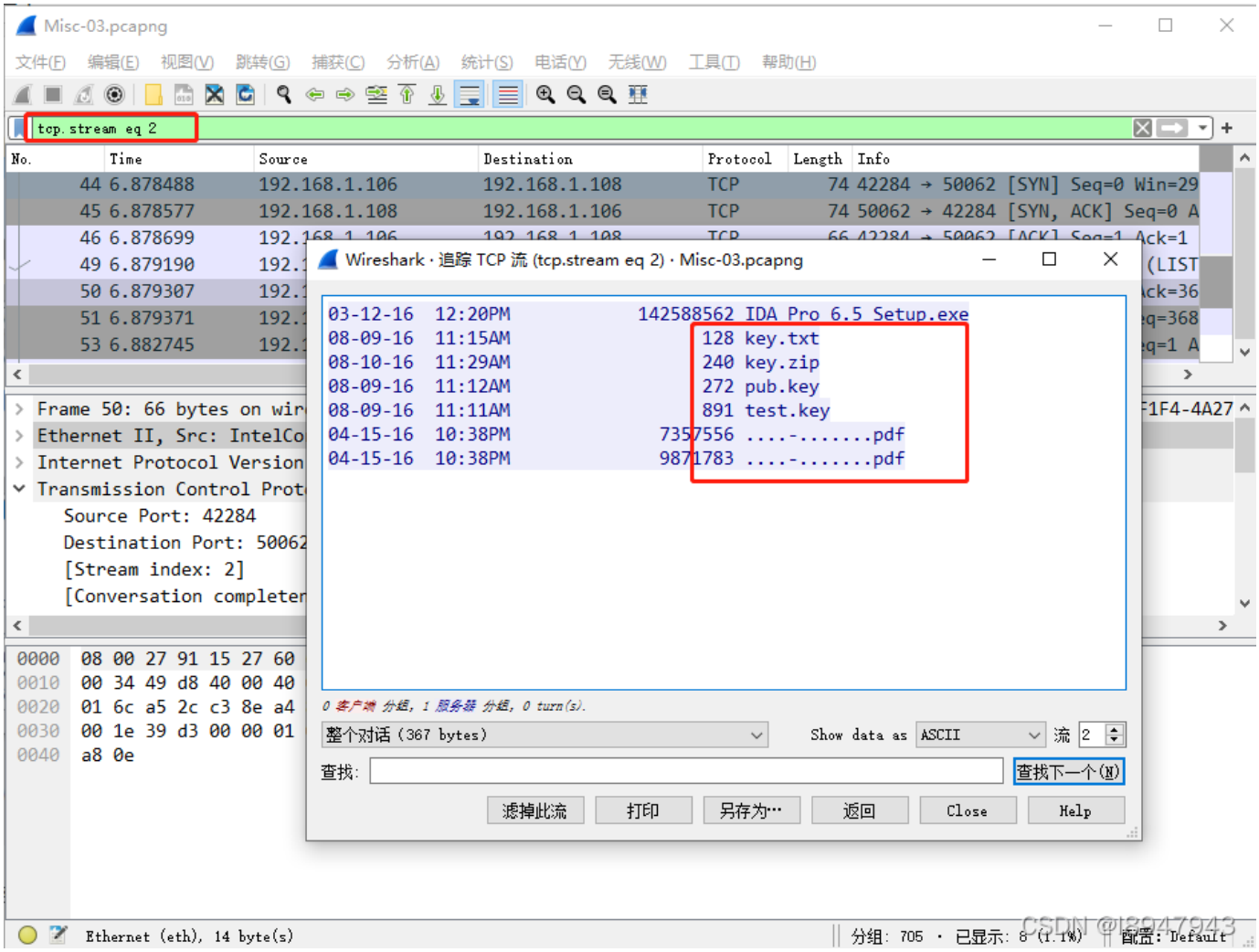


观察了一番，搜索关键词flag，ctf没有任何提示。没有思路，我们分组点点，追踪流试试

2. 问题分析

尝试追踪流

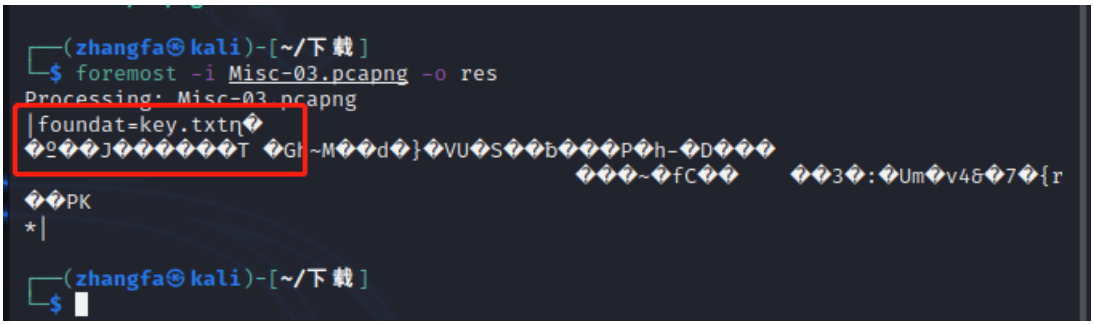
一通尝试后，观察流量包，如图：



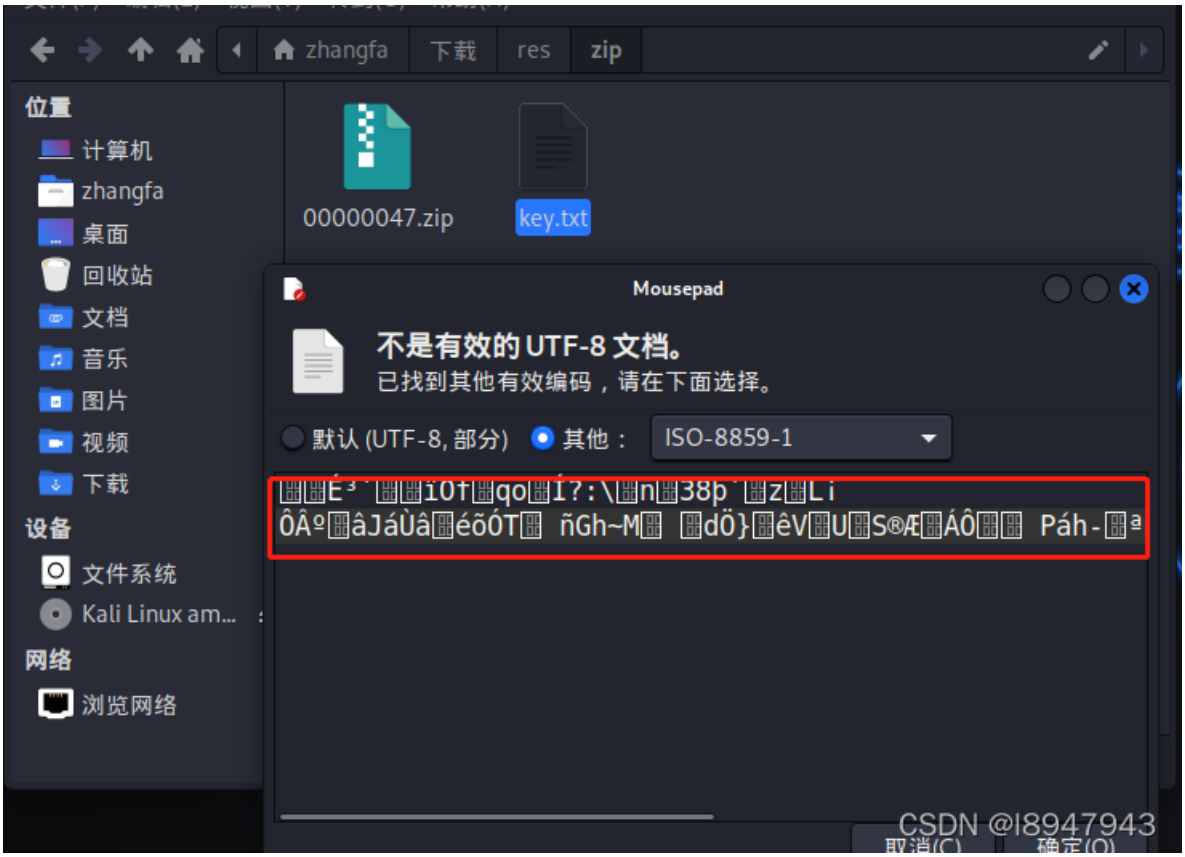
tcp流第二组时候，发现有pdf、key文件，怀疑是文件包含或者隐写。

