

# MISC-图片隐写

原创

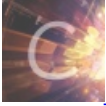
Qwzf 于 2019-07-16 17:55:08 发布 2640 收藏 7

分类专栏: [CTF](#) 文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_43625917/article/details/96160605](https://blog.csdn.net/qq_43625917/article/details/96160605)

版权



[隐写](#) 同时被 3 个专栏收录

2 篇文章 0 订阅

订阅专栏



[CTF](#)

30 篇文章 6 订阅

订阅专栏



[MISC](#)

4 篇文章 0 订阅

订阅专栏

---

## MISC-图片隐写

### MISC1: Paint&Scan

标题的意思是画图和扫描



404

贴图库中找不到该图片  
可能已被删除或者服务到期

题目提示也是。下载题目文件并解压, 得到txt文件。打开

# 404

贴图库中找不到该图片  
可能已被删除或者服务到期

很明显就是画图了。用到画图工具**gnuplot**。所以先替换，将坐标转换成gnuplot能识别的格式

# 404

贴图库中找不到该图片  
可能已被删除或者服务到期

# 404

贴图库中找不到该图片  
可能已被删除或者服务到期

然后开始画图，画图命令 `plot "Paint&Scan.txt"`



# 404

贴图库中找不到该图片  
可能已被删除或者服务到期

画出了张二维码



# 404

贴图库中找不到该图片  
可能已被删除或者服务到期

二维码扫一下，得到flag



# 404

贴图库中找不到该图片  
可能已被删除或者服务到期

**MISC2:** 九连环

## 九连环 分值: 20

来源: 实验吧

难度: 易

参与人数: 5103人

Get Flag: 1230

flag格式: flag{xxx}

解题链接: <http://ctf5.shiyanbar.com/stega/huan/123456cry.jpg>

题目没有提示。打开链接保存jpg图片

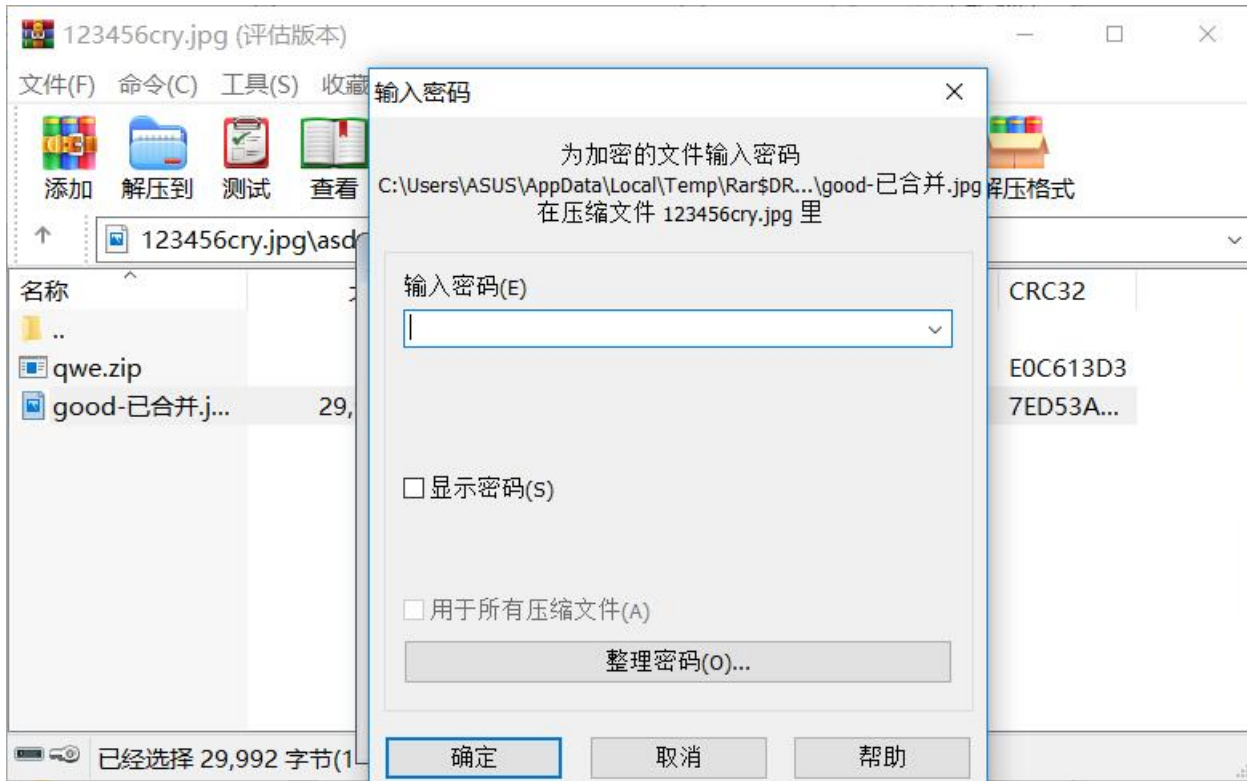
### 留下了委屈的泪水



binwalk分析一下

```
MINGW64:/d/网安/网安工具/隐写工具/图片隐写/分离工具/binwalk-master/binwalk-master/build/scripts-3.7
ASUS@LAPTOP-5D8T0U02 MINGW64 /d/网安/网安工具/隐写工具/图片隐写/分离工具/binwalk-master/binwalk-master/build/scripts-3.7
$ python3 binwalk 123456cry.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
19560       0x4C68       Zip archive data, at least v1.0 to extract, name: asd/
48454       0xBD46       Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184,
name: asd/qwe.zip
48657       0xBE11       End of Zip archive, footer length: 22
48962       0xBF42       End of Zip archive, footer length: 22
```

