

实验吧CTF题库-隐写术(部分)

转载

[andiao1218](#) 于 2017-11-17 23:00:00 发布 936 收藏 4

原文链接: <http://www.cnblogs.com/sch01ar/p/7854106.html>

版权

• Spamcarver

Spamcarver 分值: 30

来源: PicoCTF 2013

难度: 难

参与人数: 958人

Get Flag: 228人

答题人数: 256人

解题通过率: 89%

开盖有惊喜

格式: flag{xxx}

解题链接: <http://ctf5.shiyanbar.com/stega/spamcarver/spamcarver.jpg> **通过**

提交

用kali下载图片

```
root@sch01ar:~# wget http://ctf5.shiyanbar.com/stega/spamcarver/spamcarver.jpg
```

用binwalk查看是否有隐藏的文件

```
root@sch01ar:~# binwalk /root/spamcarver.jpg
```

```
root@sch01ar:~# binwalk /root/spamcarver.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
64001       0xFA01      End of Zip archive
```

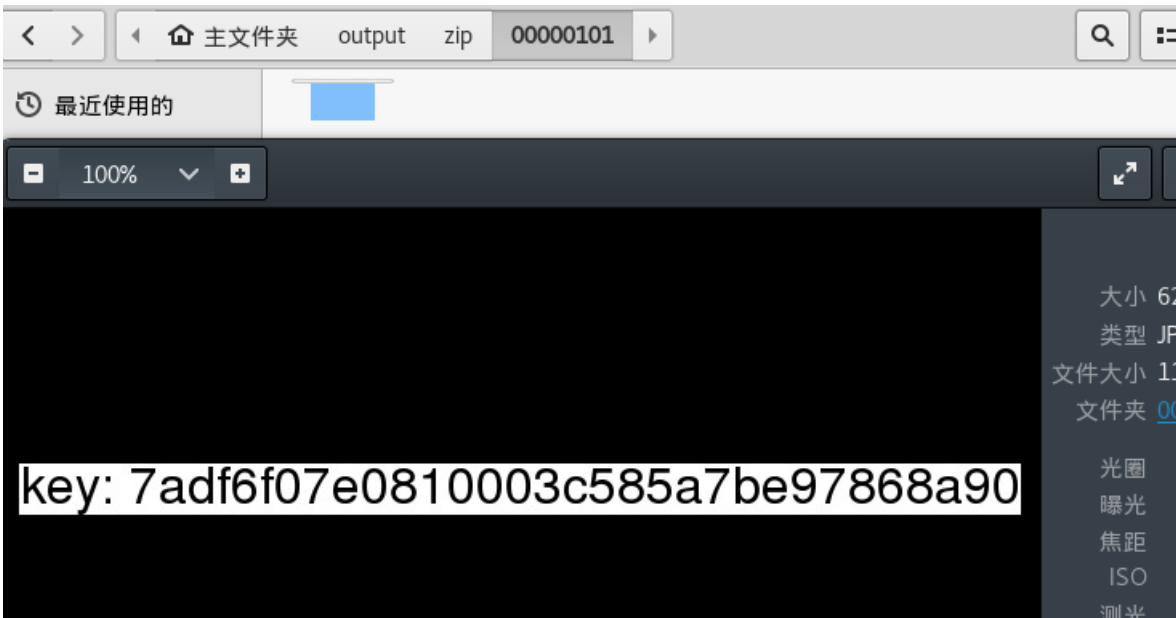
隐藏着一个zip文件

用foremost分离出文件

```
root@sch01ar:~# foremost /root/spamcarver.jpg
```

```
root@sch01ar:~# foremost /root/spamcarver.jpg
Processing: /root/spamcarver.jpg
|foundat=      UT
*|
```

在/root/output/的目录下, 得到flag



缝缝补补又三年:

NAVSAT 分值: 10

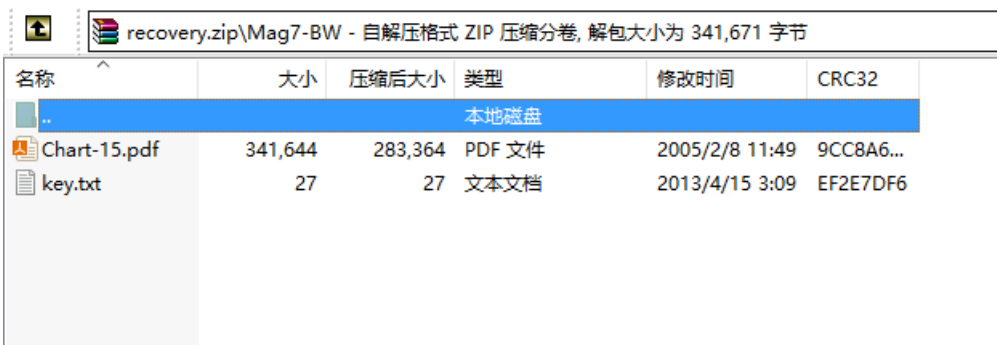
来源: PicoCTF 2013 难度: 易 参与人数: 562人 Get Flag: 233人 答题人数: 247人 解题通过率: 94%

缝缝补补又三年
格式: flag{xxx}

解题链接: <http://ctf5.shiyanbar.com/stega/navsat/recovery.zip> 通过

提交

下载zip文件, 打开



key.txt文件打不开, flag应该就在里面

用c32打开文件, flag直接显示出来

```

00000000: 3F 3F 03 04 0A 00 00 00 00 00 22 79 8E 42 F6 7D |??....."y蕉結
00000010: 2E EF 1B 00 00 00 1B 00 00 00 0F 00 1C 00 4D 61 |.?......Ma
00000020: 67 37 2D 42 57 2F 6B 65 79 2E 74 78 74 55 54 09 |g7-BW/key.txtUT.
00000030: 00 03 00 FE 6A 51 0B FF 6A 51 75 78 0B 00 01 04 |.??..Key: Ne
00000040: E8 03 00 00 04 E8 03 00 00 4B 65 79 3A 20 4E 65 |xt stop Tau Erid
00000050: 78 74 20 73 74 6F 70 20 54 61 75 20 45 72 69 64 |ani.PK.....'?
00000060: 61 6E 69 0A 50 4B 03 04 14 00 00 00 08 00 27 B6 |G2.θ濱R..?....
00000070: 47 32 1B A6 C8 9C E4 52 04 00 8C 36 05 00 14 00 |..Mag7-BW/Chart-
00000080: 1C 00 4D 61 67 37 2D 42 57 2F 43 68 61 72 74 2D |15.pdfUT...?.B?
00000090: 31 35 2E 70 64 66 55 54 09 00 03 8A 36 08 42 AF |泌Qux....?...?
000000A0: FE 6A 51 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 |..厓c?Q?Z耗部?
000000B0: 00 00 8C B7 63 94 25 51 D3 26 5A B6 6D DB B6 BA |1部mt棲國部m部限
000000C0: 6C DB B6 6D 74 97 AB BA 6C DB B6 6D DB B6 ED AA |Su 錠來 賦U s
000000D0: 53 75 FB FD E6 9B B9 73 D7 FC B8 B3 56 AE CC 73 |"wD軟瀟屬鑄@紬.
000000E0: 22 77 44 EC 78 9E 88 8C D8 E4 8A A2 E2 F4 CC 0C |,01DL.浦D||θ心f
000000F0: 2C 30 6C 44 4C 44 0E C6 D6 44 7C 7C 30 8C B2 66 |?雷D?D?虹U謹f
00000100: F6 16 AE 96 44 EC FF 44 CA 30 8C E2 56 B6 AE 66 |蛔虹禱用 &. θ.
00000110: CE 44 8C E2 B6 46 AE 66 A2 66 26 0E A6 66 30 02 |.θ. fFvθ?贏r.K
00000120: 02 30 2E AE CE 66 46 76 30 9E 1B C5 49 72 0E 4B |LH<?ogx,顯脏{?
00000130: 4C 48 A1 DC A7 1A 6F 67 78 2C 9E B6 B1 82 7B AA |Tx4\h?x隄2.?'
00000140: 54 78 34 5C 68 C7 10 78 EA 9D 32 1E E4 19 AE AD |鋼?9?弗14E4?觀
00000150: E5 48 3F 39 E3 12 B8 A5 31 34 45 34 CA 28 D3 5D |?嶸?.俚嶸$ 邗?
00000160: FE 27 CF 6F A0 21 07 90 E0 DC 75 24 20 DA F5 DD

```

也可以把开头的两个??修改成PK，然后就能打开key.txt

```

00000000: 50 4B 03 04 0A 00 00 00 00 00 22 79 8E 42 F6 7D |PK|....."yBö}
00000010: 2E EF 1B 00 00 00 1B 00 00 00 0F 00 1C 00 4D 61 |.?......Ma
00000020: 67 37 2D 42 57 2F 6B 65 79 2E 74 78 74 55 54 09 |g7-BW/key.txtUT

```

```

key.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Key: Next stop Tau Eridani

```

In Hex, No One Can Hear You Complain:

In Hex, No One Can Hear You Complain 分值 : 10

来源 : PicoCTF 2013 难度 : 易 参与人数 : 488人 Get Flag : 294人 答题人数 : 301人 解题通过率 : 98%

修改试试看?
格式:flag{xxx}

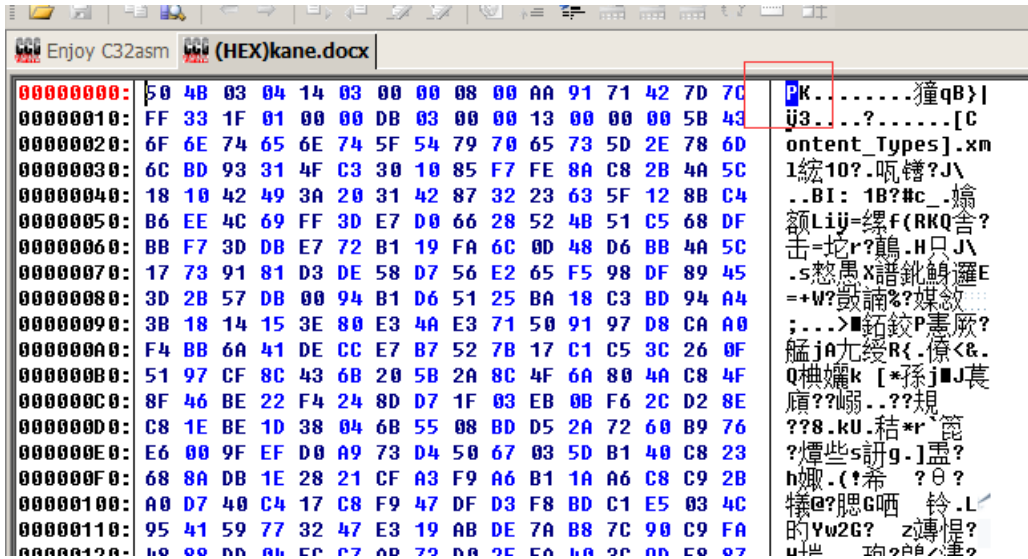
解题链接 : <http://ctf5.shiyanbar.com/stega/in-hex/kane.docx> **通过**

