




CTF-隐写术（一）

原创

红烧兔纸  于 2020-09-11 14:32:43 发布  702  收藏 7

分类专栏: [CTF-隐写术](#)

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_39934520/article/details/108528738

版权



[CTF-隐写术](#) 专栏收录该内容

14 篇文章 2 订阅

订阅专栏

声明: 以下CTF题均来自网上收集, 在这里主要是给新手们涨涨见识, 仅供参考而已。需要题目数据包的请私信或在下方留言。

1.欢迎来到地狱（来源：实验吧）

1.关卡描述

欢迎来到地狱 分值: 25

来源: HTTPERROR404

难度: 中

参与人数: 3603人

Get Flag: 605人

答题人数: 680人

解题通过率: 89%

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>

https://blog.csdn.net/weixin_39934520

2.解题步骤

分析：

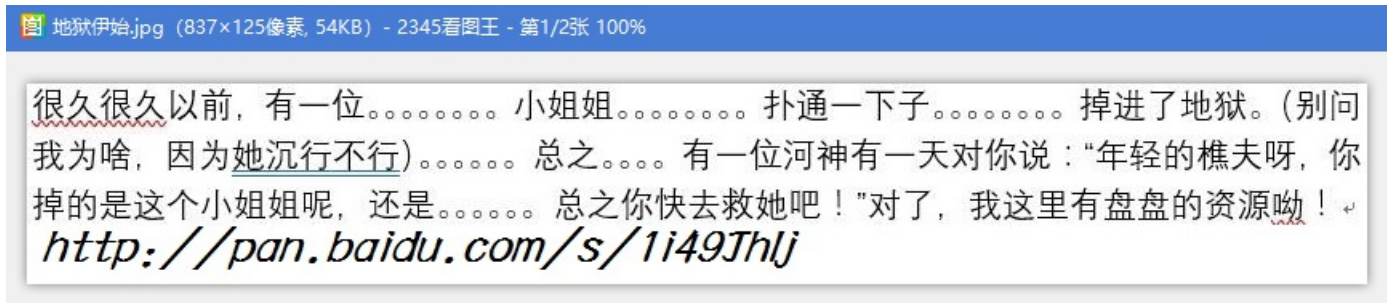
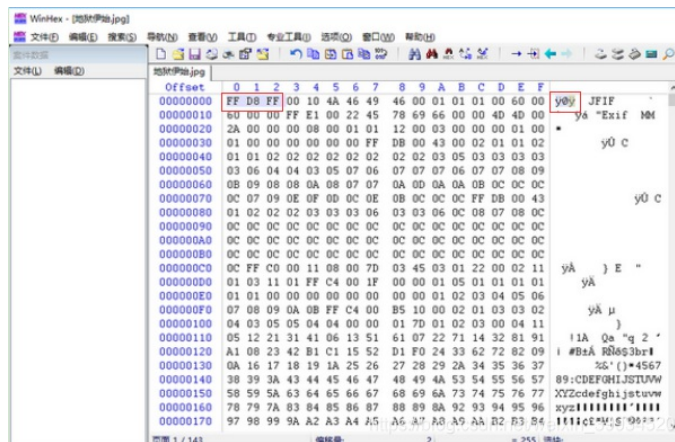
查看压缩包文件：

名称	大小	压缩后大小	类型	安全	修改时间
..(上层目录)					
快到终点了.zip	61.28 KB	61.24 KB	好压 ZIP 压缩文件		2017-10-13 18:54
地狱伊始.jpg	53.59 KB	51.63 KB	看图王 JPG 图片...		2017-10-16 12:21
第二层地狱.docx	969.50 KB	957.44 KB	DOCX 文档		2017-10-15 08:30