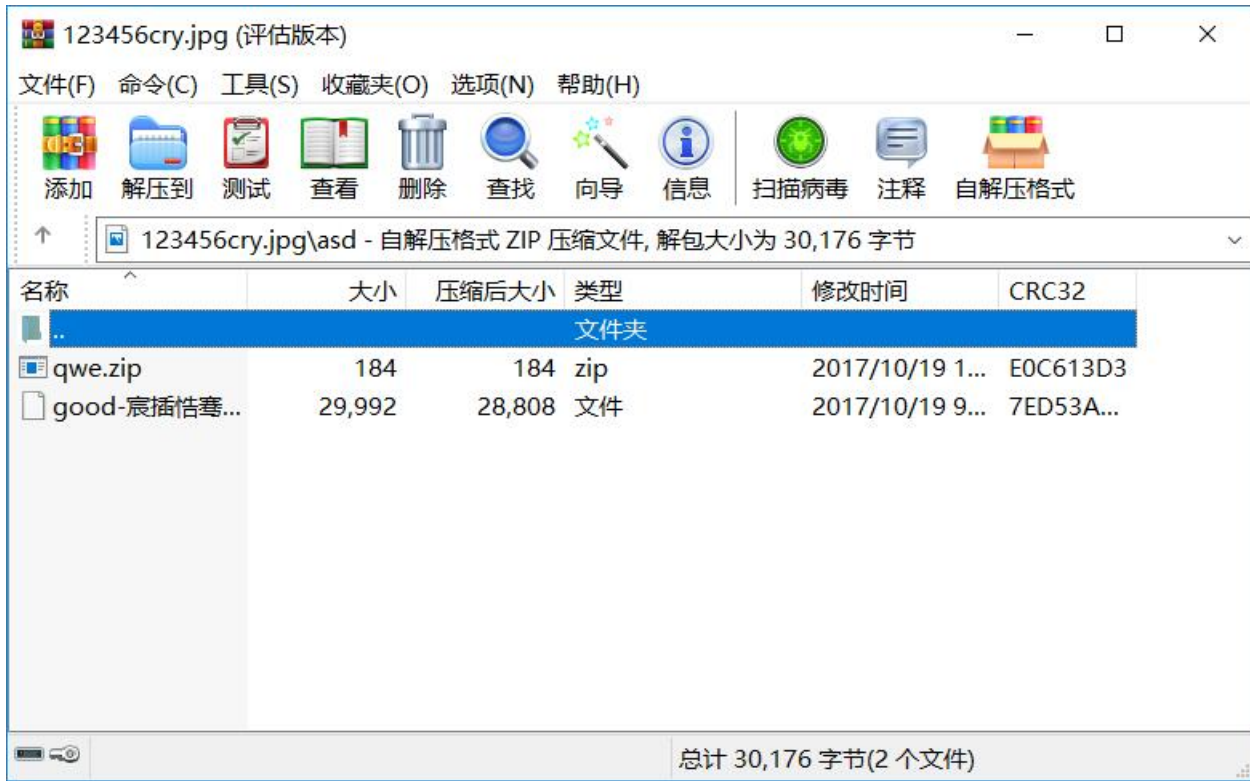
图片里隐藏了文件，foremost分离一下。为了方便，可以直接用winRAR打开jpg图片，并解压隐藏文件。



有一个加密了。先看是不是伪加密

00	01	00	18	00	69	B8	48	34	83	48	D3	01	69	B8	48	i	,	H4fhÓ	i	,	H
34	83	48	D3	01	E9	FC	59	31	83	48	D3	01	50	4B	01	4fhÓ	éüYlfhÓ	PK			
02	3F	00	14	00	01	08	08	00	48	4E	53	4B	8C	3A	D5	?		HNSKE:Ö			
7E	88	70	00	00	28	75	00	00	16	00	24	00	00	00	00	~^p	(u	\$			
00	00	00	20	00	00	00	22	00	00	00	61	73	64	2F	67	"		asd/g			
6F	6F	64	2D	E5	B7	B2	E5	90	88	E5	B9	B6	2E	6A	70	ood-â	·²â	^â¹¶.jp			
67	0A	00	20	00	00	00	00	00	01	00	18	00	69	31	23	g			il#		
00	70	48	D3	01	00	7E	00	00	00	48	D3	01	00	7E	00	~^p	(u	\$			

