

就在其中 攻防世界

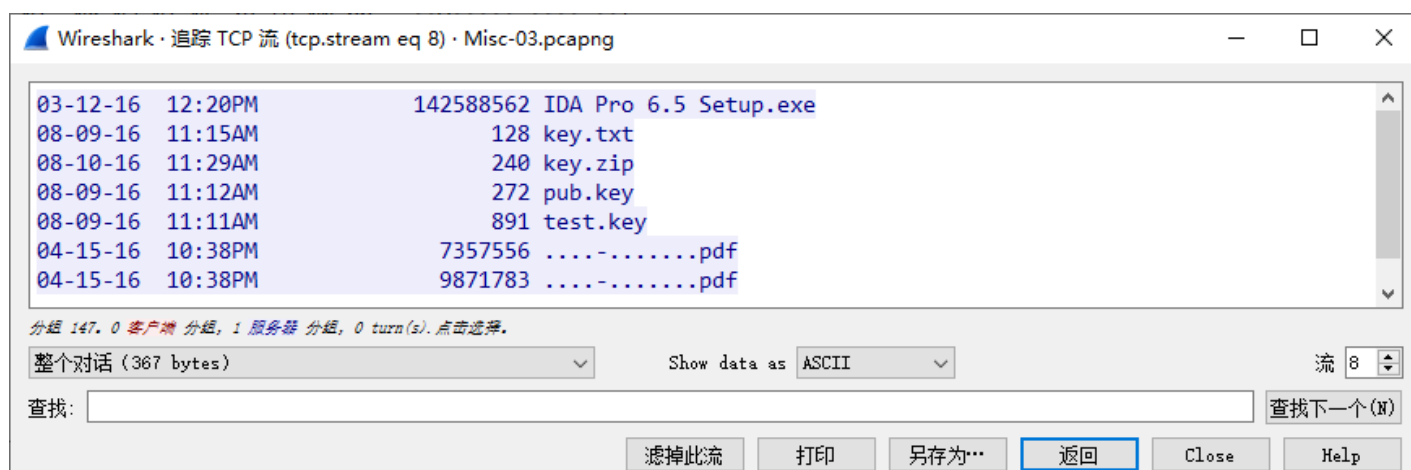
 2分

题目描述

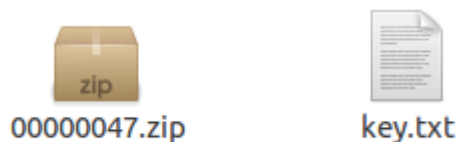
题目是一个压缩包，解压后得到一个 `pcapng` 文件

解题

用 `wireshark` 分析流量包，看到 `key.txt` , `pub.txt` 等文件

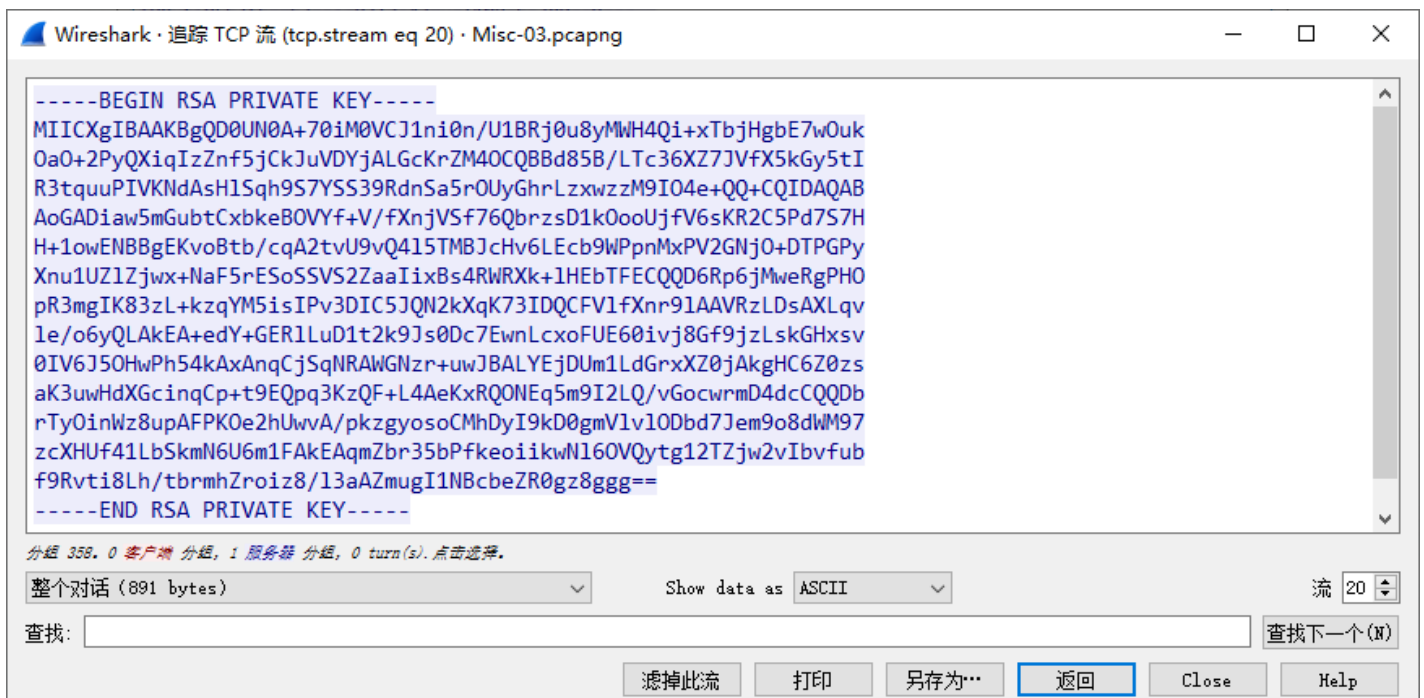


`foremost` 分离文件，得到 `jpg` , `pdf` , `zip` 文件，将 `zip` 解压得到一个 `key.txt` 文件



这个文本不能打开，可能被加密过了，可以推断是RSA加密。

从流量包寻找私钥，保存为 `rsa.key`



使用 `openssl` 进行解密

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

即可得flag

```
ams@ubuntu:~/ws$ openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt
ams@ubuntu:~/ws$ cat flag.txt
hi, boys and girls! flag is {haPPy_Use_0penSsI}
```