发现一张图片和word文档，并打开：



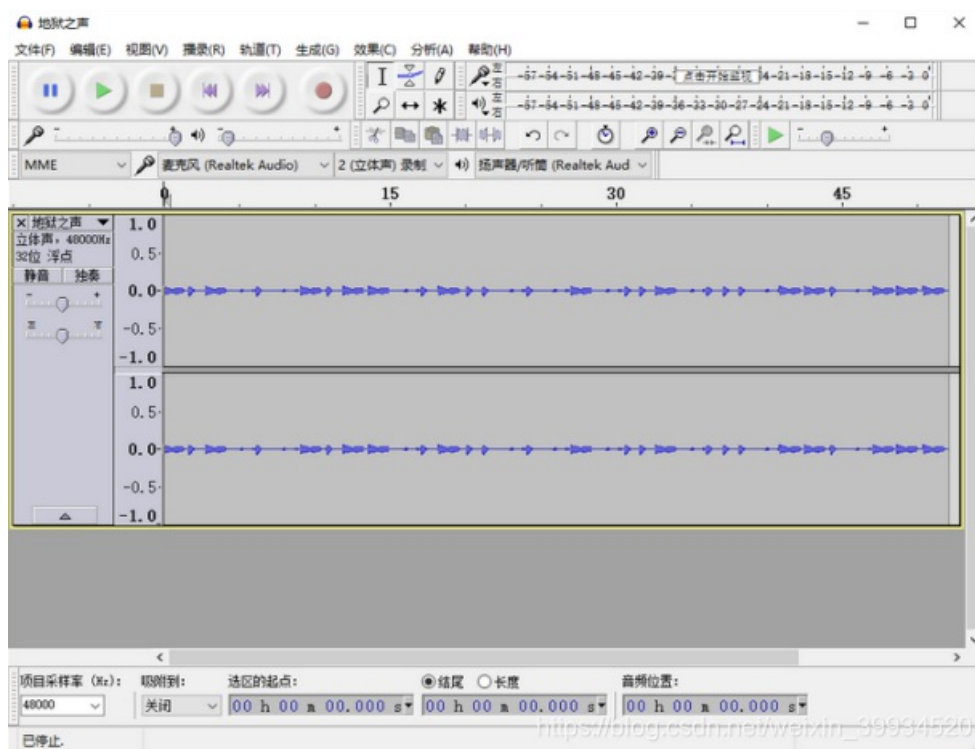
图片打不开（猜测密钥就在图片中），把图片拖入winhex中，发现缺少文件头(.jpg FFD8FF)，粘贴3字节修改一下即可。



<https://pan.baidu.com/s/1i49JhIj>



是一段音频 使用audacity来处理这段音频：地狱之声.wav



发现其类似莫斯电码，

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

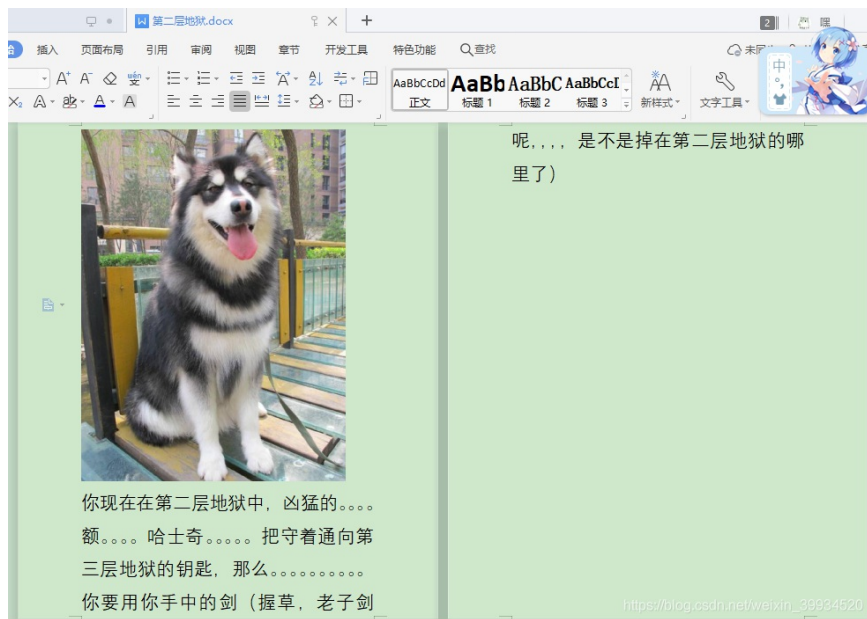
将音频听到的声音，按照摩斯电码的规律记录下来“-. .- .- .- .- .- .- .- .- .- .- .- .- .-”，用CTFCrackTools工具进行转换得到一串字符“KEYLETUSGO”