提交

下载docx文件，直接打开，打不开

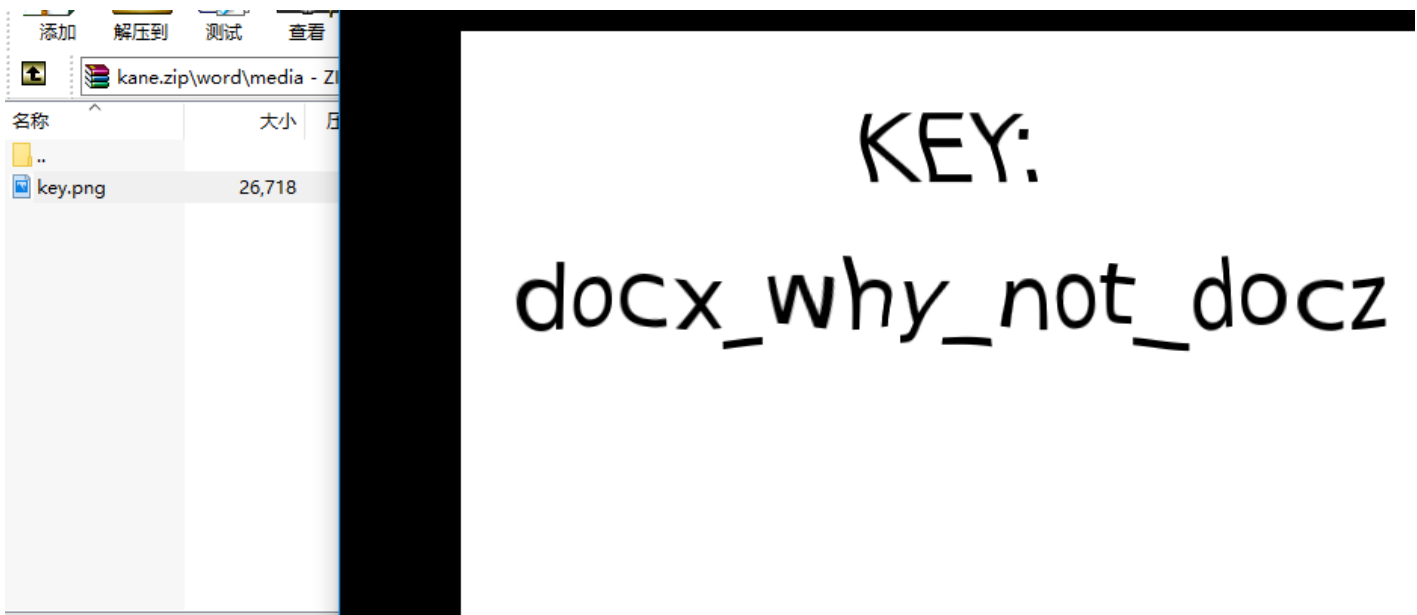
Microsoft Office Word ? X
 无法打开 Office Open XML 文件 kane.docx，因为内容有错误。

用c32打开



是个压缩文件，改个zip后缀打开

找到flag



越光宝盒:

corrupt png

解题链接：<http://ctf5.shiyanbar.com/stega/corrupt/timgK.png> 通过

提交

下载图片

图片打不开



用c32打开，发现png头不对

```

Enjoy C32asm (HEX)timgK.png
00000000: 90 47 4E 47 0E 1A 0A 1A 00 00 00 0D 49 48 44 52 PNG.....IHDR
00000010: 00 00 01 00 00 00 01 2C 08 02 00 00 00 09 91 FE ...?.....
00000020: 85 00 00 00 09 70 48 59 73 00 00 0B 13 00 00 0B ?...pHYs.....
00000030: 13 01 00 9A 9C 18 00 00 00 20 63 48 52 4D 00 00 ...殫....cHRM..
00000040: 7A 25 00 00 80 83 00 00 F9 FF 00 00 80 E9 00 00 z%..?..?..?..
00000050: 75 30 00 00 EA 60 00 00 3A 98 00 00 17 6F 92 5F u0..闌...?.o拍
00000060: C5 46 00 01 20 3F 49 44 41 54 78 DA EC FD 69 8C 臙.. ?IDATx陟齠?
00000070: 5C 59 76 26 08 9E 8B 0C D5 76 33 DF DD E9 4E D2 \Vv&.兂類u3咄致?
00000080: C9 E0 12 64 EC 91 91 A9 54 6E 92 52 29 69 32 55 舌.d輪懇Tn捻)i2U
00000090: 92 5A B5 09 55 25 34 66 A9 5F 8D 41 0F 30 03 0C 抗?U%4f 屹.0..
000000A0: 06 98 6E 60 A6 67 06 E8 59 7A 06 EA FA 31 5D 98 .棍\ .鎡z.掄1]?
000000B0: 00 00 77 FF 00 00 00 00 01 F2 60 60 0E 00 00 00

```

把90 47 4E 47 0E 1A 0A 1A修改成89 50 4E 0D 0A 1A 0A

```

Enjoy C32asm (HEX)timgK.png
00000000: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG...IHD
00000010: 00 00 01 00 00 00 01 2C 08 02 00 00 00 09 91 FE ...?.....
00000020: 85 00 00 00 09 70 48 59 73 00 00 0B 13 00 00 0B ?...pHYs.....
00000030: 13 01 00 9A 9C 18 00 00 00 20 63 48 52 4D 00 00 ...殫....cHRM..
00000040: 7A 25 00 00 80 83 00 00 F9 FF 00 00 80 E9 00 00 z%..?..?..?..
00000050: 75 30 00 00 EA 60 00 00 3A 98 00 00 17 6F 92 5F u0..闌...?.o拍
00000060: C5 46 00 01 20 3F 49 44 41 54 78 DA EC FD 69 8C 臙.. ?IDATx陟齠?

```

保存，打开图片，得到flag



Dark Star:

Dark Star 分值 : 20

来源 : [PicoCTF 2013](#)

难度 : 中

参与人数 : 983人

Get Flag : 334人

答题人数 : 361人

解题通过率 : 93%

Sure are a lot of stars out there... but there's a lot of empty space for things to hide in, too.

解题链接 : <http://ctf5.shiyanbar.com/stega/dark-star/darkstar.img> **通过**

提交

下载文件

用binwalk查看，里面有很多的image文件

```
root@sch01ar:~# binwalk /root/darkstar.img
```



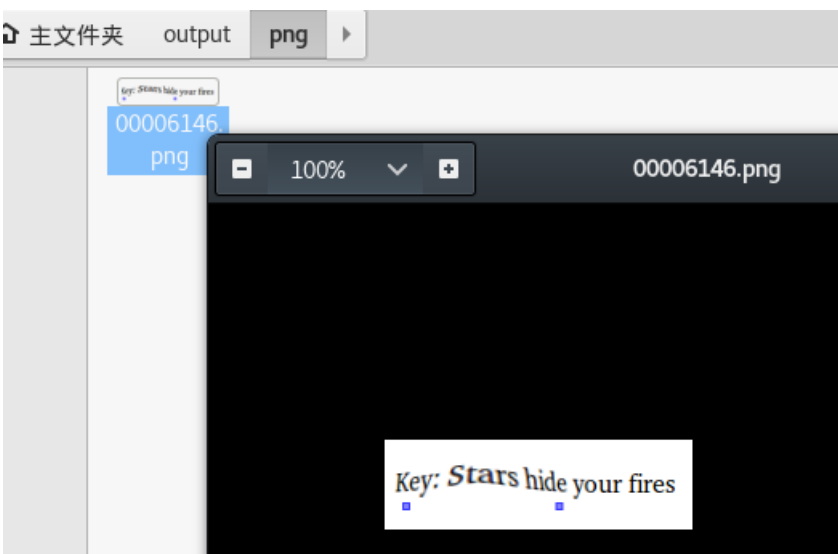
```
root@sch01ar:~# binwalk /root/darkstar.img
```

DECIMAL	HEXADECIMAL	DESCRIPTION
3146752	0x300400	PNG image, 192 x 56, 8-bit/color RGBA, non-interlaced
3146809	0x300439	Zlib compressed data, default compression
4719616	0x480400	JPEG image data, JFIF standard 1.01
4721664	0x480C00	JPEG image data, JFIF standard 1.01
4729856	0x482C00	JPEG image data, JFIF standard 1.01
4730238	0x482D7E	Copyright string: "Copyright (c) 1998 Hewlett-Packard
4738048	0x484C00	JPEG image data, JFIF standard 1.01
4738346	0x484D2A	Copyright string: "Copyright 1999 Adobe Systems Incomp
4740040	0x4853C8	JPEG image data, JFIF standard 1.02
4743332	0x4860A4	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rd obe.com/tiff/1.0/" xmlns:exif="htt
4754432	0x488C00	JPEG image data, JFIF standard 1.01
4754814	0x488D7E	Copyright string: "Copyright (c) 1998 Hewlett-Packard
4762624	0x48AC00	JPEG image data, JFIF standard 1.01
4764672	0x48B400	JPEG image data, JFIF standard 1.01
4768768	0x48C400	JPEG image data, JFIF standard 1.01
4771840	0x48D000	JPEG image data, JFIF standard 1.01
4772138	0x48D12A	Copyright string: "Copyright 1999 Adobe Systems Incomp
4773924	0x48D824	JPEG image data, JFIF standard 1.02
4793236	0x492394	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#' xml
4794731	0x49296B	Unix path: /ns.adobe.com/xap/1.0/sType/ResourceRef#'
4794794	0x4929AA	Unix path: /ns.adobe.com/xap/1.0/mm/'>
4795282	0x492B92	Unix path: /purl.org/dc/elements/1.1/'>
4803584	0x494C00	JPEG image data, JFIF standard 1.01
4809728	0x496400	JPEG image data, JFIF standard 1.01

用foremost分离文件

```
root@sch01ar:~# foremost /root/darkstar.img
```

分离出一个png图片，打开，得到flag



Chromatophoria:

Chromatophoria 分值 : 20

来源 : PicoCTF 2013

难度 : 中

参与人数 : 672人

Get Flag : 281人

答题人数 : 300人

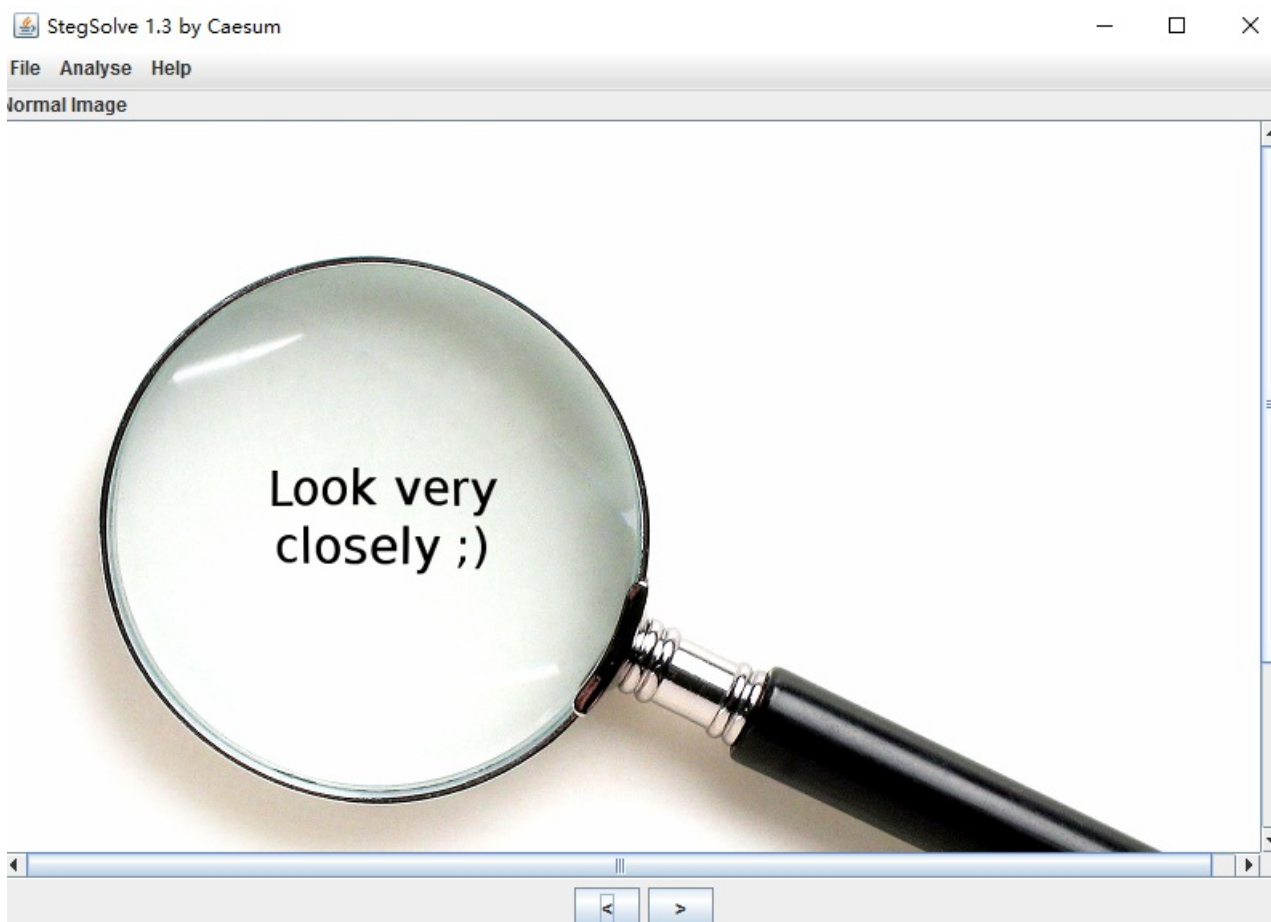
解题通过率 : 94%

While refueling at a gas giant, you are hailed by a race of cuttlefish-people who dwell within it. Their transmission is entirely visual; you suspect that they may be communicating through the color values.

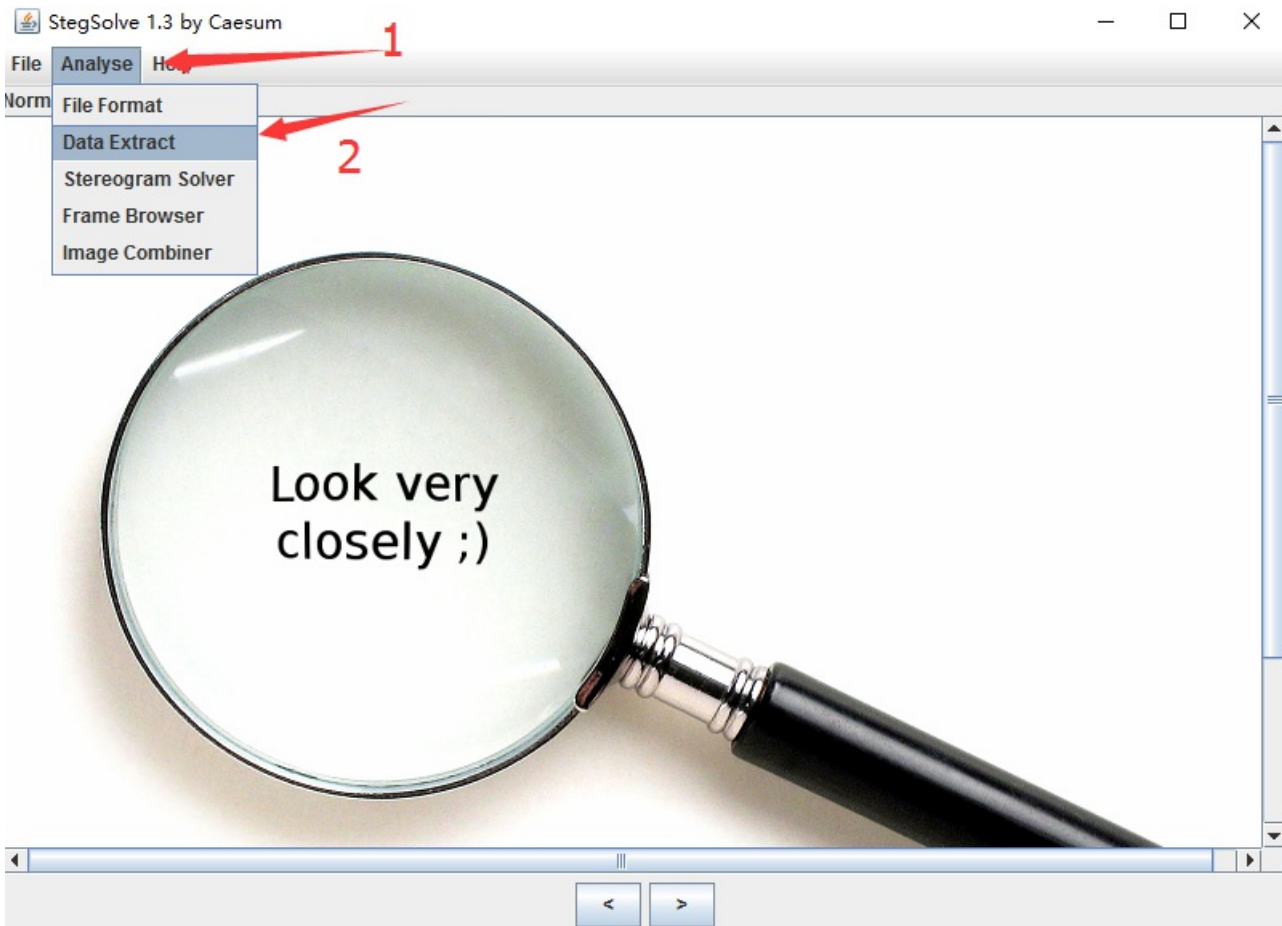
解题链接 : <http://ctf5.shiyandar.com/stega/chromatophoria/steg.png> **通过**

