

# CTF-实验吧Writeup-Misc类（持续更新）

原创

IcePeak 于 2018-09-06 20:51:14 发布 1284 收藏 2

分类专栏: [网络安全](#) 文章标签: [CTF-Writeup](#)

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/Nothwest\\_Green/article/details/82467408](https://blog.csdn.net/Nothwest_Green/article/details/82467408)

版权



[网络安全](#) 专栏收录该内容




4 篇文章 0 订阅

订阅专栏

终于想起来更新实验吧STEGA的Writeup了（手动滑稽

## 1.欢迎来到地狱

解压欢迎来到地狱.zip, 看到三个文件。

名称	修改日期	类型	大小
 地狱伊始.jpg	2018/9/5 20:29	JPG 文件	54 KB
 第二层地狱.docx	2017/10/15 8:30	Microsoft Word	970 KB
 快到终点了.zip	2017/10/13 18:54	好压 ZIP 压缩文件	62 KB

尝试打开地狱伊始.jpg文件, 当然打不开, 走不完的是出题人的套路~

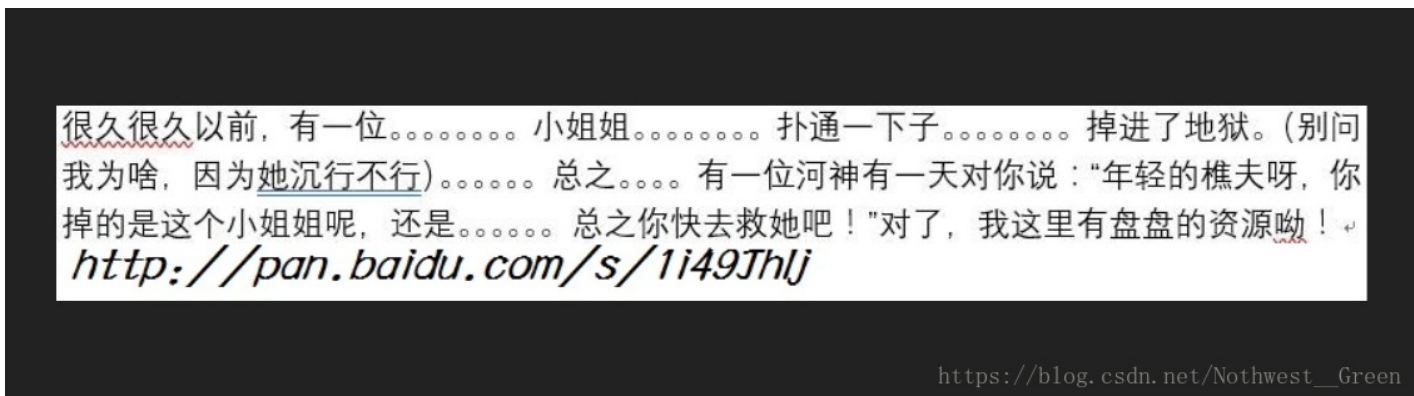
图片无法正常显示。



丢进winhex看看, 少了jpg文件头, 我们将jpg文件头FF D8 FF E0 插入。

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	yøÿà	JFIF
00000016	00	60	00	00	FF	E1	00	22	45	78	69	66	00	00	4D	4D	`	ÿá "Exif MM
00000032	00	2A	00	00	00	08	00	01	01	12	00	03	00	00	00	01	*	
00000048	00	01	00	00	00	00	00	00	FF	DB	00	43	00	02	01	01		ÿÛ C
00000064	02	01	01	02	02	02	02	02	02	02	02	03	05	03	03	03		
00000080	03	03	06	04	04	03	05	07	06	07	07	07	06	07	07	08		
00000096	09	0B	09	08	08	0A	08	07	07	0A	0D	0A	0A	0B	0C	0C		
00000112	0C	0C	07	09	0E	0F	0D	0C	0E	0B	0C	0C	0C	FF	DB	00		ÿÛ
00000128	43	01	02	02	02	03	03	03	06	03	03	06	0C	08	07	08	C	
00000144	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C		