是伪加密，把504B0102后第五、第六位0108改为0000，即可破解伪加密



解压

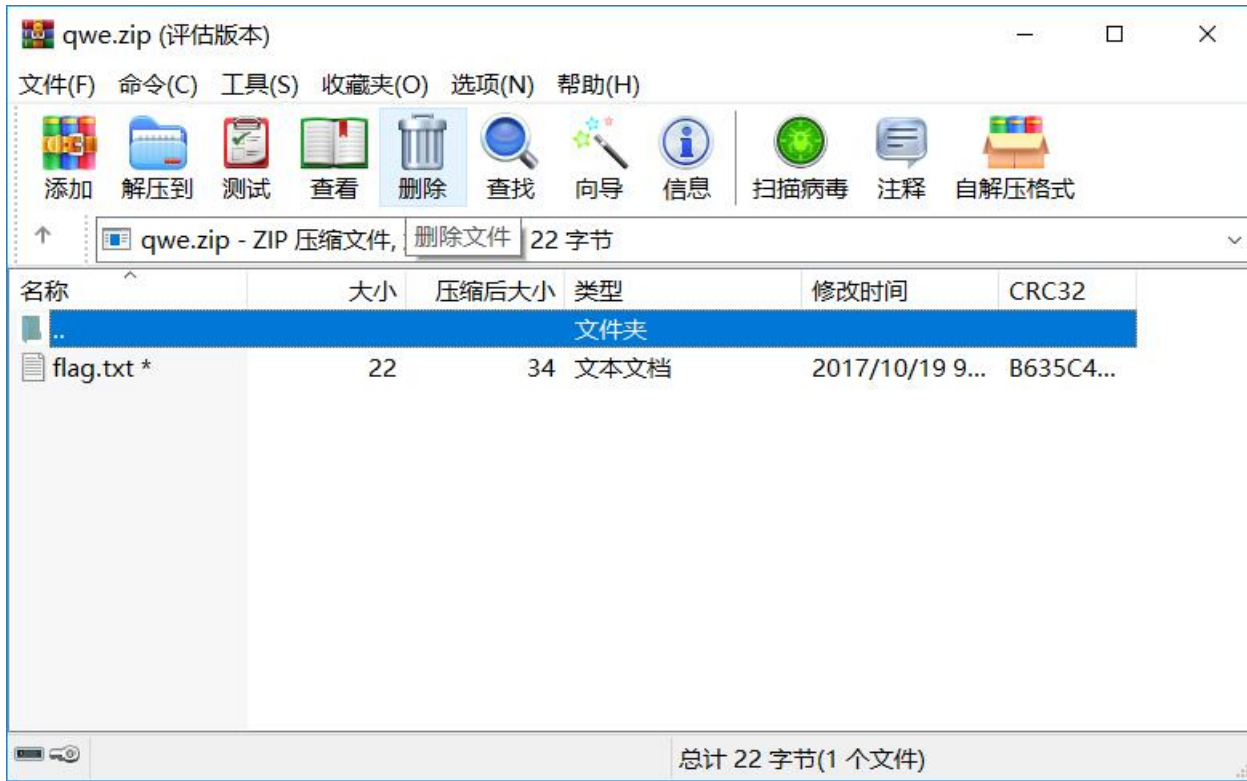


这应该是张jpg图片，用winHex查看果然是。加文件后缀 `.jpg`，打开图片

# 非常好



没有有效信息，那看一下解压得到的qwe.zip压缩包，用winRAR打开

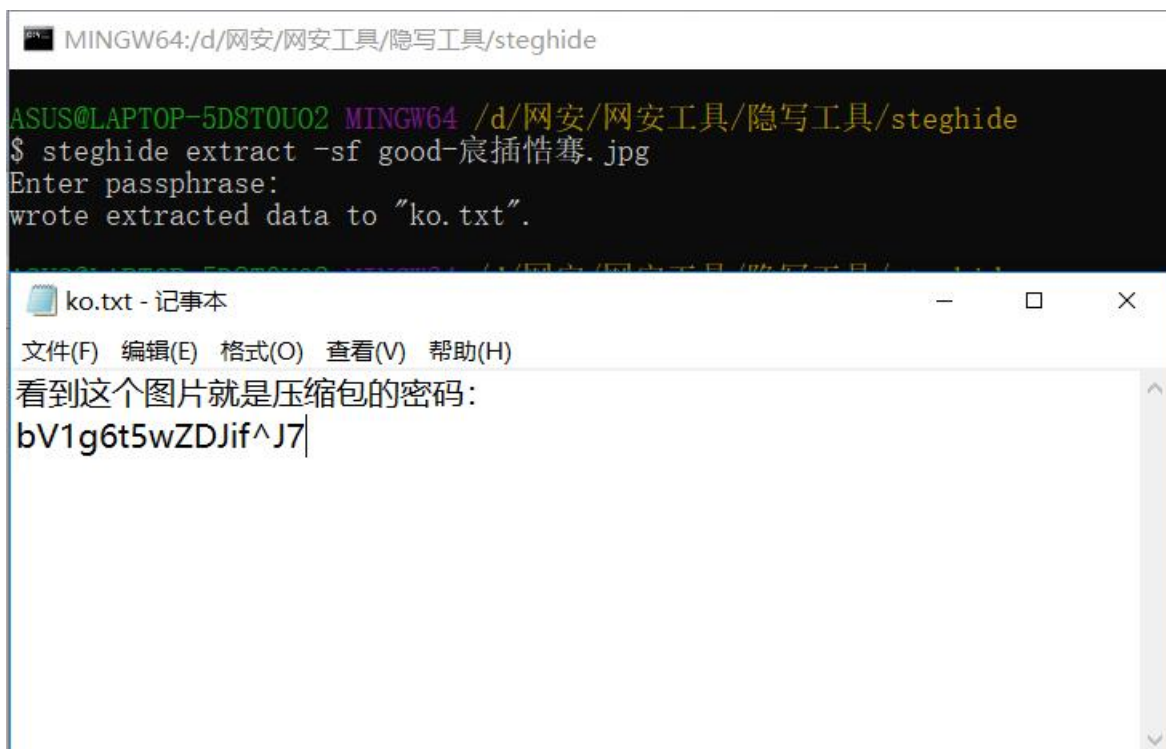


发现加密的flag.txt文件。用winHex打开qwe.zip，发现并不是伪加密。好像进行不下去了，于是参考了下大牛的博客。发现要用到一个工具**steghide**。


用法：`steghide extract -sf picture.jpg`

然后输入密码，没有密码则回车跳过

于是刚才那张图片就可以用到了



得到一个ko.txt文件。打开，发现flag.txt文件的密码了，输入密码，打开flag.txt。得到flag



```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{1RTo8w@&4nK@z*XL}
```

### MISC3: 欢迎来到地狱

欢迎来到地狱 分值: 25

来源: [HTTPERROR404](#)