提交

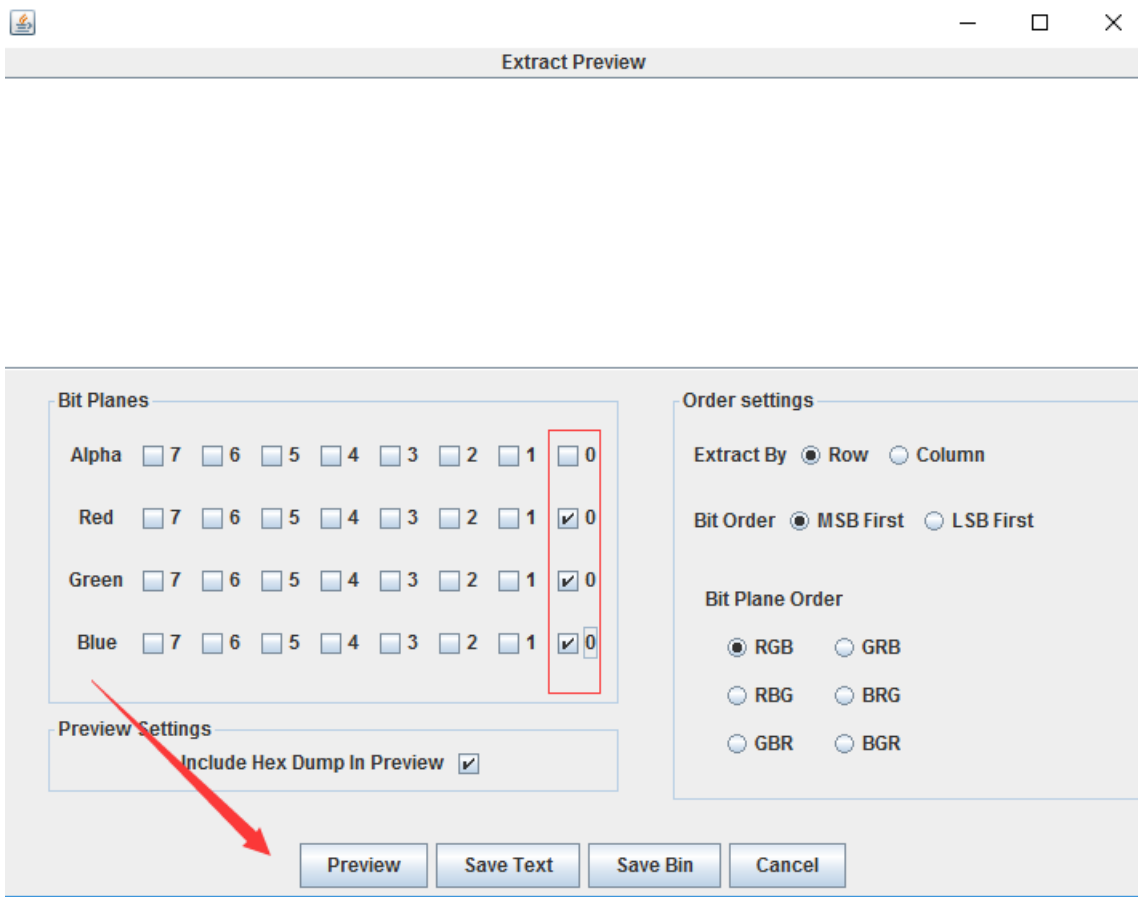
下载图片，用Stegsolve打开



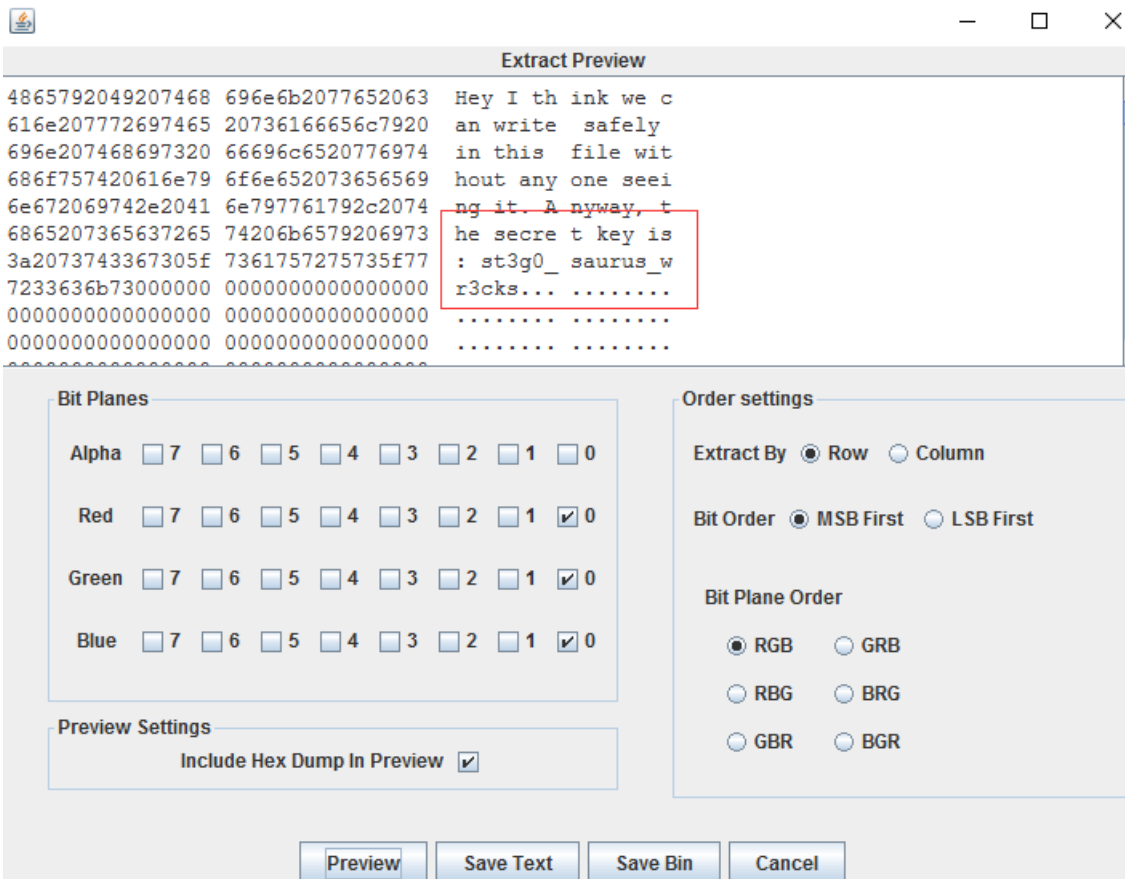
然后选择



勾起这三个勾，然后点击Preview



发现flag



九连环：

先看一下是否有隐藏的文件

```

[root@sch01ar]~# 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, compre
ssed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657       0xBE11      End of Zip archive
48962       0xBF42      End of Zip archive

```

图片里隐藏有zip文件

分离出来

```

[root@sch01ar]~# foremost 123456cry.jpg
Processing: 123456cry.jpg
|foundat=asd/PK
foundat=asd/good-已合并.jpg
rf0LI*!@T@R@M@000[00LQI00B0>0"Kvf\}02nf0000}00{00}0000000300u_0u00q00u0001000 Z
0X0XX@ 0p/01:000000N00000h r000000000da0dat0 0q0000
foundat=asd/qwe.zipPK
*|

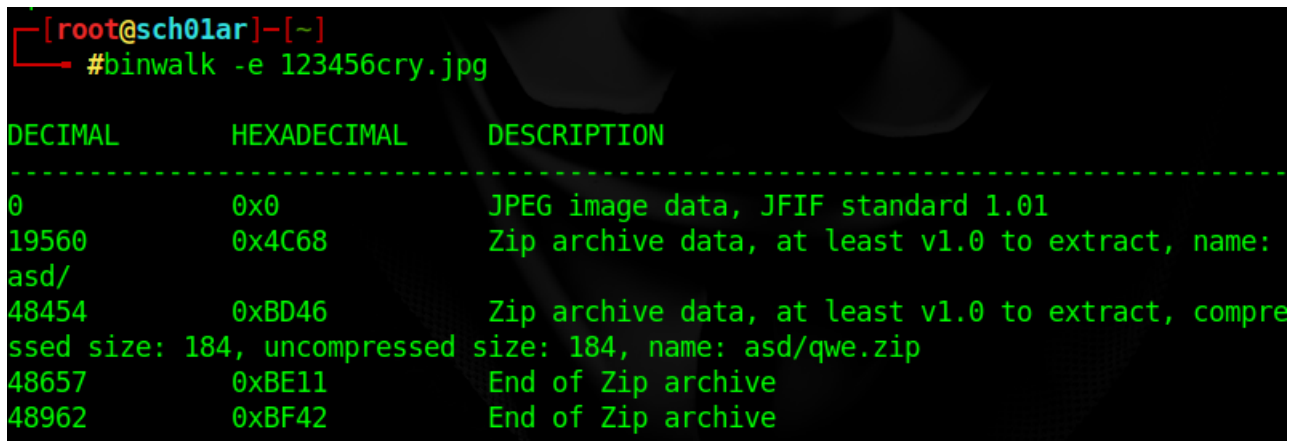
```

分离出的zip文件里有一个图片和一个压缩包，都需要密码

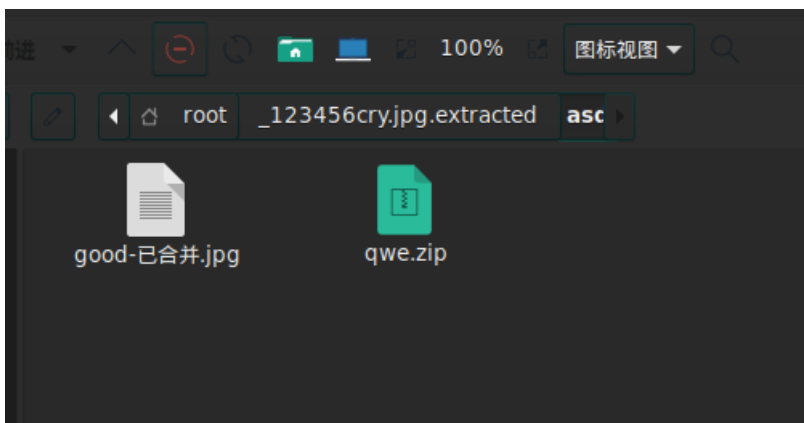


使用binwalk直接分离图片和压缩文件

```
[root@sch01ar]-[~]
└─ #binwalk -e 123456cry.jpg
```



图片被直接分离出来



• FIVE1

题目提示

FIVE1 分值：10

来源：倾心

难度：易

参与人数：273人

Get Flag：77人

答题人数：92人

解题通过率：84%

图片内藏有5位数密码，你能找出来吗？

flag格式：flag{xxx}

解题链接：<http://ctf5.shiyanbar.com/stega/FIVE1/1111110000000000.jpg>

提交

图片内有五位数密码

图片：



下载图片

```
[root@sch01ar]~# wget http://ctf5.shiyanbar.com/stega/FIVE1/1111110000000000.jpg
```

下载完图片后查看图片是否有隐藏的文件

```
[root@sch01ar]~# binwalk 1111110000000000.jpg
```

```
[root@sch01ar]~# binwalk 1111110000000000.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
7395	0x1CE3	Zip archive data, encrypted at least v2.0 to extract, compressed size: 32506, uncompressed size: 45602, name: hacker.jpeg
40051	0x9C73	End of Zip archive

有一个zip的隐藏文件，zip里有一个hacker.jpeg的图片

foremost分离jpg图片和zip压缩包

```
[root@sch01ar]~# foremost 1111110000000000.jpg
```

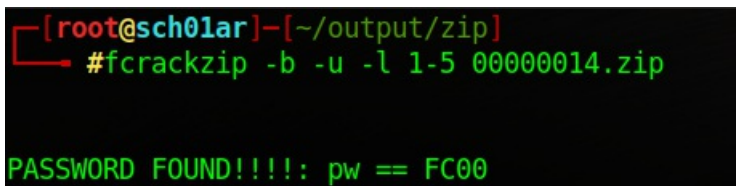
但是zip文件有密码



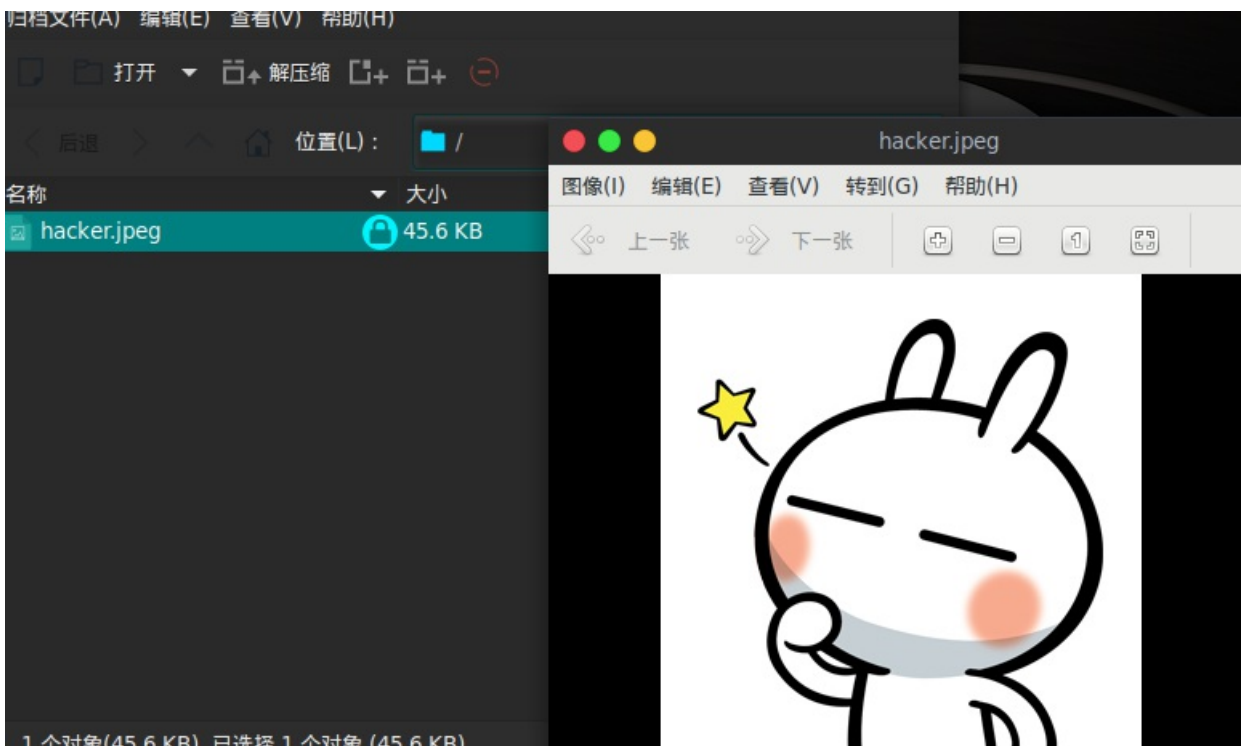
fcrackzip爆破一下密码