丢入kali中foremost

```
foremost -i Misc-03.pcapng -o res
```

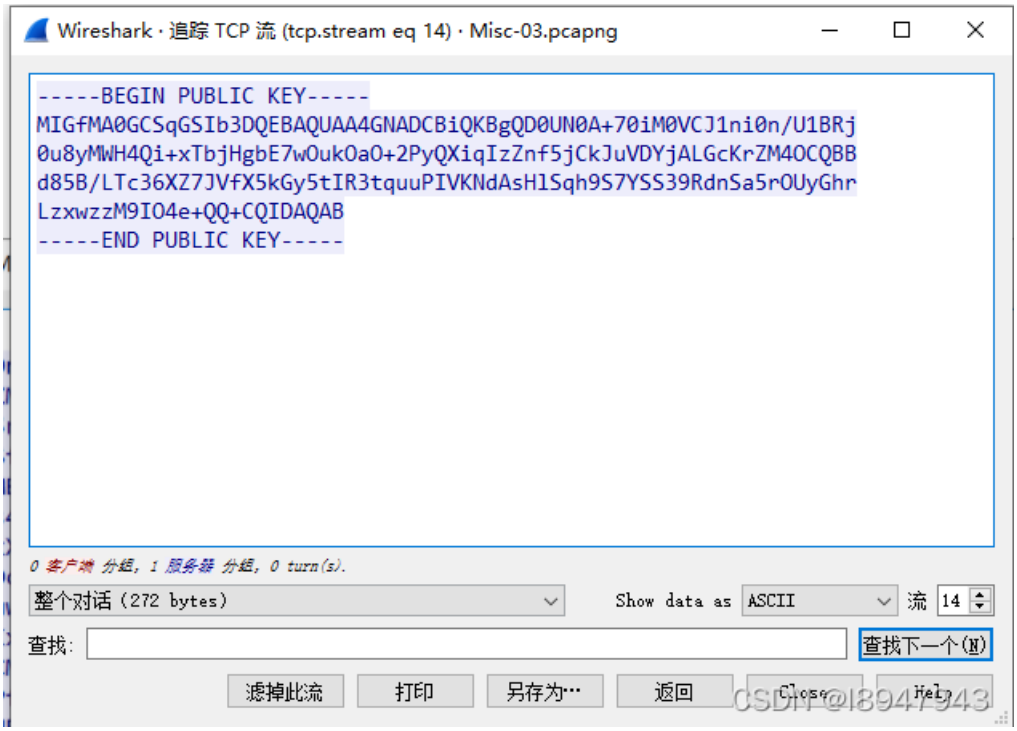


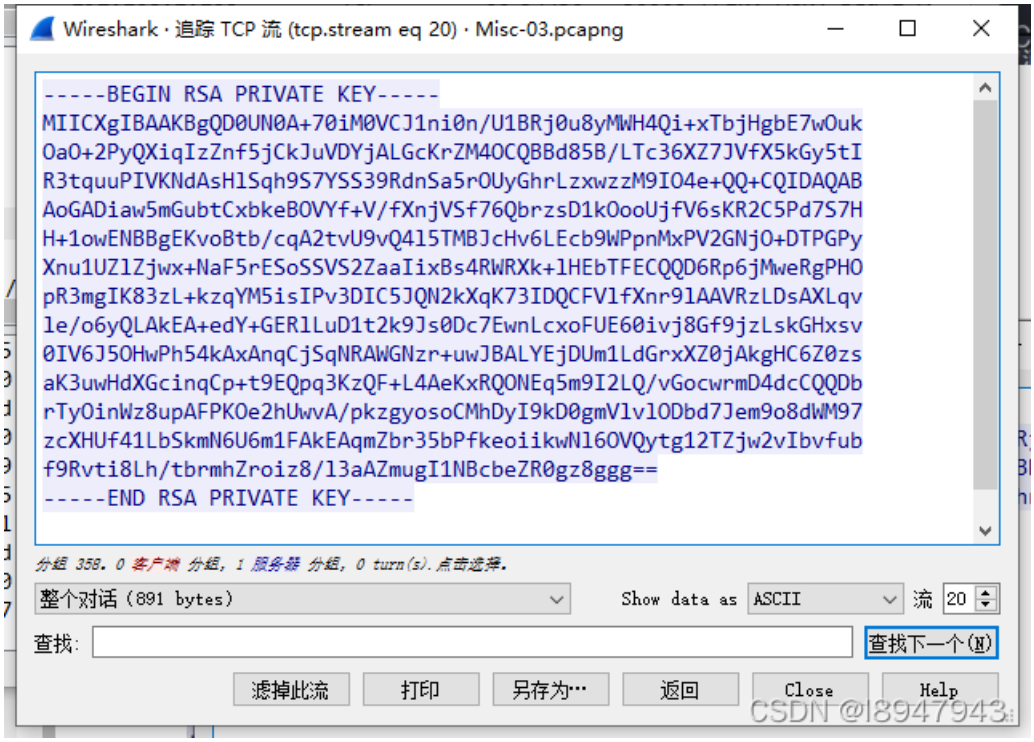
去瞅瞅这个这个文件，打开res->zip->key.txt



一个key一堆乱码？尝试其他编码格式后，发现没有任何变化。。。没有思路了，是不是丢掉了什么！
怀疑是被加密的东西，因为前面分析流量包有pub.key，去shark中搜搜去。