难度: 中

参与人数: 9741人

Get Flag: 1963人

答题人数: 2119人

解题通过率: 93%

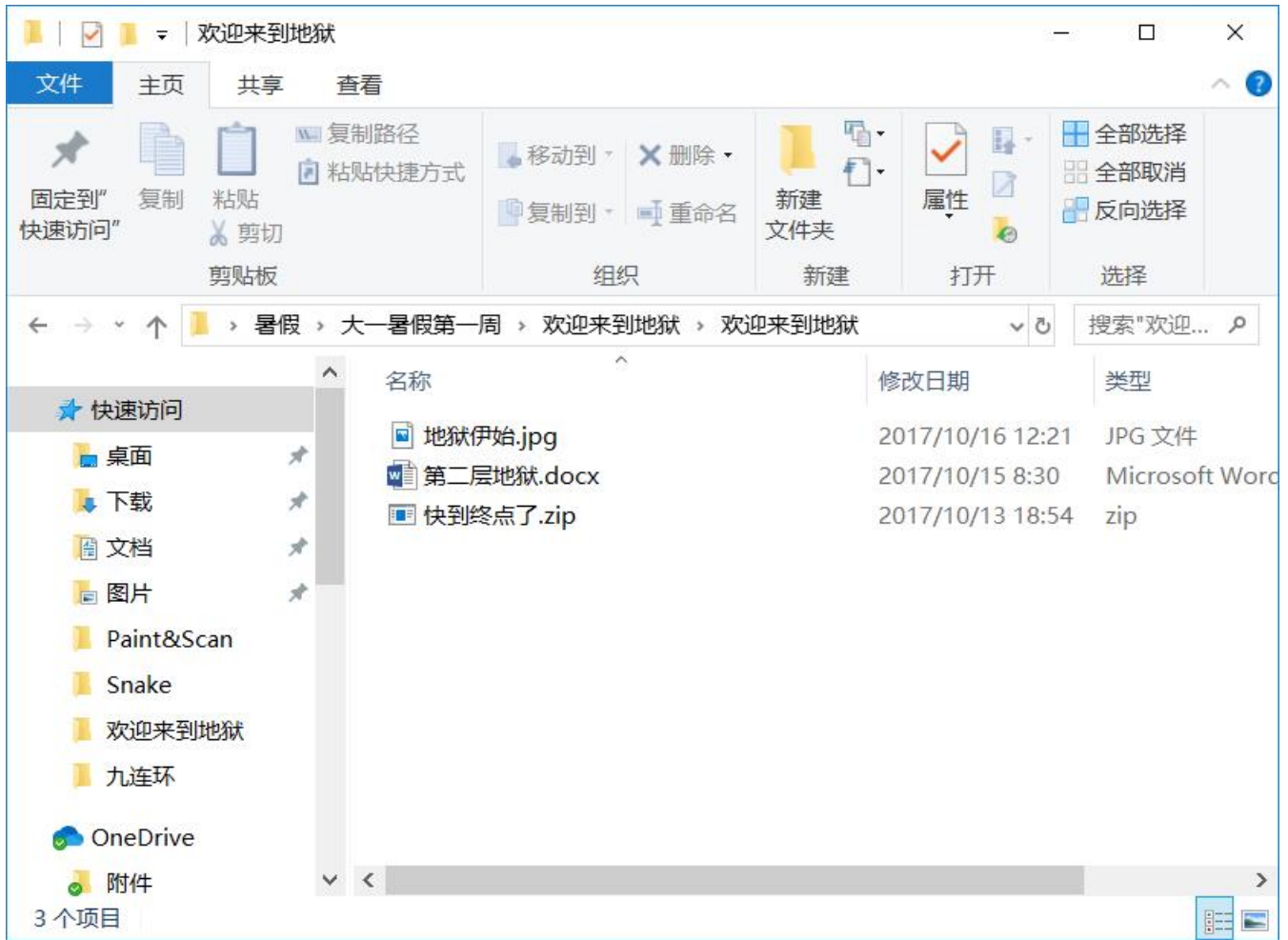
连环套哦。格式CTF{xxxx}。

解题链接: <http://ctf5.shiyanbar.com/stega/hell/欢迎来到地狱.zip>

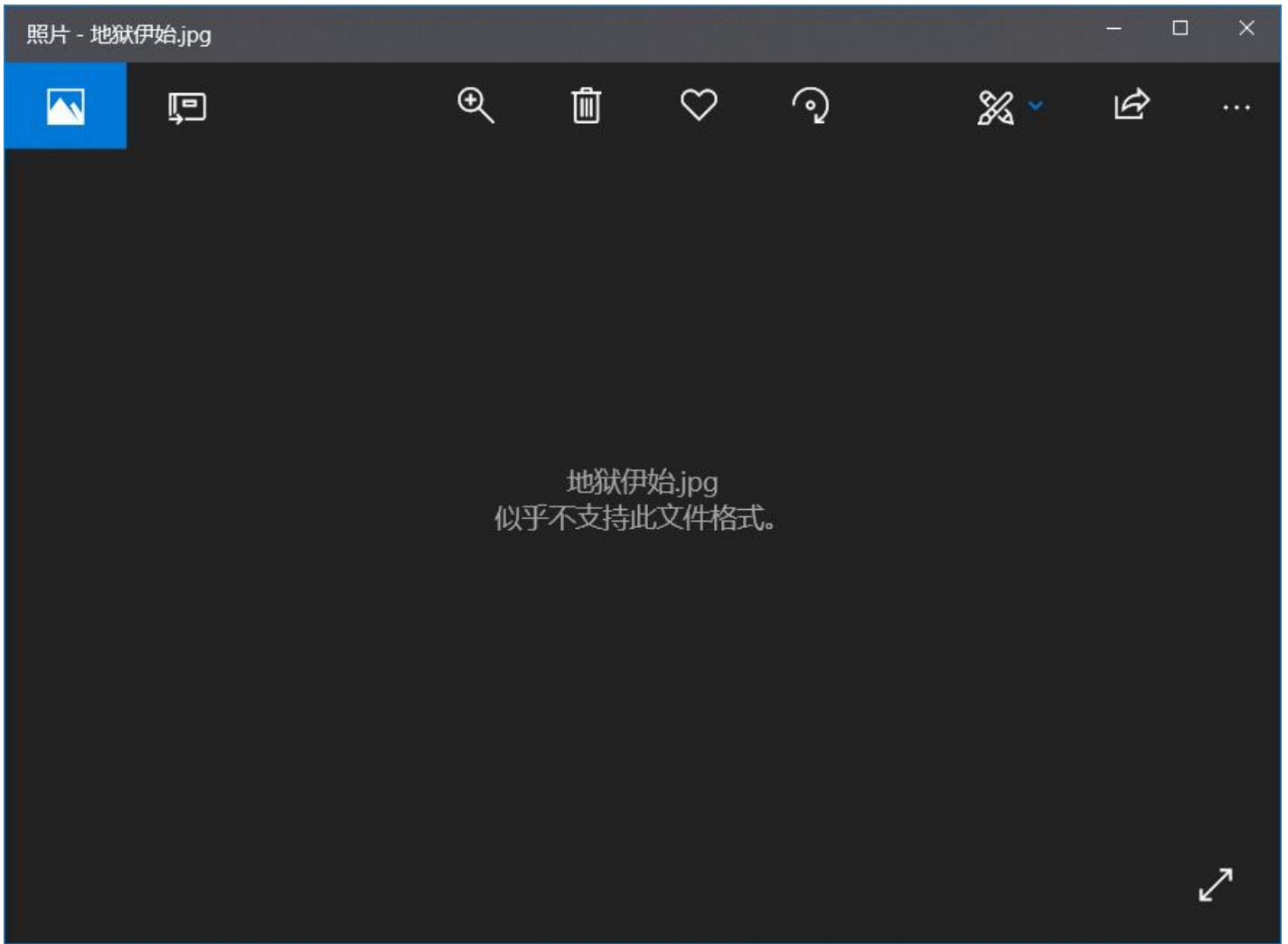
提交

下载题目文件并解压

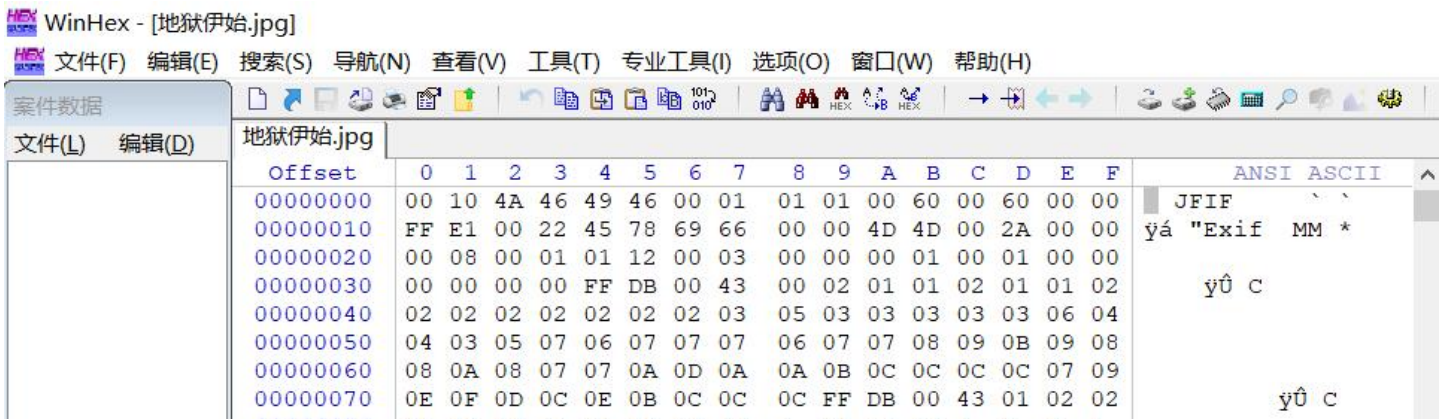




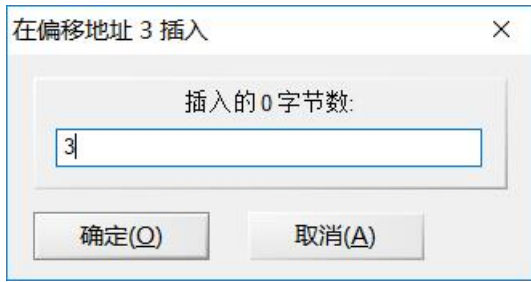
打开地狱伊始.jpg