```
[root@sch01ar]--[~/output/zip]
└─ #fcrackzip -b -u -l 1-5 00000014.zip
```

得到密码，FC00



打开hacker.jpeg又是一张图片



用c32打开，拉到最后，看到一句话

echo
"LS0uLi4gIC4tICAuLi4uLiAgLS0uLi4gIC4tICAuLi4uLiAgLi0gIC0tLi4uICAuLi4uLSAgLi4uLS0gIC0tLS4uICAtLS0tLiAgLi4uLi0gIC4tICAtLS0tLSAgLiAg" >1.txt

对echo后的语句进行base64解码

解出了一串摩斯密码

----- .- --.... .-- ----.- .- ----- .

解密

英文字母：
7A57A5A743894A0E

转换为摩斯电码 清除 生成摩斯代码的分隔方式：空格分隔 单斜杠/分隔

摩斯电码：（格式要求：可用空格或单斜杠/来分隔摩斯电码，但只可用一种，不可混用）

----- .- --.... .-- ----.- .- ----- .

转换为英文字母

转换为英文字母成功！

结果为：7A57A5A743894A0E

拿去进制转换得不出什么有用的东西

拿去md5解密，得到admin，admin就是flag

密文: 7A57A5A743894A0E
类型: 自动 [帮助]

查询 加密

查询结果：
admin

[添加备注]

• 欢迎来到地狱

欢迎来到地狱.zip里有三个文件

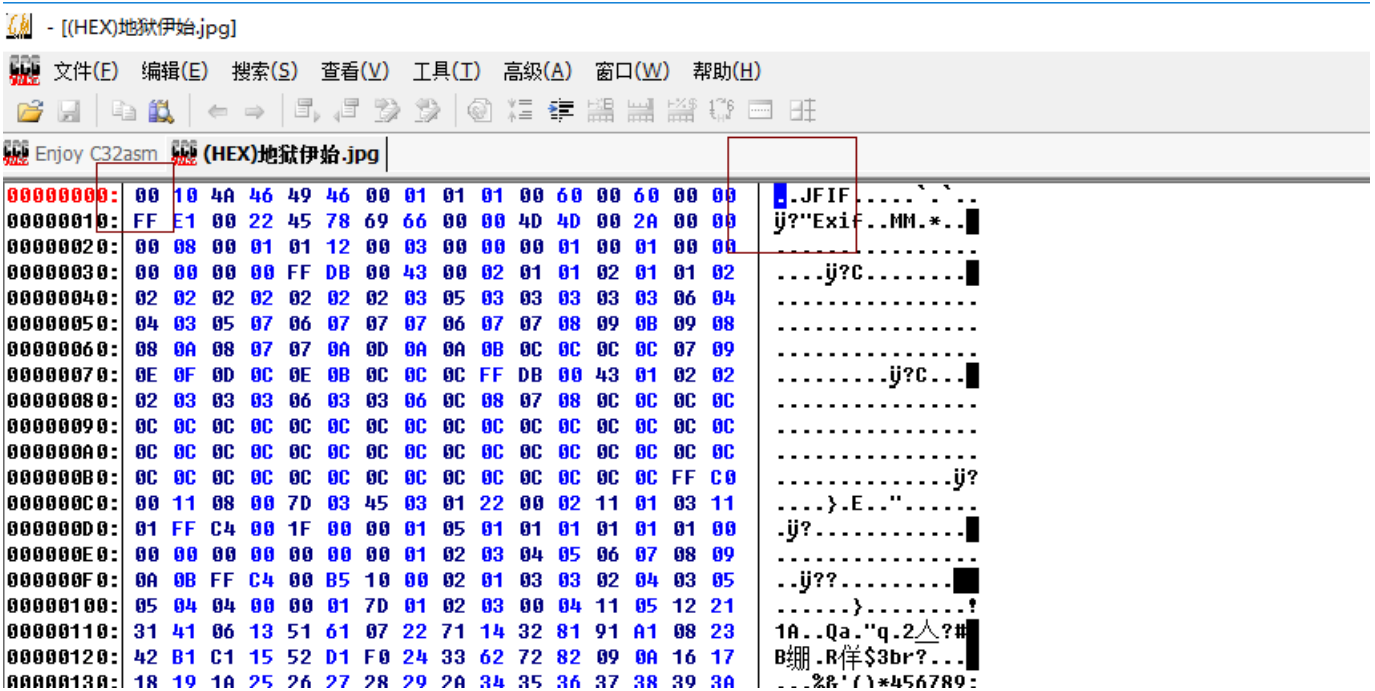


从地狱伊始.jpg开始

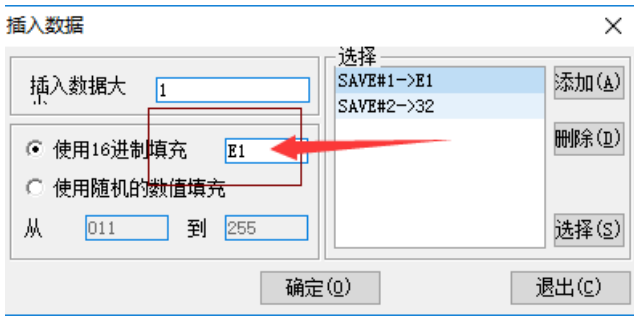
图片无法正常显示



用c32打开，看看文件头是否是正常的



文件头前少了FF D8 FF E1，添加上去，编辑->插入数据

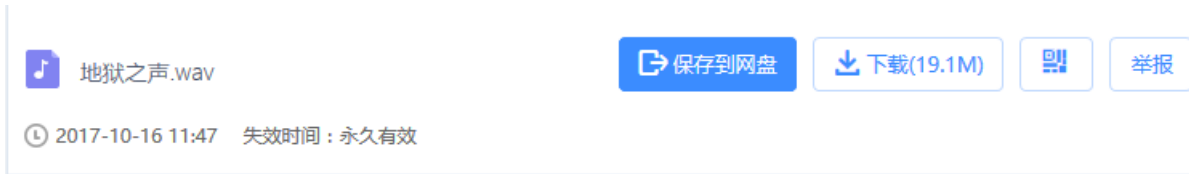


在此处依次添加E1, FF, D8, FF

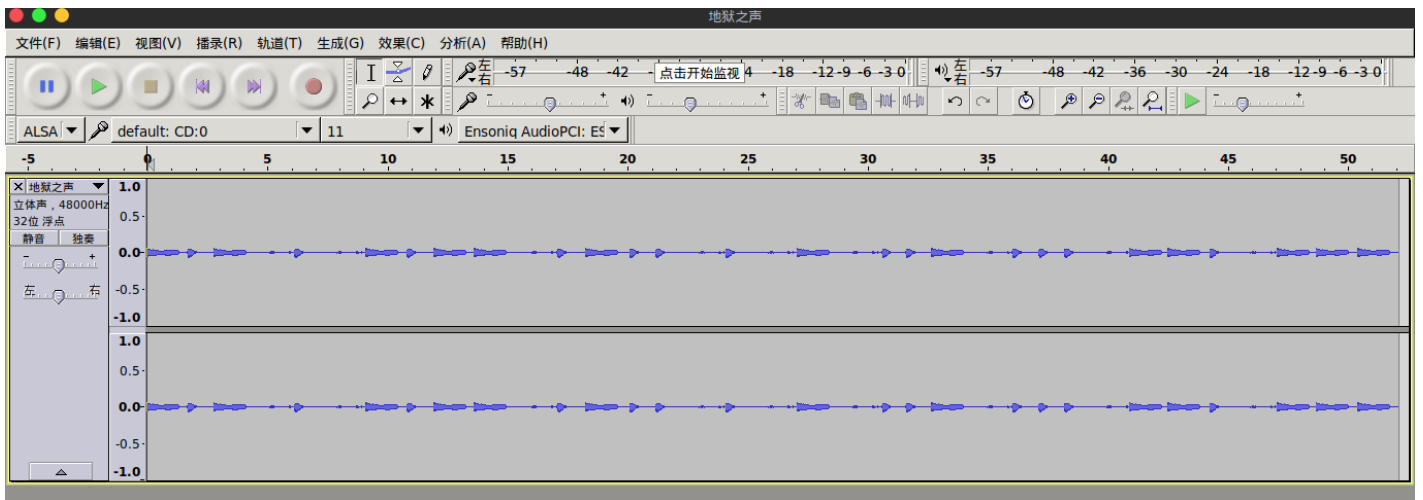
添加完后保存，图片就可以正常显示

很久很久以前，有一位..... 小姐姐..... 扑通一下子..... 掉进了地狱。(别问我为啥，因为她沉行不行)..... 总之.... 有一位河神有一天对你说：“年轻的樵夫呀，你掉的是这个小姐姐呢，还是..... 总之你快去救她吧！”对了，我这里有盘盘的资源呦！
<http://pan.baidu.com/s/1i49Jhlj>

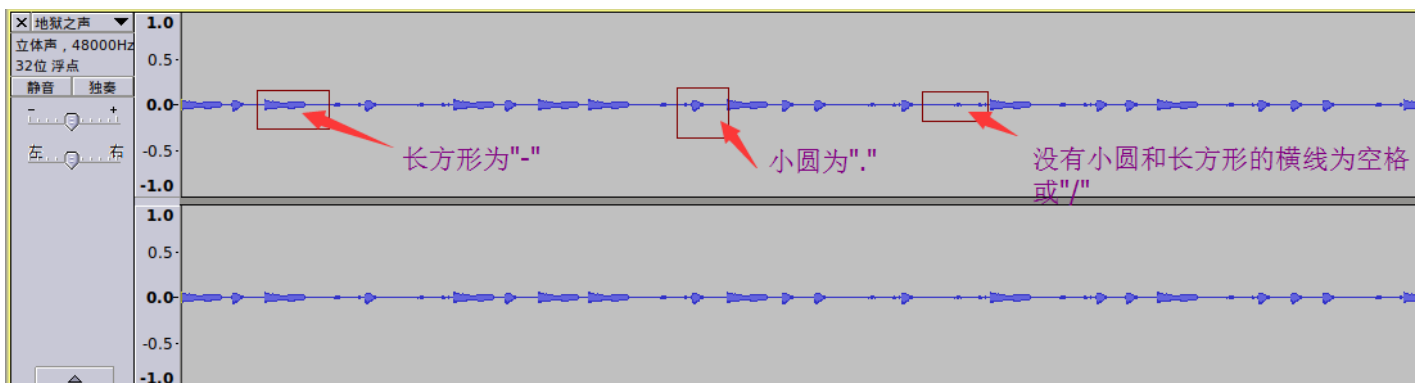
有一个百度网盘的链接，<https://pan.baidu.com/s/1i49Jhlj>，打开，是一个音频文件

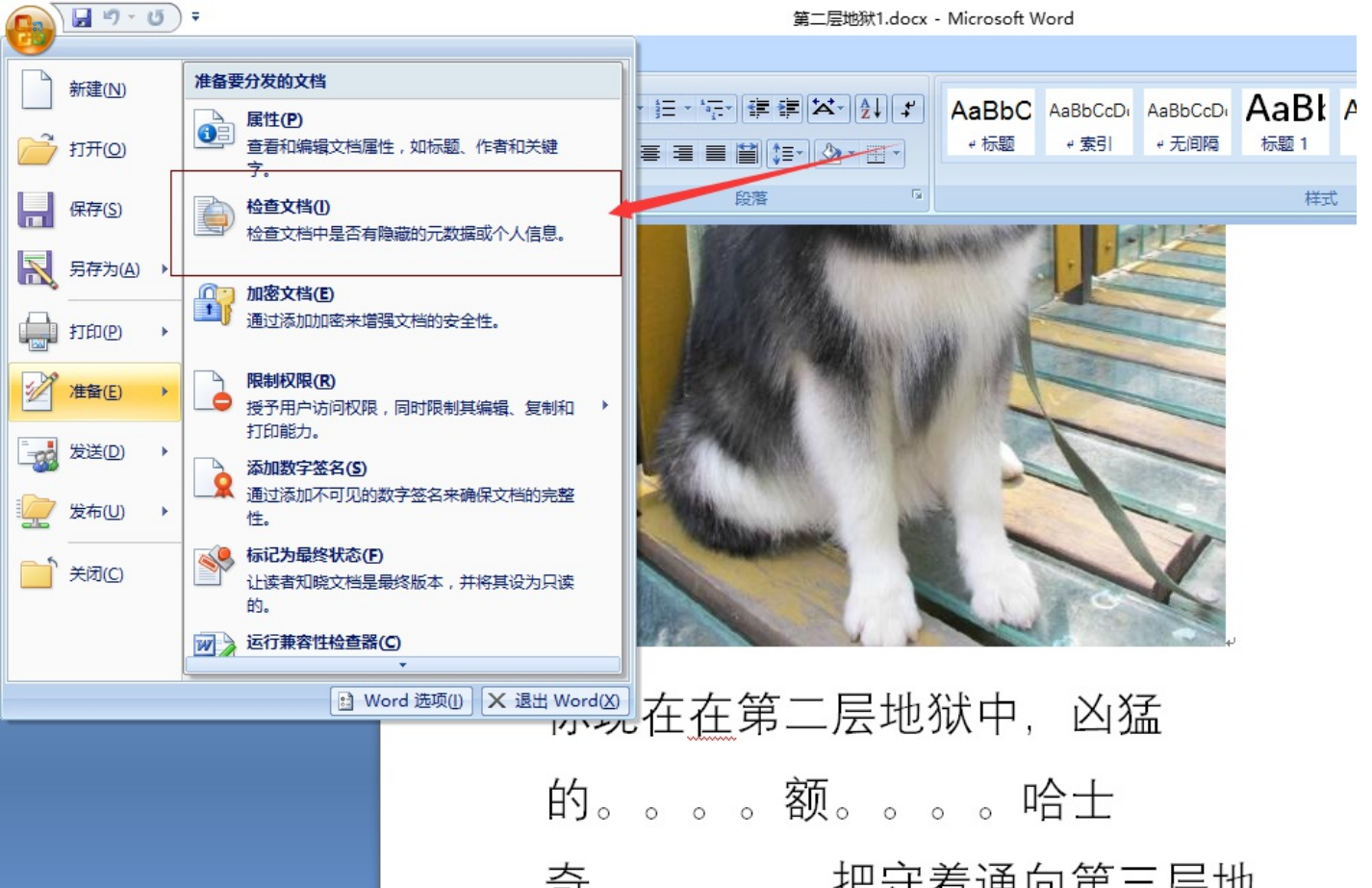


下载，用Audacity打开

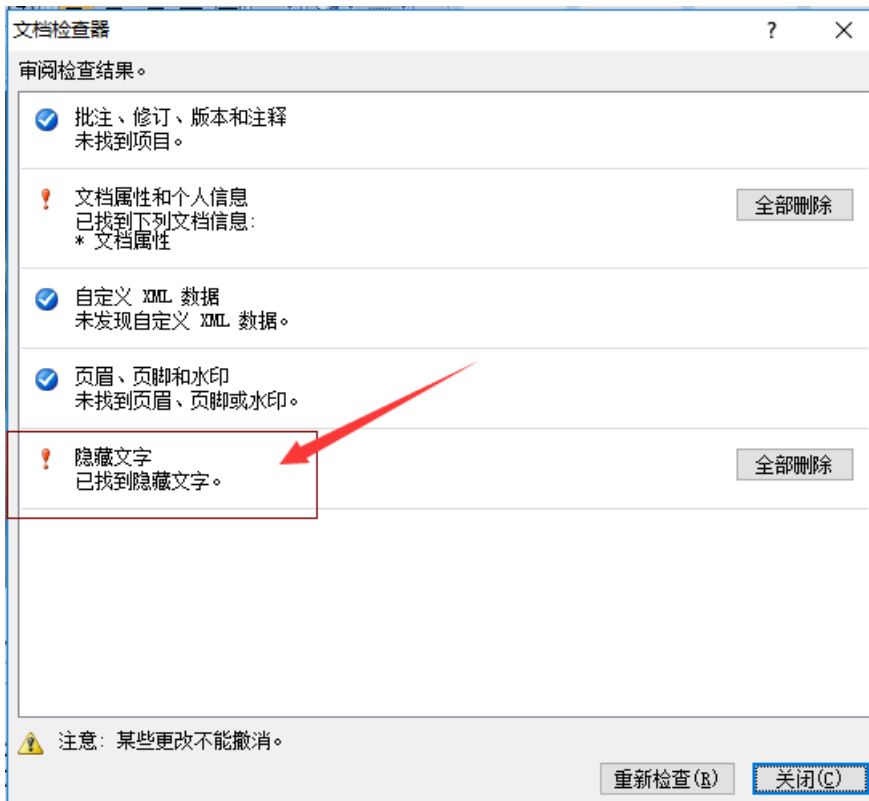


目测为摩斯密码





检测到存在隐藏文字



既然有隐藏文字，那就显示这些隐藏的文字

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： dog.png

2. 输入需要解开信息的密码（如果没有密码可以不填）：

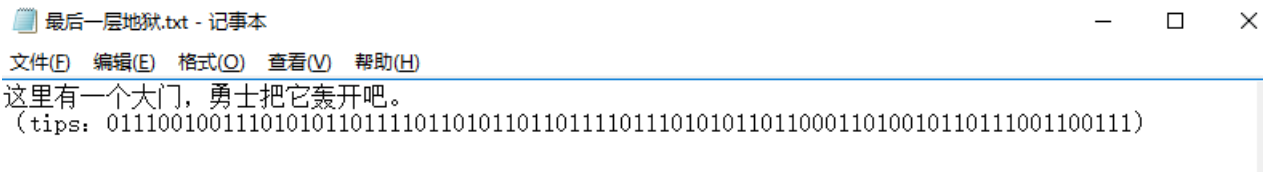
解密出隐藏的信息

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

得到一个key，这个key就是下一关的密码



一个地狱大门.jpg和最后一层地狱.txt



一串二进制

