

隐写术

原创

obsetear 于 2019-07-28 16:41:01 发布 104 收藏

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。

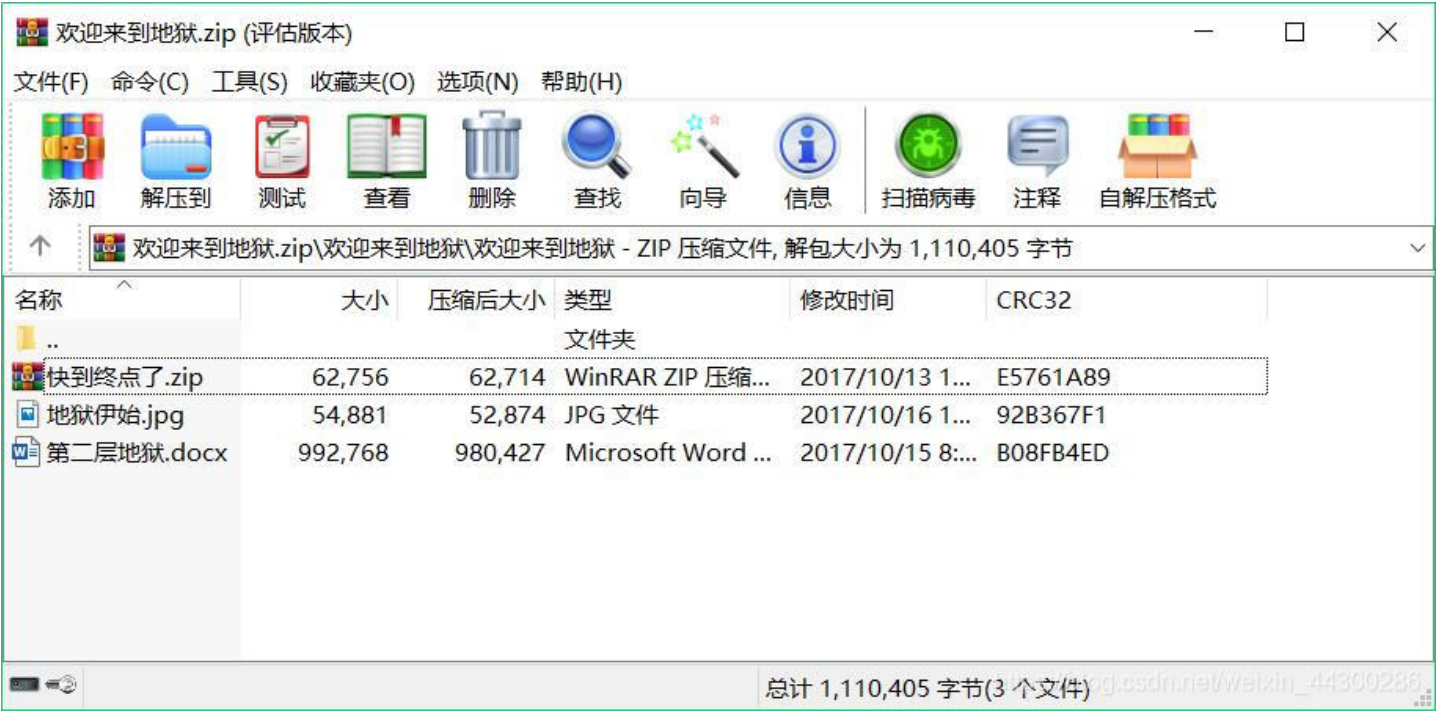
本文链接：https://blog.csdn.net/weixin_44300286/article/details/97614334