无法打开，用winHex查看一下文件格式，发现缺少文件头



jpg图片的文件头是FFD8FF，添加文件头



保存图片并打开



图片里有个百度云盘链接，输入浏览器打开



地狱之声.wav

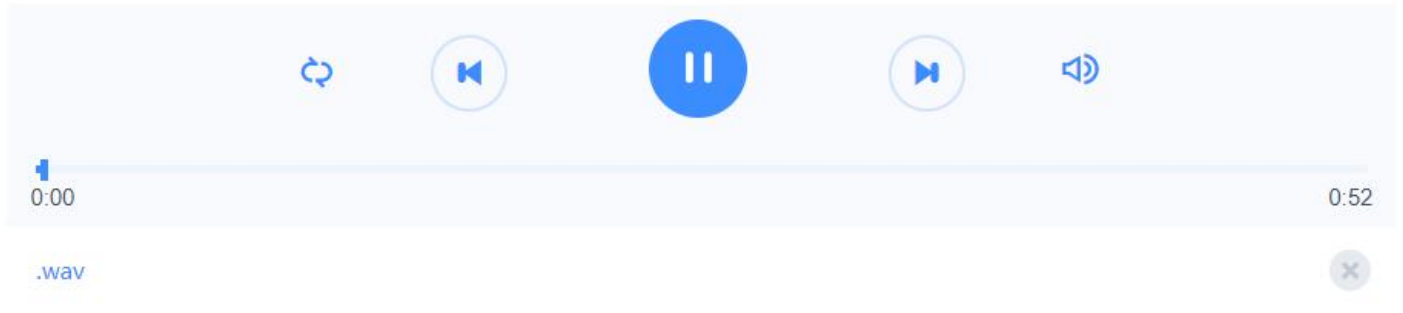
保存到网盘

下载(19.1M)

保存到手机

举报

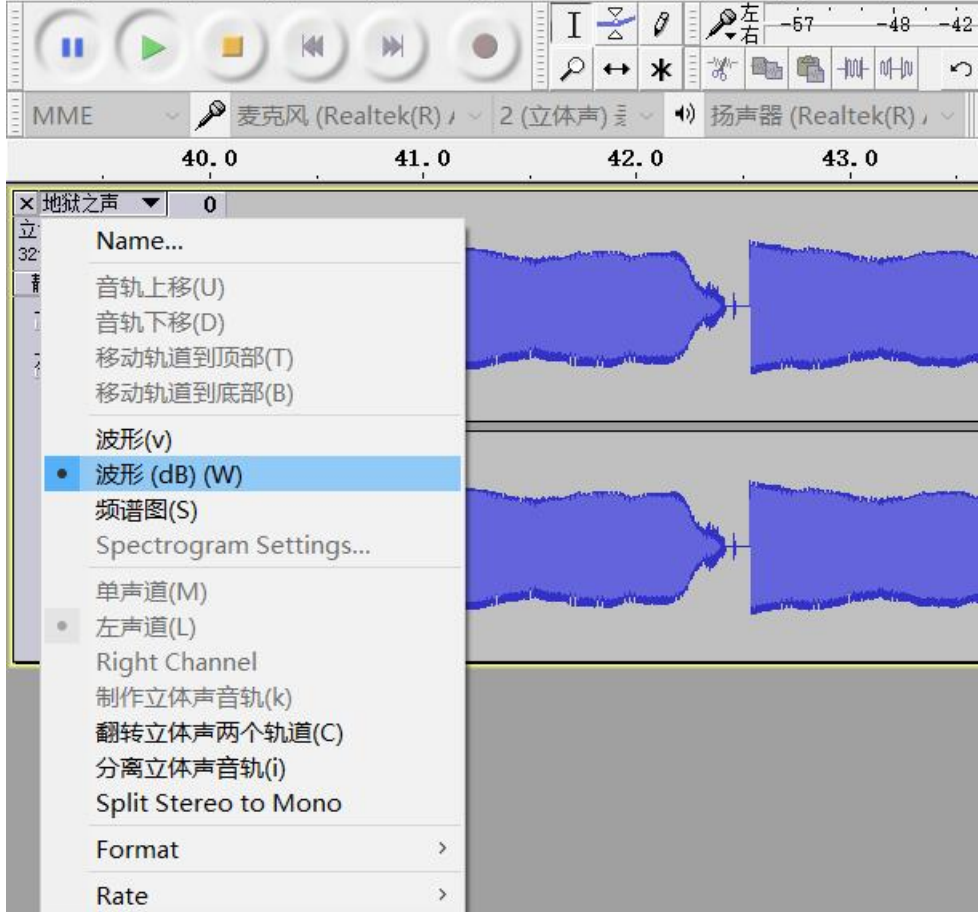
2017-10-16 11:47 失效时间: 永久有效



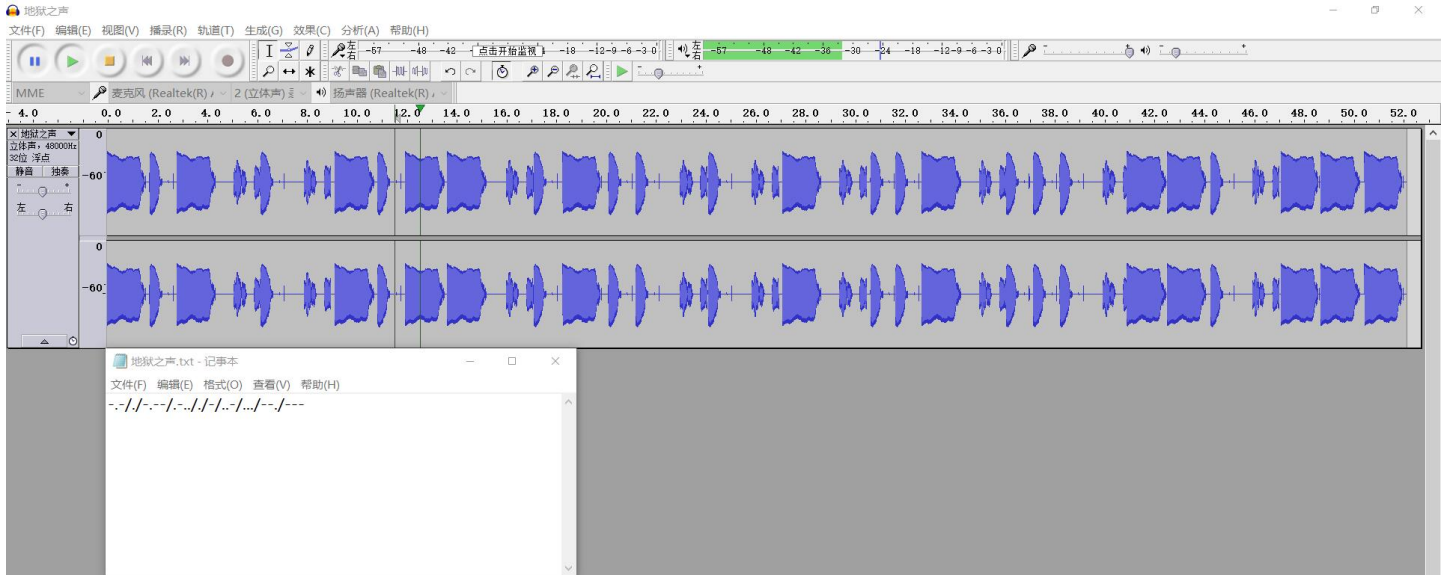
下载wav音频文件，播放，发现比较有规律。应该是音频隐写了。使用音频分析工具Audacity打开wav文件，然后