```
01110010011101010110111101101101101111011101101101100011010010110111001100111
```

八个为一组进行转换

```
01110010 01110101 01101111 01101011 01101111  
01110101 01101100 01101001 01101110 01100111
```

转得的ascii码值

ASCII转换到 ASCII (例: a b c)

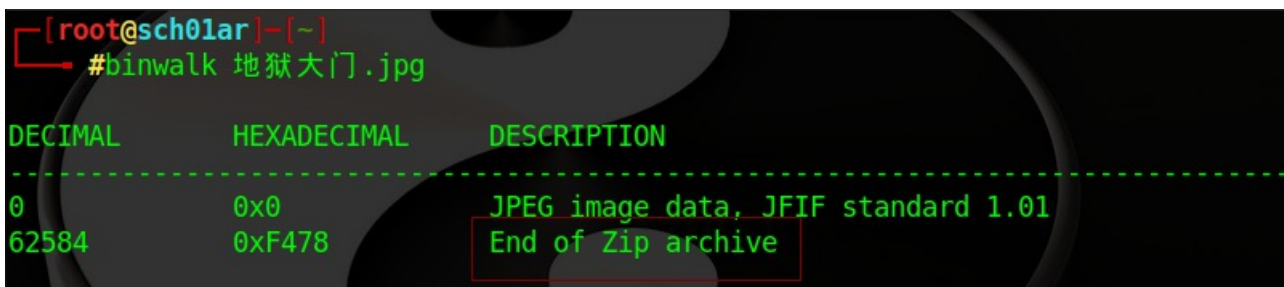
ruokouling

添加空格 删除空格 将空白字符转换

ruokouling, 即弱口令

查看一下地狱之门.jpg是否有隐藏的文件