KEYLETUSGO

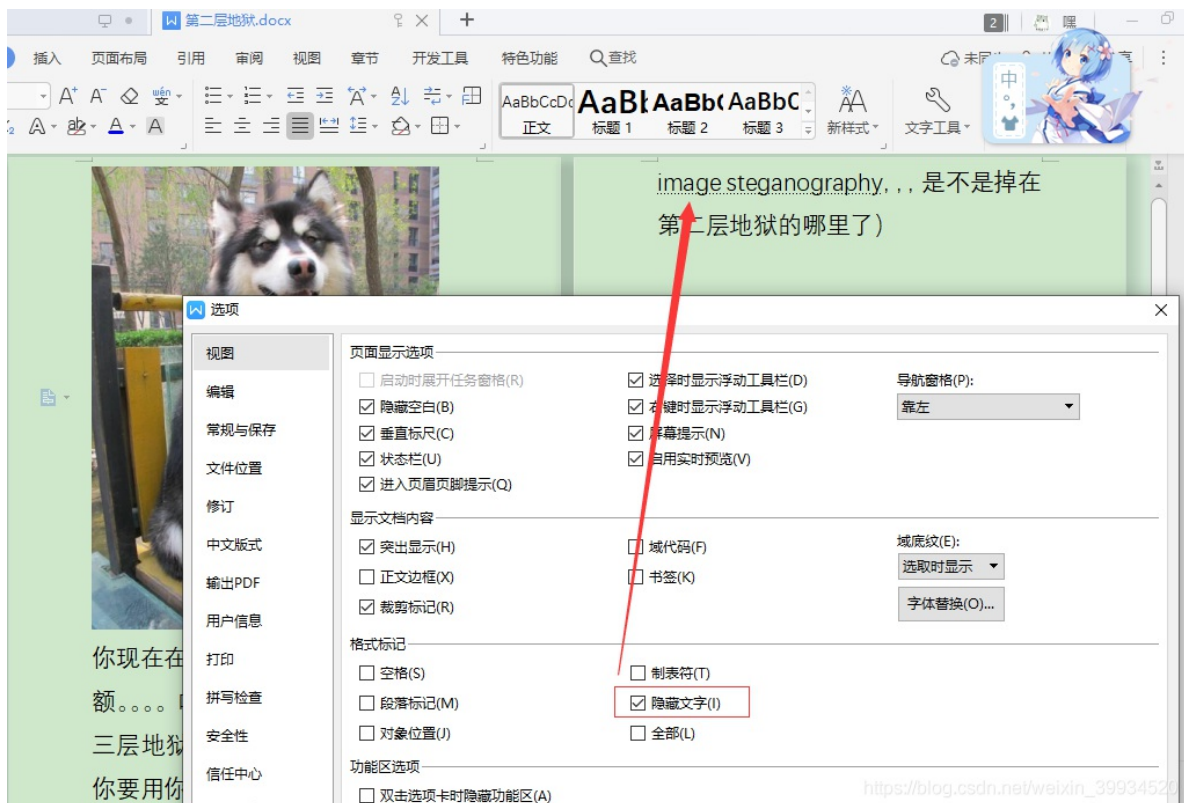
得到word密码:**letusgo**(小写有点坑)