版权

隐写

题目来源：实验吧

题目描述：欢迎来到地狱



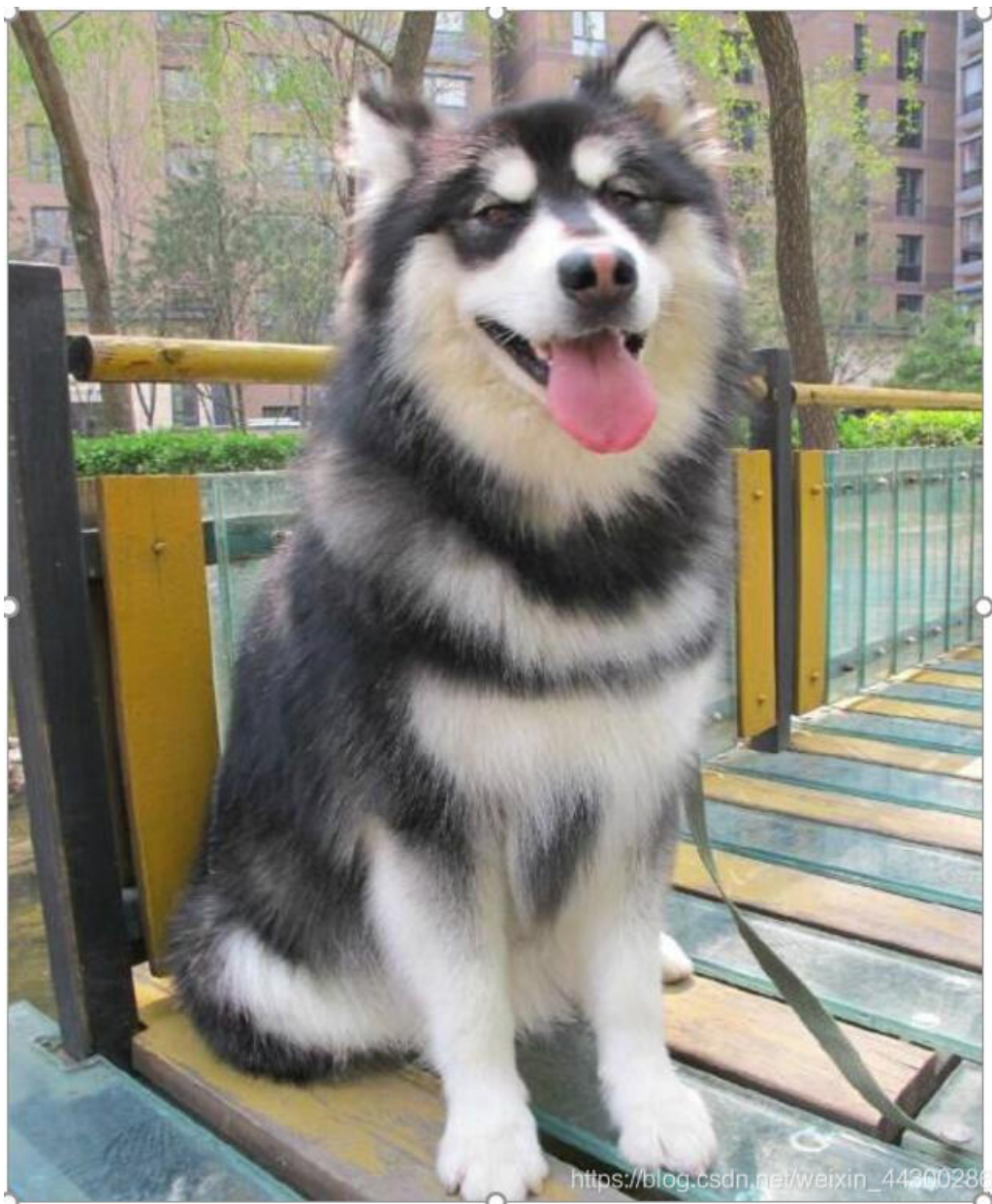
打开压缩包我们发现里面还有一个压缩包，一个jpg图片和一个docx文件，除了jpg图片以外其他的都需要密码才能打开，而jpg图片打开后却是

地狱伊始.jpg
似乎不支持此文件格式。

用winhex打开发现有FFD9文件尾却没有FFD8文件头

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	10	4A	46	49	46	00	01	01	01	00	60	00	60	00	00
FF	E1	00	22	45	78	69	66	00	00	4D	4D	00	2A	00	00
00	08	00	01	01	12	00	03	00	00	00	01	00	01	00	00
00	00	00	00	FF	DD	00	42	00	00	01	01	00	01	01	00

