xctf攻防世界 MISC高手进阶区 再见李华

原创

l8947943 于 2022-01-17 13:26:22 发布 5747 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/122537741

攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境，下载附件

题目给了一个压缩包，包含一张jpg图片，如图：

没有其他信息，猜测是md5的加密玩意，但是少内容

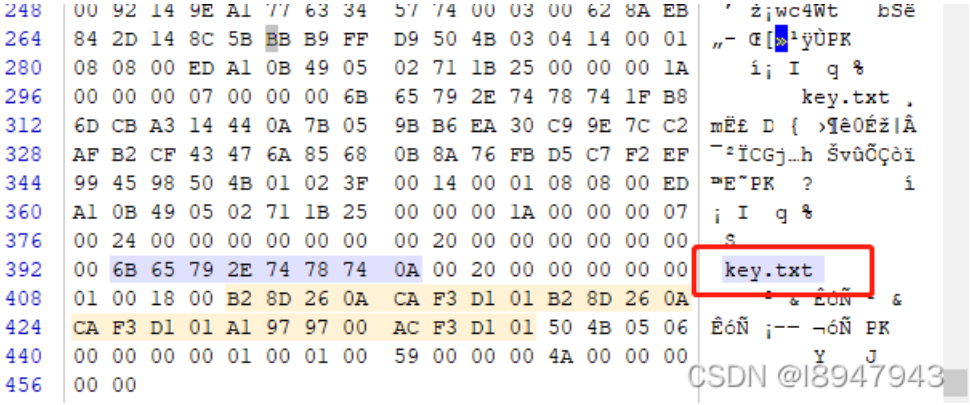
2. 问题分析

1. 丢入StegSolve

   一通乱点，没有发现隐藏的内容，通道分析也没有什么奇怪的点。

2. 丢入winhex

   文件头FFD8FF开头的，emmm，没问题，拉到最后瞅瞅，发现了猫腻，如图：



   隐写包含一个key.txt，果断分离呗

3. 丢入kali进行foremost

```
foremost -i mail2LiHua.jpg -o res
```

结果如图：

果然有东西，打开瞅瞅，发现是个.zip压缩包，需要打开密码

4. 暴力破解

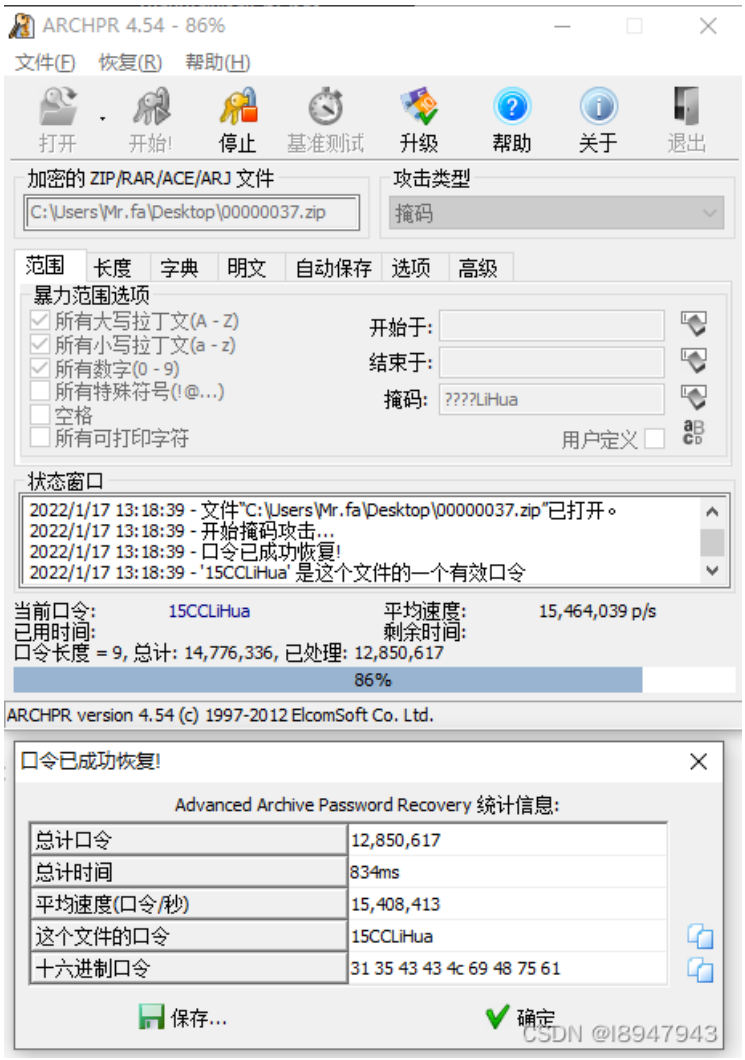
   先分析，题目提示：**假如你是李华（LiHua)，收到乔帮主一封密信，没有任何特殊字符，请输入密码，不少于1000个字。同学，记得署名哦～**

emmm， LiHua收款信件，且要用于签名，那就用这个作为压缩密码试试，发现打不开！

看了看其他人的wp，使用的掩码匹配！不过神仙们，你们怎么知道构造几位字符啊，我一点都找不到位数方向。。。

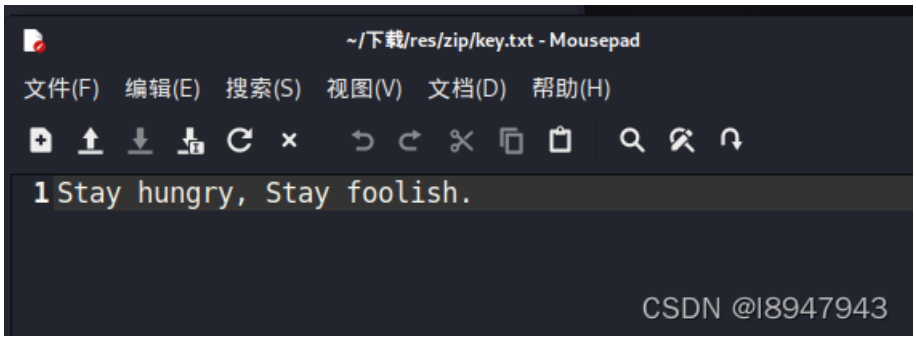
妈的，吃完饭想了想，明白了为啥用四位，继续补充。**题目说不少于1000字，这1000指的不是真的1000个，而是四位字符！！！所以构造的是???LiHua**。真各种脑洞猜

使用工具ARCHPR，如图：



解压码为：15CCLiHua

解压结果如图：



最终的答案为：`Stay hungry, Stay foolish.`