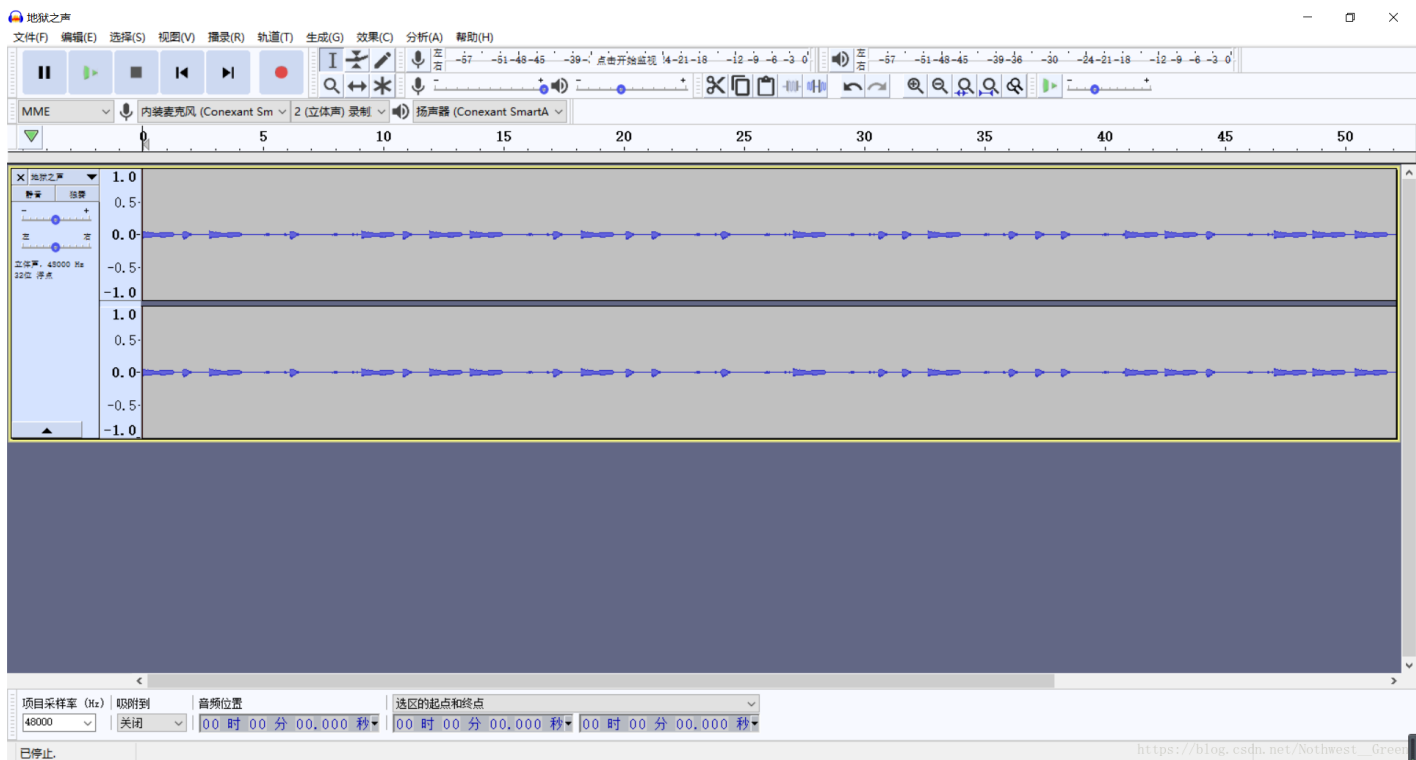
保存后即可正常打开图片。



有一个百度网盘的链接，<https://pan.baidu.com/s/1i49Jhlj>，打开，是一个音频文件。

地狱之声.wav

下载，用Audacity打开。



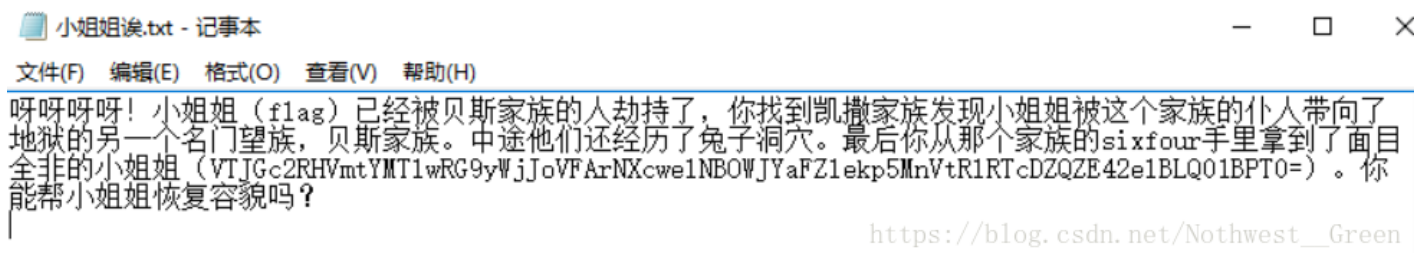
不出意外，是摩斯电码没跑了。



使用binwalk分离文件，有一个隐藏的加密zip压缩包。

解压密码猜测：Password

打开txt文件



仔细阅读文字，发现加密方式依次为

base64 -> rabbit -> caesar

得到base64加密过的字符串

```
VTJGc2RHVmtYMTlwRG9yWjJoVFArNXcwe1NBOWJYaFZ1ekp5MnVtR1RTcDZQZE42e1BLQ01BPT0=
```

base64解密

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

rabbit解密

```
fxbqrwrwnwmngrjxsmsrnhx
```

caesar解密，得到所有结果

kcgvwbwasbrslwocxwsxwsmc  
ldhwxcxbtcstmxpdyxyxtnd  
meixydycudtunyqezyuzyuoe  
nfjyzedvEUvoZrfazvazvpf  
ogkzafaewfvwpasgbawbawqg  
phlabgbfxgwxqbthcbxcbxrh  
qimbchcgYhxyrcuidcydcysi  
rjncdidhziyzsdvjedzedztj  
skodejeiajzatewkfeafeauk  
tlpefkfjBkabufxlgfbgfbvl  
umqfglgkclbcvgymhgchgcwm  
vnrghmhlDmcdwhznihdihdxn  
woshinimendexiaoJiejieyo  
xptijojnfoefyjbpkjfkjfpz  
yqujpkkogpfgzkcqlkglkgaq  
zrvklqlphqghaldrmlhmlhbr  
aswlmrmqirhibmesnminmics  
btxmnsnrjsijcnftonjonjdt  
cuynotosktjKdogupokpokeu  
dvzopuptluklephvqplqplfv  
ewapqvqumvlmfqiwrqmrqmgw  
fxbqrwrvnwmngrjxsrnsrnhx  
gycrsxswoxnohskytsotsoiy  
hdstytxpyopitlzutputpjz  
iaetuzuyqzpqjumavuquvqka  
jbfuvavzraqrkvnbwvrwvrlb

发现有一条密文是拼音，Bingo~

CTF{woshinimendexiaoJiejieyo}