地狱之声

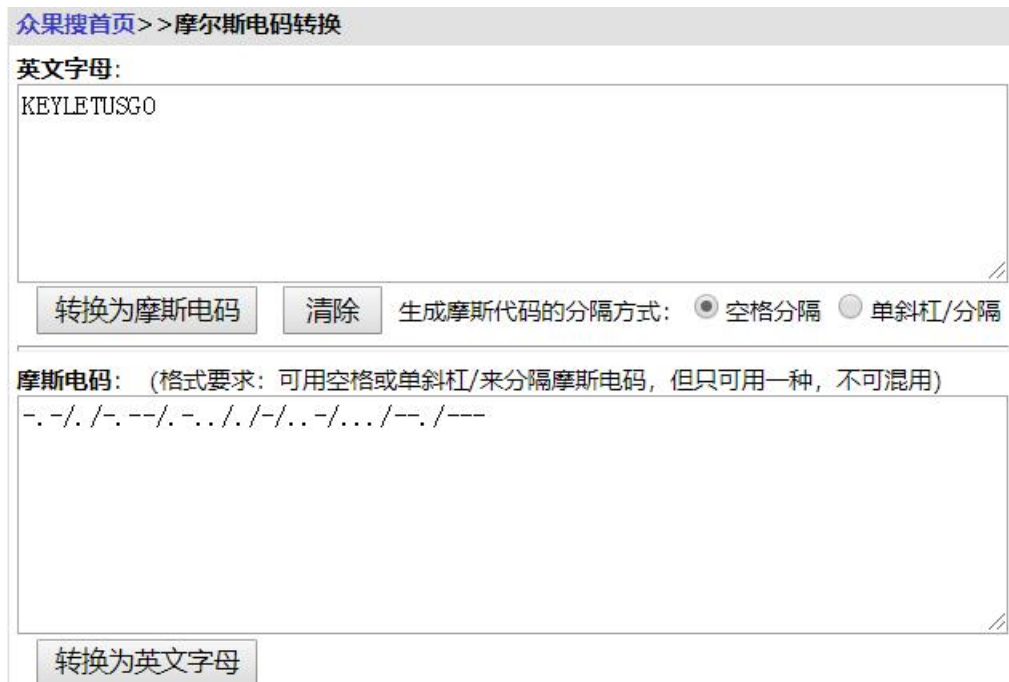
文件(F) 编辑(E) 视图(V) 播录(R) 轨道(T) 生成(G) 效果(C) 分析(A) 帮助(H)



发现大致有三种波形。想到了摩斯电码，于是将不同波形转换成摩斯电码

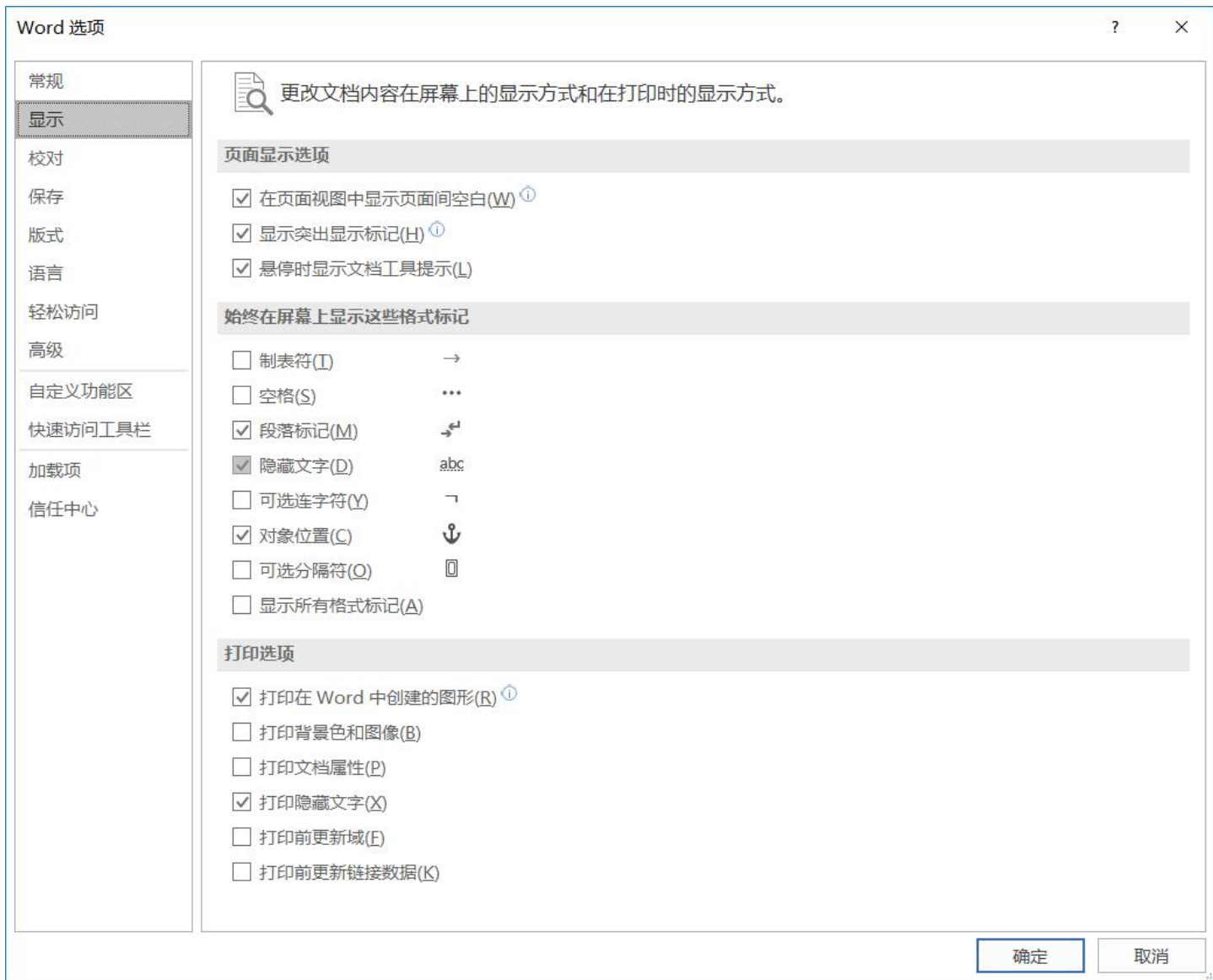


摩斯电码解密得到



打开第二层地狱.docx，发现被加密了。上面应该就是密码了，有点坑的是密码小写，即letusgo

打开之后，选择显示隐藏文字



发现

你现在在第二层地狱中，凶猛的。。。。  
额。。。。哈士奇。。。。把守着通向第三  
层地狱的钥匙，那么。。。。。。。。。。你要  
用你手中的剑（握草，老子剑呢，

image steganography, , , 是不是掉在  
第二层地狱的哪里了)

image steganography(图片隐写术)