然后拿着这串key去打开docx文件，发现要转换成小写并只输入key后的内容才行。
然后我们就可以看到一只凶猛的。。。哈士奇？



哈士奇什么的不重要，重要的是后面那串文字中有提示

image steganography, , , 是不是掉在

图片隐写术，然后用在线工具解密

解密网站：<http://www.atool9.com/steganography.php>

ATOOL 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

1. 从电脑中选择一张带有隐藏信息的图片： 哈士奇.png

2. 输入需要解开信息的密码（如果没有密码可以不填）：

解密出隐藏的信息

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

https://blog.csdn.net/weixin_44300286

又获得一串钥匙，不用说，这肯定是那个压缩包的密码



然后打开压缩包，发现里面有一个jpg图片和一个txt文件，对图片binwalk一下，发现里面有一个zip压缩包

```
Windows PowerShell
PS C:\Users\12840\Desktop> binwalk 地狱大门.jpg
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
62584       0xF478       End of Zip archive, footer length: 22

PS C:\Users\12840\Desktop>
```

https://blog.csdn.net/weixin_44300286

然后我们既可以用foremost进行分离，也可以用winhex进行分离

```
Windows PowerShell
PS C:\Users\12840\Desktop> foremost 地狱大门.jpg
```

```
4A 00 7B 29 63 CC 84 FB 9A 2A 2D CE 79 08 3F 3A
29 01 FF D9 50 4B 03 04 14 00 01 08 08 00 15 95
4D 4B 55 82 E6 3E 34 01 00 00 39 01 00 00 10 00
00 00 E5 B0 8F E5 A7 90 E5 A7 90 E8 AF B6 2E 74
78 74 CF 80 FC E5 B3 00 DA 7F 5E 58 4F 45 B0 C5
0C 98 53 2E 99 28 57 15 4D 2E CE C4 1B D9 1B 8D
45 03 FF B2 7F F6 72 99 D2 6B DB 7E 42 CE B3 0C
F2 43 21 E3 72 02 11 29 23 CB D1 77 7B 1B 3A 8E
53 0B 93 6C 89 F6 A1 26 D8 30 D1 03 E9 71 85 B0
4B 6E 83 1E EC BF A9 8D 9D 97 9F 24 6C 2F 9B 51
5E E2 A8 97 C8 5E 29 BB 32 24 68 C7 A8 0A 68 AC
52 25 11 43 AA A6 41 F2 17 E3 E7 E9 2F 90 39 2A
```

C6	B2	44	70	F3	48	D2	59	F4	7C	1D	7C	D0	D3	04	19
10	43	74	11	FE	E9	A9	07	14	80	78	C6	5F	1B	97	25
F2	22	BC	82	6B	47	41	A0	C9	C1	FC	B6	A7	7C	F8	A0
67	B6	4B	40	1C	B3	67	68	85	4C	CF	24	FA	F9	C9	15
9E	BD	0B	E2	40	0B	AE	A3	A1	C8	A5	F0	B5	02	71	87
40	F0	99	7E	4E	1D	94	42	0B	CC	70	C8	06	23	57	21
16	08	D3	A6	2B	FC	DA	2B	69	1C	80	85	70	F4	3E	00
43	7F	81	E8	D5	94	81	82	98	C5	A9	74	6D	4D	77	08
0C	63	D1	B8	34	BE	6E	DA	2C	2C	4C	2A	0D	A0	3E	CC
21	B8	3B	26	35	18	74	54	02	7B	B1	67	20	70	11	8B
82	57	D8	BF	1D	5D	20	8D	71	64	78	A7	E5	40	CC	DF
07	AF	32	02	93	F4	50	4B	01	02	3F	00	14	00	01	08
08	00	15	95	4D	4B	55	82	E6	3E	34	01	00	00	39	01
00	00	10	00	24	00	00	00	00	00	00	00	20	00	00	00
00	00	00	00	E5	B0	8F	E5	A7	90	E5	A7	90	E8	AF	B6
2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00
77	BD	C4	B6	0F	44	D3	01	6A	B5	C0	75	0E	44	D3	01
6A	B5	C0	75	0E	44	D3	01	50	4B	05	06	00	00	00	00
01	00	01	00	62	00	00	00	62	01	00	00	00	00	00	00

分离后发现zip果然是被加密了的，我们这不是还有一个txt文件没有用嘛，打开txt文件，发现里面有提示

最后一层地狱.txt - 记事本

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

这里有一个大门，勇士把它轰开吧。

(tips:

011100100111010101101111011010110110111101110101011011011110111010101101100011010010110111001100111)

文字描述的很明显，就是关于这个大门的提示，然后用python脚本跑一下这一串二进制字符。

python脚本如下：

```

flag='01110010011101010110111101101011011011110111010101101100011010010110111001100111'
ans = ''
length = len(flag)//8
for i in range(length):
    ans += chr(int(flag[i*8: (i+1)*8], 2))

print(ans)

```

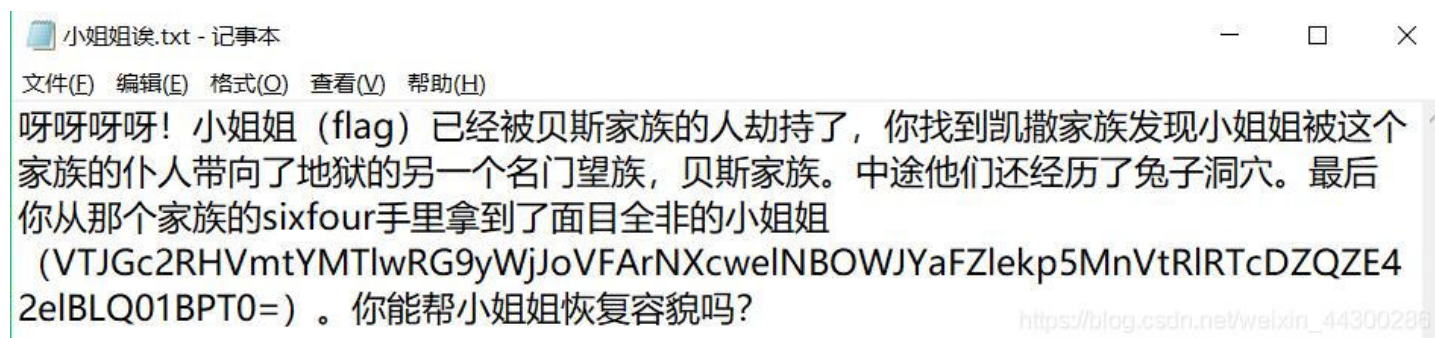

运行结果:

```
Python 3.7.3 Shell
File Edit Shell Debug Options Window Help
Python 3.7.3 (v3.7.3:ef4ec6ed12, Mar 25 2019, 22:22:05) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\12840\Desktop\二进制转字符串.py =====
>>> ruokouling
>>>
```

我一开始还以为这就是压缩包的密码，后来仔细看才发现它提示的是压缩包的密码是“弱口令”，然后我们再用破解压缩包密码的软件Ziperello进行字典破解，最后得到密码



终于剩下最后一个txt文件了，本来我还以为打开最后一个txt文件就结束了的，没想到里面还有文章



仔细读一下文字，发现加密过程应该是这样，先用凯撒加密，然后再用rabbit加密，最后是base64加密，因此最后我们看到的是base64加密的字符。所以解密过程应该是先base64，再rabbit，最后是凯撒。

最后用在线解密工具解就行了。

VTJGc2RHVmtYMTlwRG9yWjJoVFArNXcwe1NBOWJYaFZlekp5MnVtRlRTcDZQZE42e1BLQ01BPT0=

加密

解密

☐ 解密结果以16进制显示

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

https://blog.csdn.net/weixin_44300286

fxbqrwrwnwmngrjxsrsrnhx

在此输入密钥

密码是可选项，也就是可以不填。

< 解密

加密 >

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

https://blog.csdn.net/weixin_44300286

fxbqrwrwnwmngrjxsrsrnhx

位移

加密

解密

woshinimendexiaojiejieyo

https://blog.csdn.net/weixin_44300286

凯撒解密一般都不会告诉你偏移量，所以得一个一个去试，反正也不多就26个数。

总结：这次做题收获最大的就是又收集到了一波工具，这道题虽然套路深，但每个提示都很明显，都能看得懂，就是缺少工具的话解起来就麻烦些，比如最后破解压缩包密码，在我没有那个软件的时候，用暴力破解的软件破解了几十分钟，好像最后还没爆出来，但我用那个软件的时候，还不到一秒就破解出来了。看来还是自己太菜，以后还得多多做题。