```
└─[root@sch01ar]-[~]
└─┬─ #binwalk 地狱大门.jpg
```



有一个隐藏的zip压缩包

分离文件

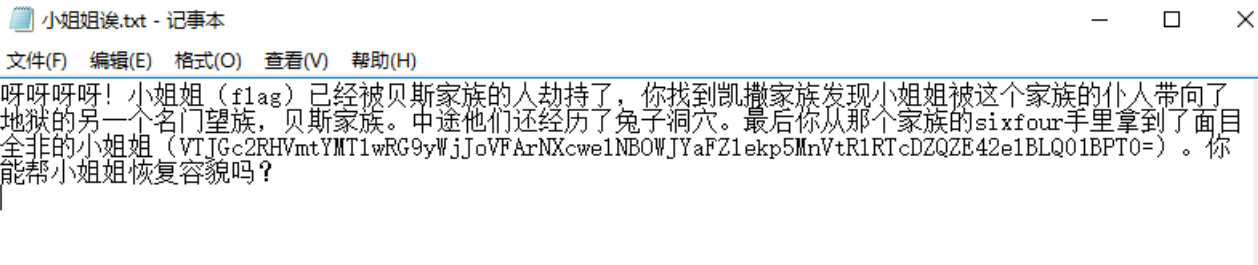


但是需要密码打开压缩包里面的内容

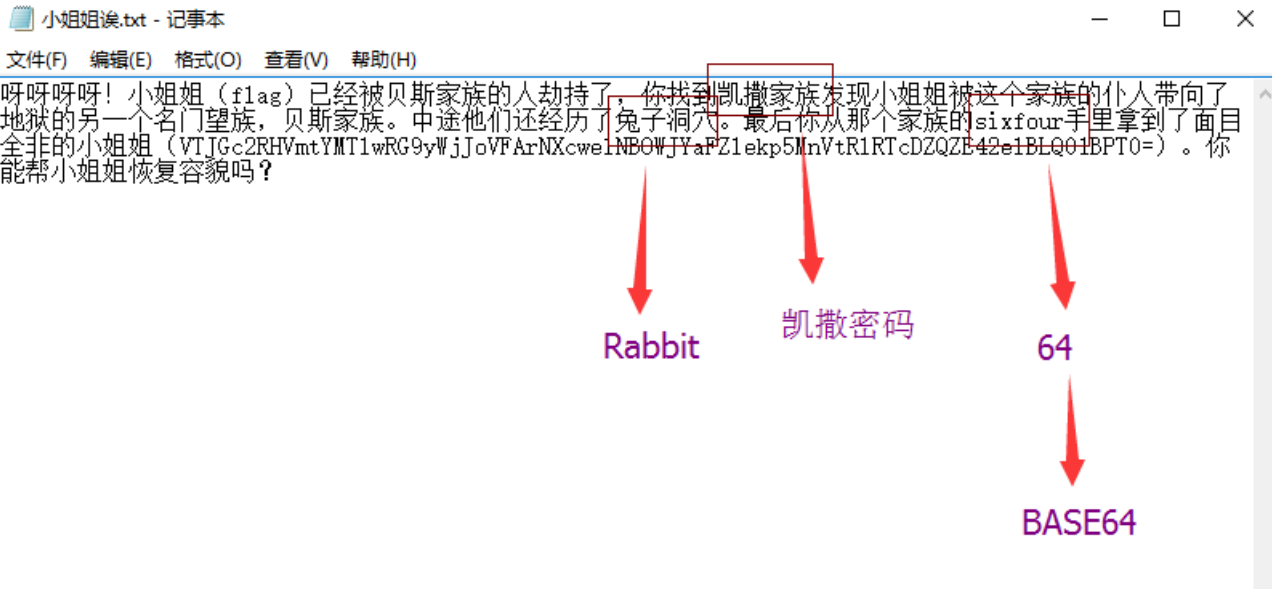


根据二进制解出的提示, 密码可能是弱口令, Password成功

里面的txt里有一段话, 还有一段密文



根据这段话，可得到三个解密方法



首先对

```
VTJGc2RHVmtYMT1wRG9yWjJoVFArNXcwe1NBOWJYaFZ1ekp5MnVtR1RTcDZQZE42e1BLQ01BPT0=
```

进行base64解密，得到

```
U2Fs dGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==
```

再进行Rabbit解密，得到

```
fbqqrwrvnmngrjxsrnshhx
```

最后进行凯撒密码的解密，得到所有可出现的结果

```
kcgvbwabrsrlwocxwsxwsmc
ldhwxcxbtcstmxpdyxyxtnd
meixydycudtunyqezyuzyuoe
nfjyzezdveuvozrfazvazvpf
ogkzafaewfvwpasgbawbawqg
phlabgbfxgwxqbthcbxcbxrh
qimbchcgyhxyrcuidcydcysi
rjnccidhziyzsdvjedzedztj
skodejeiajzatewkfeafeauk
tlpefkfjbkabufxlgfbgfbvl
umqfglgkclbcvgymhgchgcwm
vnrghmhlmdcdwhznihdihdxn
woshinimendexiaojiejieyo
xptijojnfoefyjbpkjfkjfpz
yqujpkogpfgzkcqlkglkgaq
zrvklqlphqghaldrmlhmlhbr
aswlrmqirhibmesnminmics
btxmnsnrjsijcnftonjonjdt
cuynotosktjkdogupokpokeu
dvzopuptluklephvqplqplfv
ewapqvqumvlfqiwrqmrqmgw
fxbqrwrwnwmngrjxsrnsrnhx
gycrsxswoxnohskytsotsoiy
hzdstytxpyopitlzutputpjz
iaetuzuyqzpqjumavuquvuka
jbfuvavzraqrkvnbwvrwvrlb
```

发现有一条密文像拼音

密文框：

```
kcgvbwabrsrlwocxwsxwsmc
ldhwxcxbtcstmxpdyxyxtnd
meixydycudtunyqezyuzyuoe
nfjyzezdveuvozrfazvazvpf
ogkzafaewfvwpasgbawbawqg
phlabgbfxgwxqbthcbxcbxrh
qimbchcgyhxyrcuidcydcysi
rjnccidhziyzsdvjedzedztj
skodejeiajzatewkfeafeauk
tlpefkfjbkabufxlgfbgfbvl
umqfglgkclbcvgymhgchgcwm
vnrghmhlmdcdwhznihdihdxn
woshinimendexiaojiejieyo
xptijojnfoefyjbpkjfkjfpz
yqujpkogpfgzkcqlkglkgaq
zrvklqlphqghaldrmlhmlhbr
```

这个就是flag

- 女神又和大家见面了

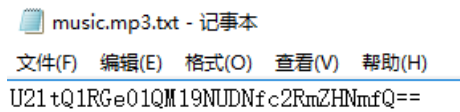
下载图片，用binwalk看一下是否有隐藏文件