解密网站: <http://www.atool.org/steganography.php>

所以保存word文档里的图片，用上面网站解密

www.atool9.com/steganography.php

ATOOOL在线工具  
www.atool.org

PS / 编辑器 多媒体 站长工具 开发者工具 便民工具 关于&合作 QQ登录

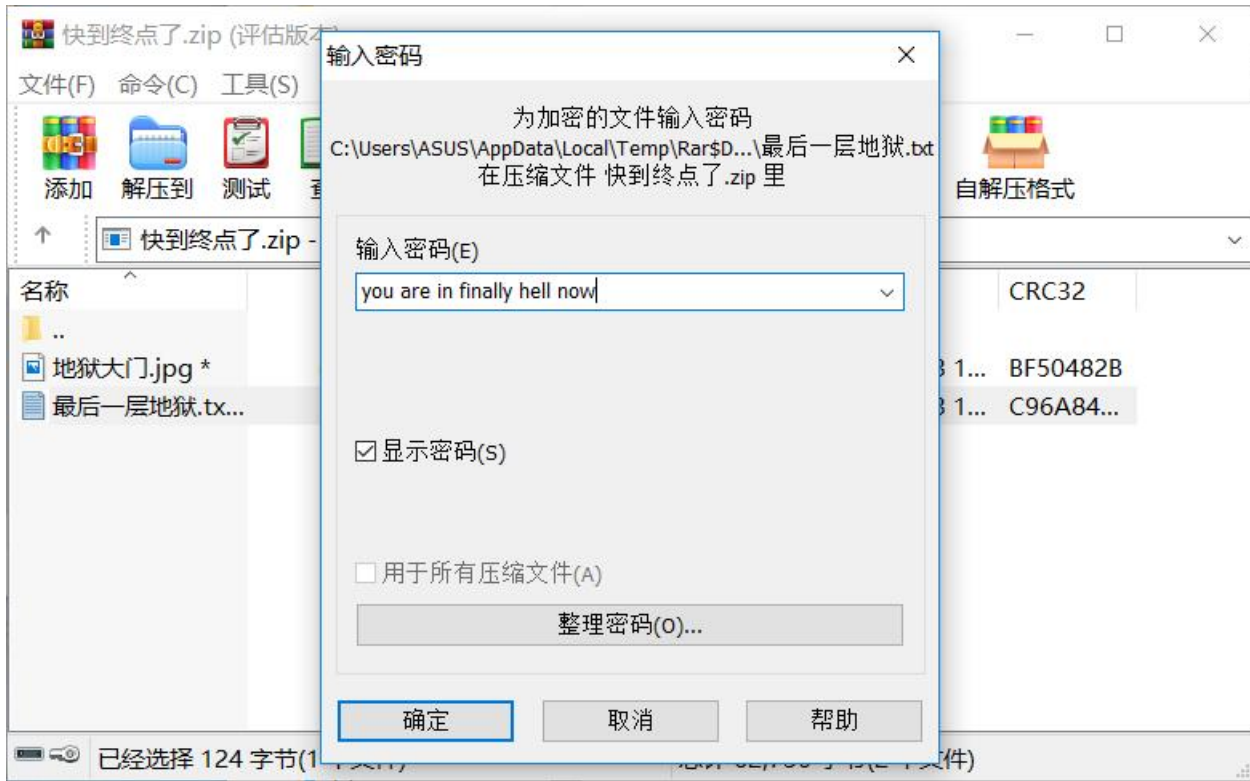
## 二、解密带隐藏信息的图片

1. 从电脑中选择一张带有隐藏信息的图片:  1.png

2. 输入需要解开信息的密码 (如果没有密码可以不填):