打开word后:

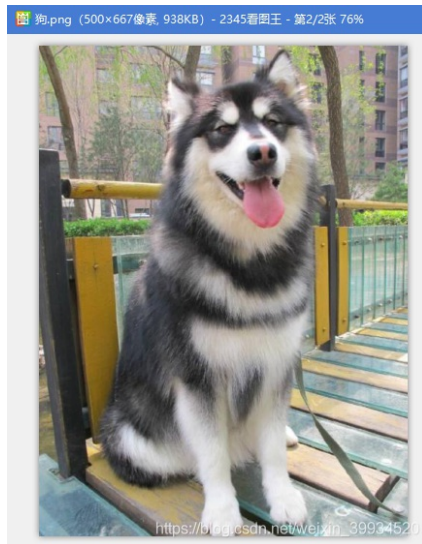


看看 word里面有没有隐藏文字

文件--> 选项--> 隐藏文字的勾勾上 出来了 steganography 上工具。。。



文档文字中说这张狗是通向第三层的钥匙，所以把狗的图片复制出来进行分析。



推荐两个在线解读隐藏信息的图片：

<http://www.atool.org/steganography.php>

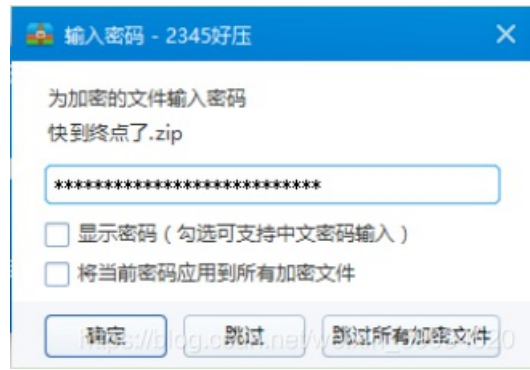
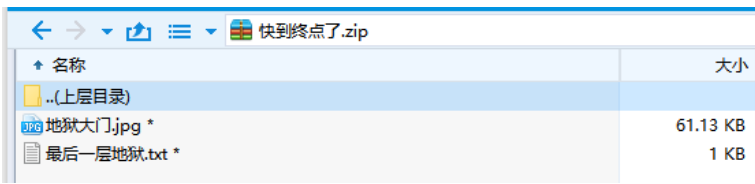