```
└─[root@sch01ar]-[~]
└─ #wget http://ctf5.shiyanbar.com/stega/3.jpg
```



```
C:\Users\hp\Desktop\MP3Stego_1_1_18\MP3Stego>Decode.exe -X -P simctf music.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'music.mp3' output file = 'music.mp3.pcm'
Will attempt to extract hidden information. Output: music.mp3.txt
the bit stream file music.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 3416]Avg slots/frame = 417.837; b/smp = 2.90; br = 127.963 kbps
Decoding of "music.mp3" is finished
The decoded PCM output file name is "music.mp3.pcm"
```

输出了一个music.mp3.txt的文件，打开



music.mp3.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
U2ltQ1RGe01QM19NUDNfc2RmZHNmfQ==

是一串密文，base64解密一下

SimCTF{MP3_MP3_sdfdsf}	U2ltQ1RGe01QM19NUDNfc2RmZHNmfQ==
------------------------	----------------------------------

得到flag

- so beautiful so white

so beautiful so white 分值 : 10

来源 : 北邮天枢战队 难度 : 易 参与人数 : 2026人 Get Flag : 1004人 答题人数 : 1072人 解题通过率 : 94%

压缩包的密码就藏在这幅白色图片中，仔细找找看吧
格式 : CTF{}

解题链接 : <http://ctf5.shiyanbar.com/stega/white.zip>

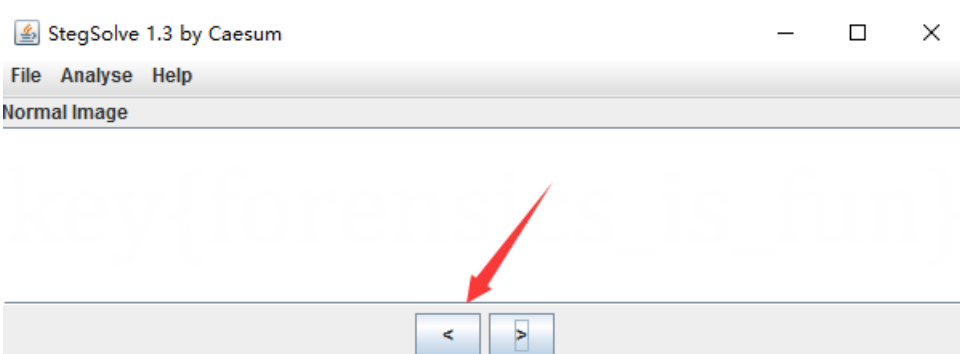
提交

题目提示：压缩包的密码在白色图片中

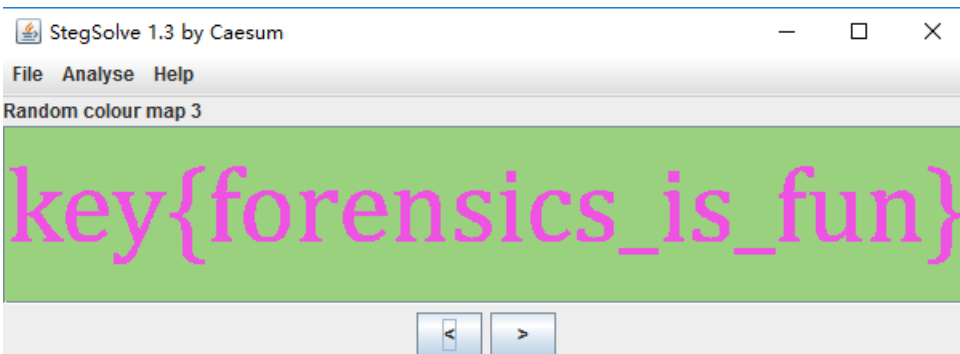
white.zip文件中两个文件



一个有解压密码的zip.zip，里面应该有发flag，还有一个password.png的白色图片，解压密码应该在里面
Stegsolve打开password.png，为一张空白图片

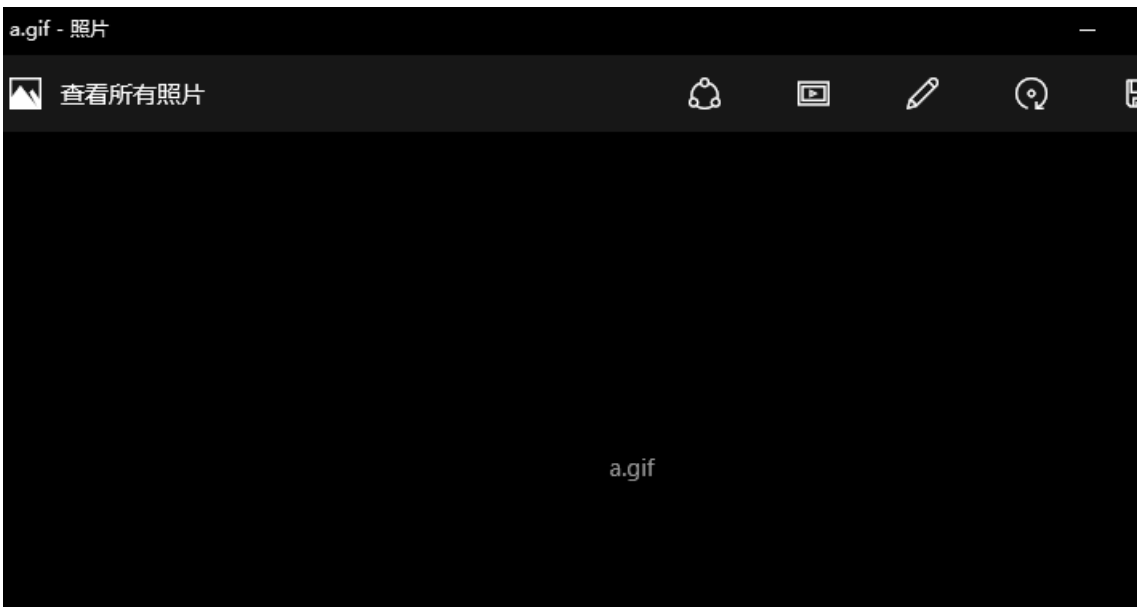


点击这个按钮几次，就会得到一个key

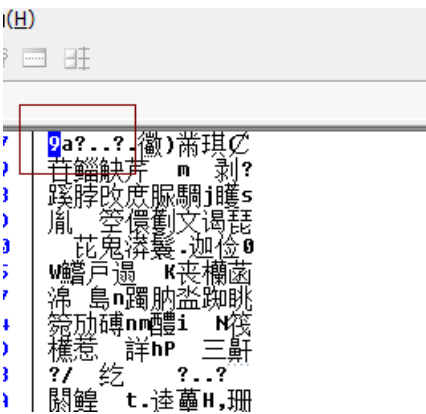


这个key应该就是zip.zip的解压密码

里面有个a.gif，但是不能正常显示



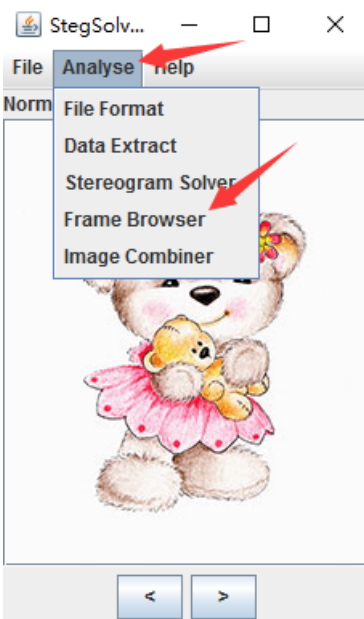
可能文件头有问题，用c32打开



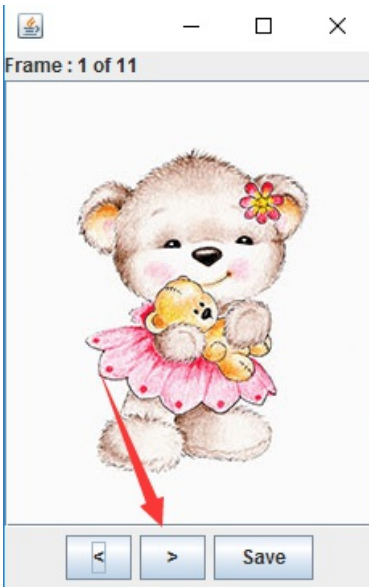
前面的GIF8没有了，把文件头补上去，47 49 46 38

打开gif动图可以看到一个小熊，然后一串字符串一闪而过

用Stegsolve打开



选择Frame Browser



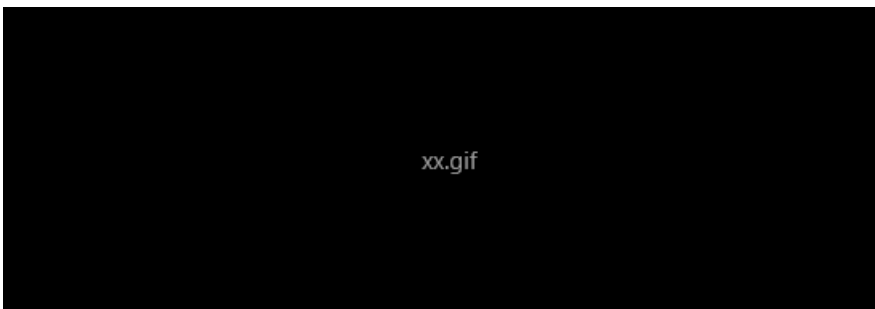
点击这个按钮，依次看每一帧图片

最终得到flag, CTF{AS3X}

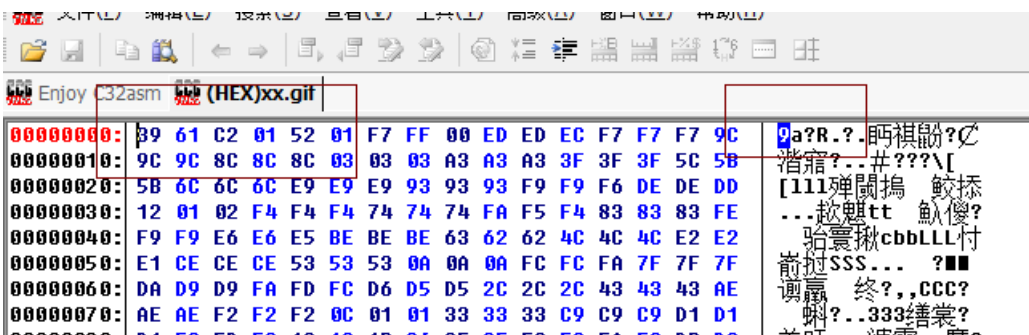
• 打不开的文件

看题目名，估计就是和文件头有关

gif文件打不开



用c32打开



文件头少了47 49 46 38，补上去

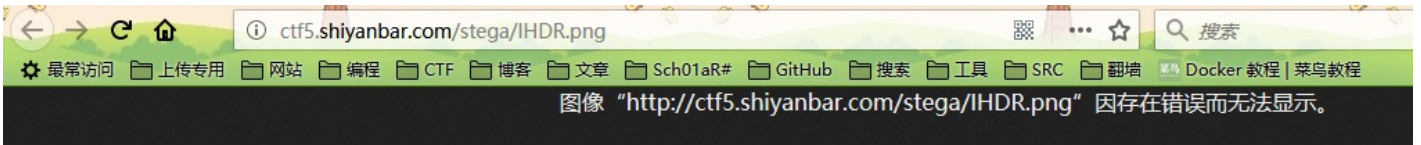
补完之后打开动图，key在动图的帧中

用Stegsolve打开，得到一串字符串：dGhpcyBpcyBhlGdpZg==

base64解密一下得到key, this is a gif

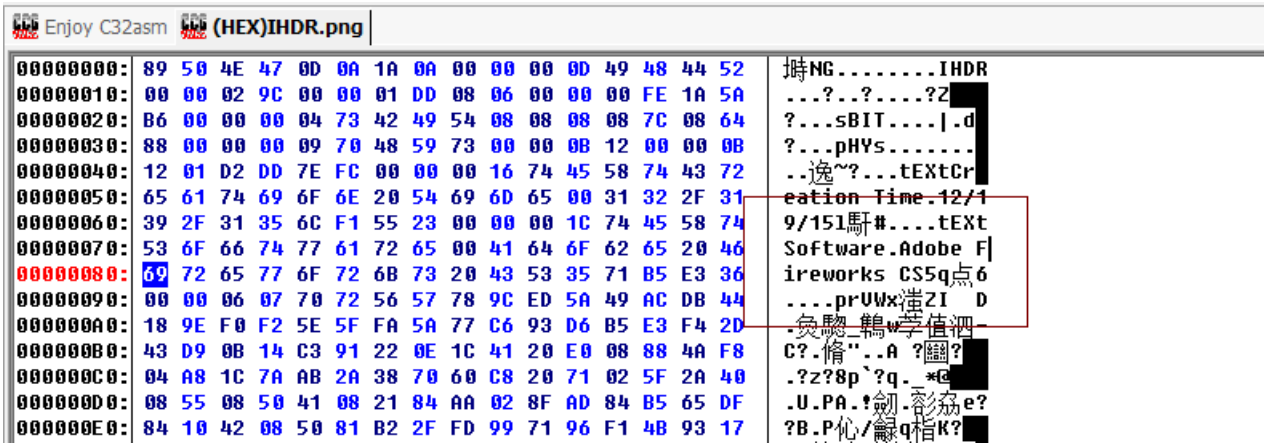
• IHDR

图片不能在网站上显示



下载后能显示

用c32打开



图片提示, Adobe Firework CS5

用Adobe Firework CS5打开图片, 移走下方的图片, 得到flag



• Fonts

Fonts 分值: 10

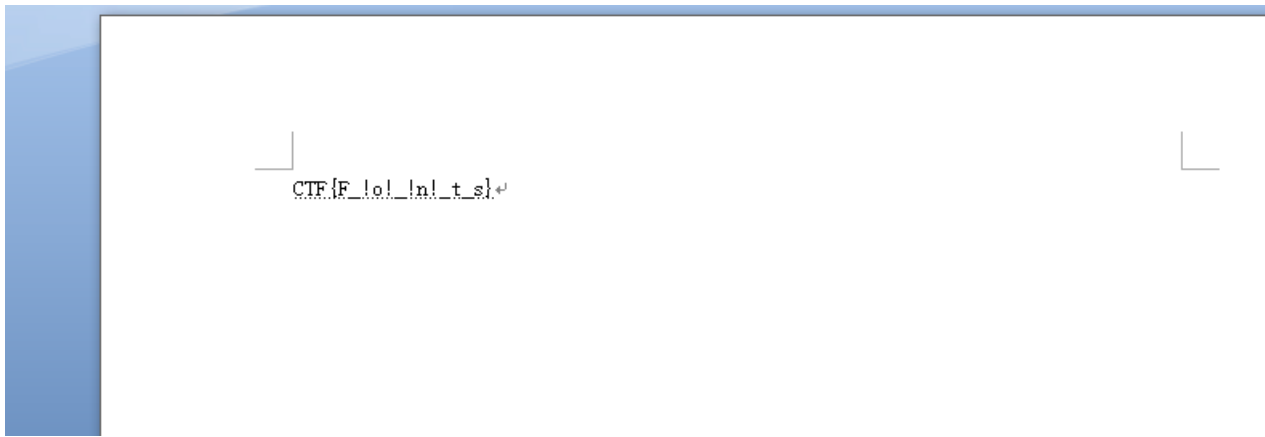
来源: hanyuhang 难度: 易 参与人数: 1396人 Get Flag: 896人 答题人数: 903人 解题通过率: 99%

Flag格式: CTF{xxxx}

解题链接: <http://ctf5.shiyanbar.com/stega/Fonts.doc> 通过

提交

下载文档，打开，得到flag



- 想看正面？那就要看仔细了！

下载图片



右键查看属性



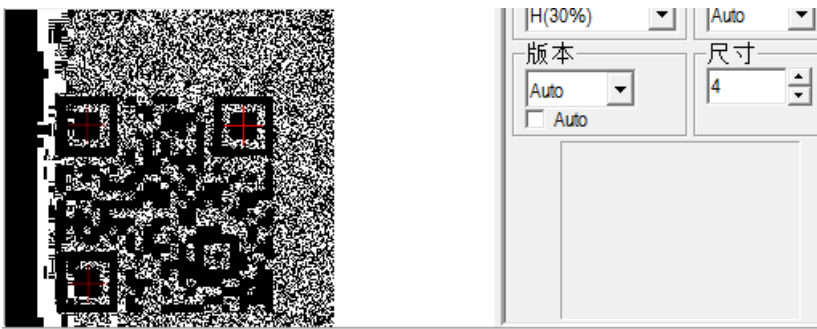
base64解码一下，得到flag

- 无处不在的广告

下载图片，用Stegsolve打开



在此处找到一个二维码，用qr research扫一下，得到flag



已解码数据 1:

位置:(66.2,175.0)-(346.7,176.2)-(69.2,460.4)-(349.5,461.3)

颜色正常, 正像

版本: 2

纠错等级:L, 掩码:6

内容:

FLAG:his is a new word