图片中隐藏的信息为: **key{you are in finally hell now}**

这应该就是快到终点了.zip的解压密码了



同理解压地狱大门.jpg

打开最后一层地狱.txt



8位二进制一组，二进制转ASCII码



文本

ruokouling

十六进制    autospace



十进制

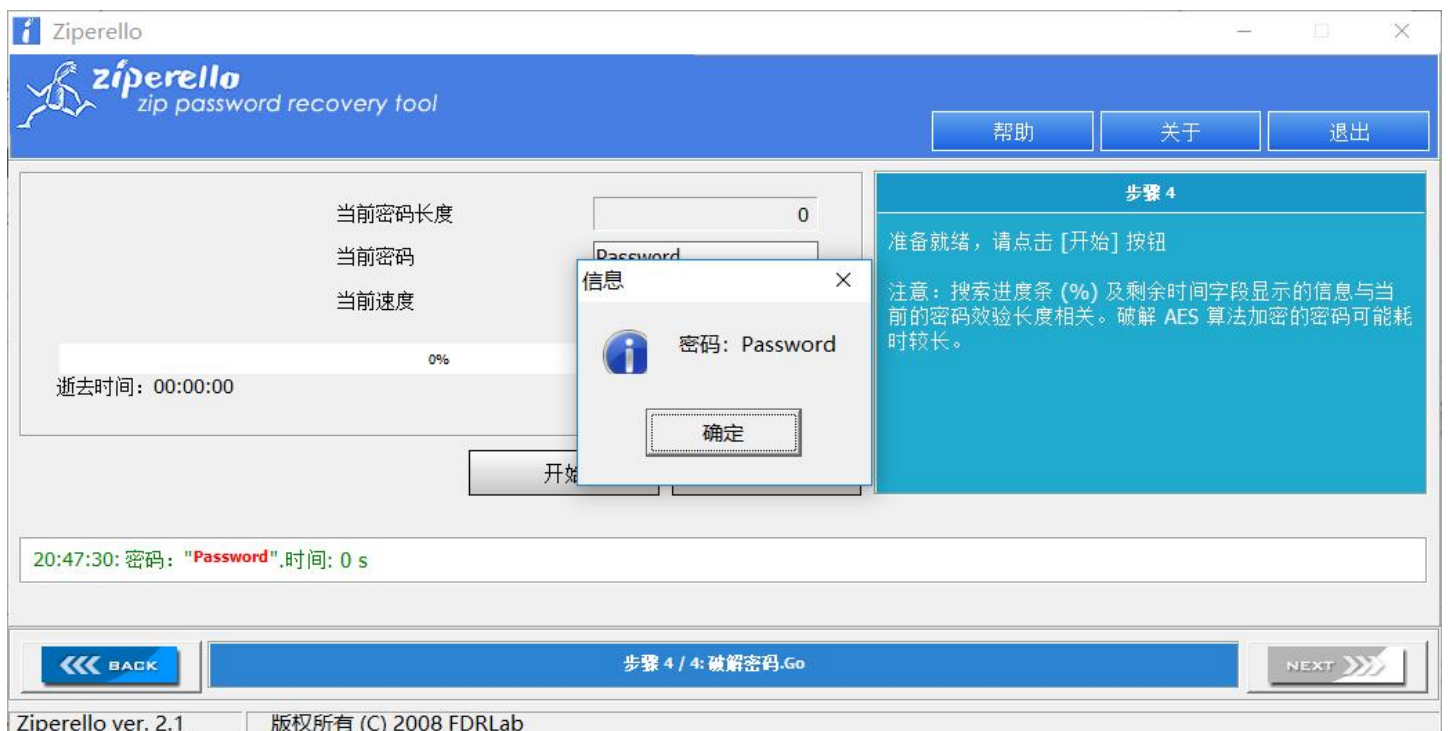


二进制

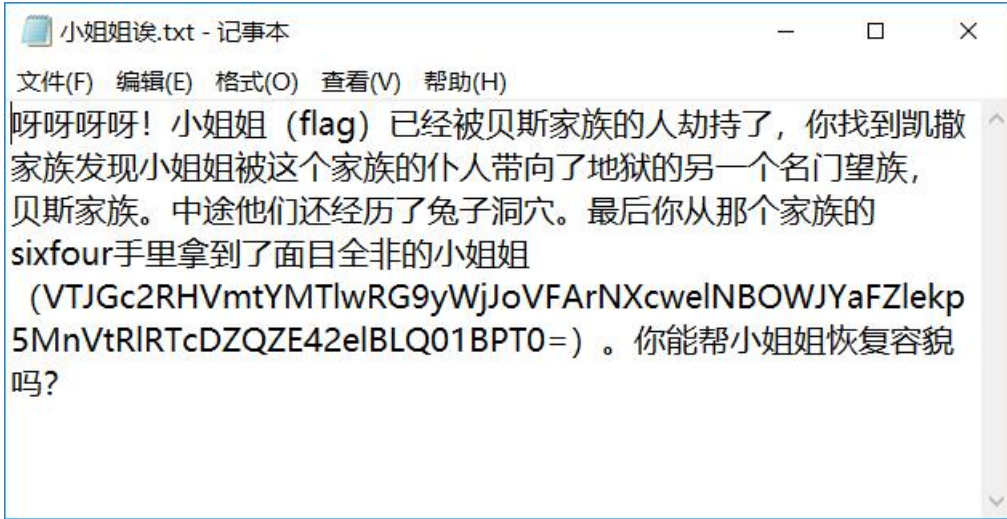
01110010 01110101 01101111 01101011 01101111 01110101 01101100 01101001 01101110 01100111

发现解密结果是：弱口令

将地狱大门.jpg用winRAR打开，发现txt加密文件。并不是伪加密，应该就是上边提示的是弱口令。改地狱大门.jpg后缀为\*\*.zip\*\*，用Ziperello和弱口令字典破解得



输入密码解压txt文件，并打开



很明显Base64解码

## Base64编码转换

```
VTJGc2RHVmtYMTlwRG9yWjJoVFARNXcweINBOWJYaFZlekp5MnVtRlRTcDZQZE42e1BLQ01BPT0=
```

解密结果以16进制显示

```
U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==
```

继续转

# Base64编码转换

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

解密结果以16进制显示

Salted\_\_i□□M4≈mxU{2r<M\*z=ƒ0

发现Salted，应该就是所谓的“加盐”了

## 在线加密解密(采用Crypto-JS实现)

[Feedback](#)

[散列/哈希](#) [BASE64](#) [图片/BASE64转换](#)

明文: <input type="text" value="fxbqwrwnwmngjrxsrnsrnhx"/>	加密算法: <input type="radio"/> AES <input type="radio"/> DES <input type="radio"/> RC4 <input checked="" type="radio"/> Rabbit <input type="radio"/> TripleDes 密码: <input type="text"/> <input type="button" value="加密 &gt;"/> <input type="button" value="&lt; 解密"/>	密文: <input type="text" value="U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA=="/>
---	---	--

试了之后发现是加密算法是Rabbit

看到明文，结合txt文件里“凯撒家族”和“sixfour”，应该要凯撒解密,且偏移量可能是10或6或4。为了方便，我直接找到解密所有结果的

# 解密

fxbarwvwmnrixsmrnhx

解密

使用英文字典智能分析

第1次解密:fxbarwvwmnrixsmrnhx  
第2次解密:ewapayqunvlnfaiwrcmrcmew  
第3次解密:dyzopuotluklephvaplaplfy  
第4次解密:cuynotosktikdogupokpokeu  
第5次解密:btxmsnrjsiicrfntonionidt  
第6次解密:aswlmumairhibmesnmimics  
第7次解密:zrvklqphqshaldmlbmlhbr  
第8次解密:yauikpkogofgzkcalkgkgaq  
第9次解密:xptlioinfoefyibpkifkifzp  
第10次解密:woshinimendexiao1ie1ievo  
第11次解密:vmrgbmlqmcdbznihdihdxn  
第12次解密:umafglgkclbcvymhgchgcwm  
第13次解密:tlpefkfbkabufxlgfbgfbvl  
第14次解密:skodeiei aizatewkfeafeauk  
第15次解密:rincdidhziyzsdviedzedztl  
第16次解密:qimbchgyhxyrcuidcvdcysi  
第17次解密:phlabgbfxgwxqbtbcbxbxrh  
第18次解密:ogkzafaewfvwpasgbawbawog  
第19次解密:nfivyzezdveuyozrfazvzvpf  
第20次解密:meixydvcdutunvqezvuzvuoe  
第21次解密:ldwxcxbtcstmxpdxtyxtnd  
第22次解密:kcgvwbwasbrslwocxwsxwsmc  
第23次解密:ibfuvavzraackvnbwvrvrlb  
第24次解密:iaetuzuvazpajuma vuqvuka  
第25次解密:hzdsvtxpvpitlzutputpiz  
第26次解密:gycrsxswoxnshskvtsotsoiy

得到flag了。

做了三道题，总结完毕。

小白进阶ing