找到密钥





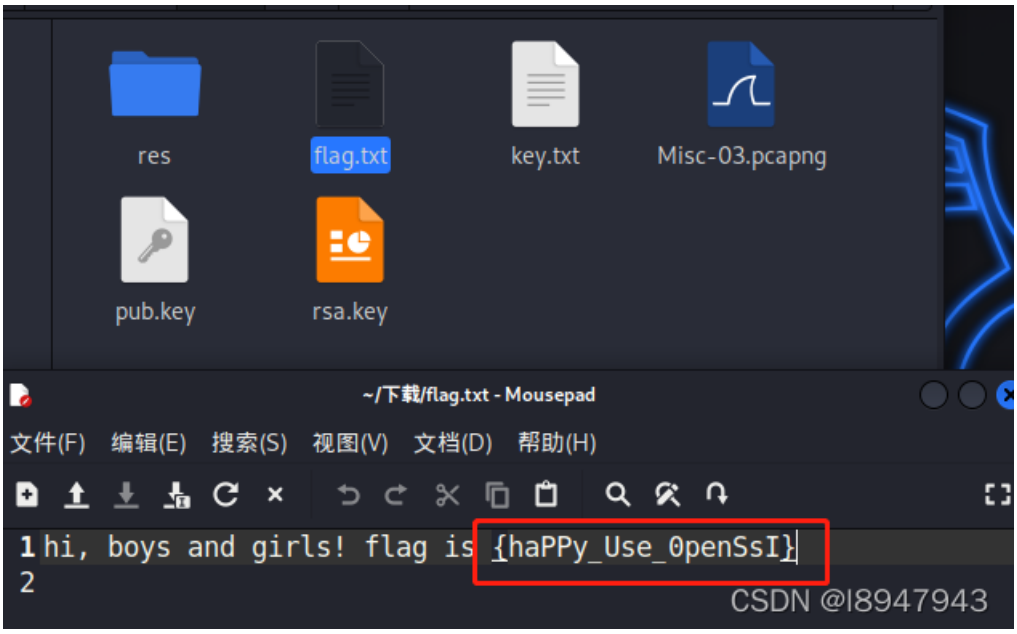
一共发现了两个key文件，突然想起曾经研究过的rsa非对称加密，而出现publickey和私钥，大体思路就明朗了。

OpenSSL解密

发现wp是让rsa去解密txt…查了查使用openssl的加密命令：

```
openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt
```

结果如图：



最终答案为：`flag{haPPy_Use_0penSsI}`

3. 总结

wireshark用的不熟，好麻烦。另外公钥私钥加密过程是需要进一步了解的。
相关OpenSSL文章：

- https://www.cnblogs.com/274914765qq/p/4675535.html
- https://zhuanlan.zhihu.com/p/91029303
- https://www.cnblogs.com/yangxiaolan/p/6256838.html