http://tools.jb51.net/aideddesign/img_add_info

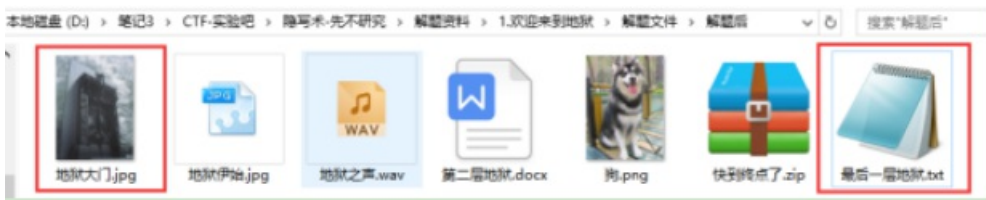


密钥：**key{you are in finally hell now}**

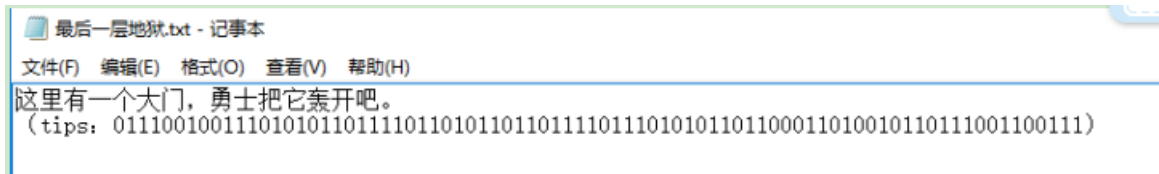
根据刚才的经验，知道这个key肯定是最后一个压缩包所要用的



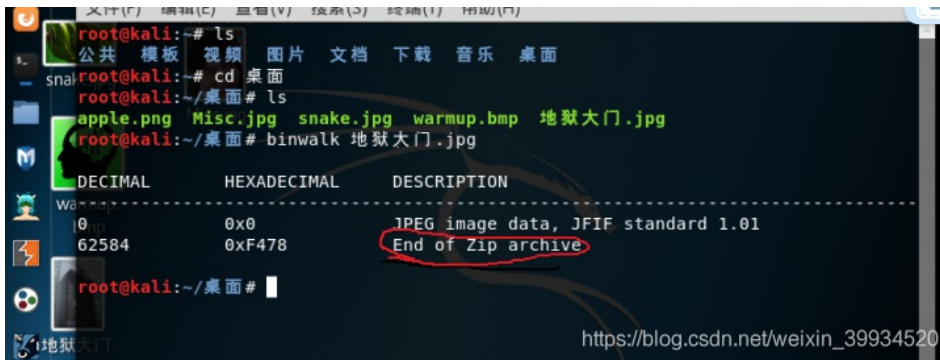
解压后有两个文件：



一张图片和一个txt文本信息，打开这个txt文档



通过里面的文字说明可以知道这个文档是那张图片所需要的密钥，而文档理由提出按二进制数字，将其8个一组进行转换ASCII码，得到“ruokouling”，翻译成中文就是“弱口令”，好吧，这个的意思要么这个拼音是图片的密钥，要么就是图片的解密需要弱口令，而需要弱口令的通常是爆破的时候，也就是说这张图片可能隐藏了一个压缩文件，所以用kali里的binwalk工具查看



把图片 地狱大门.jpg 的后缀改成 地狱大门.zip

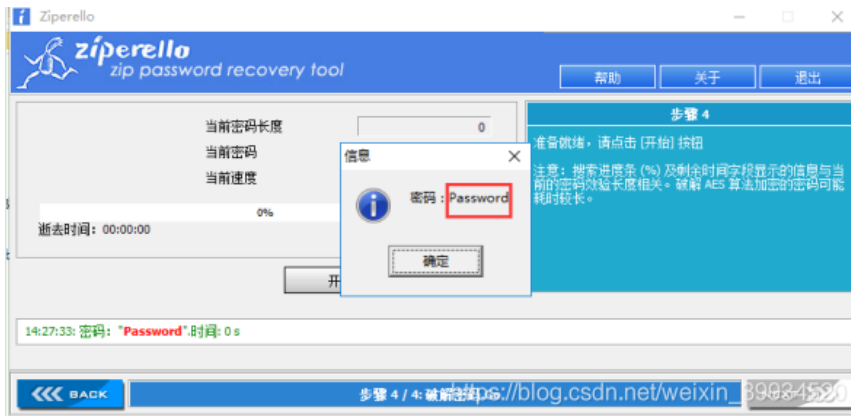


然后打开：

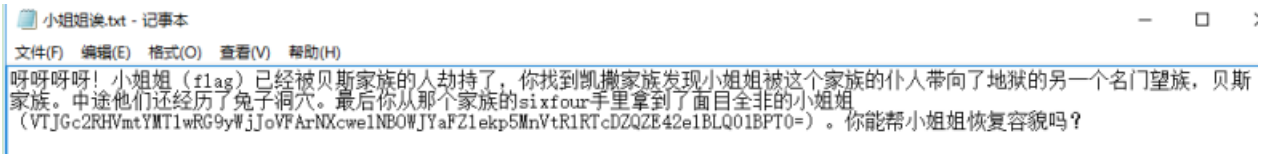


需要解密:

通过之前的解密得到的提示, 需要使用弱口令, 所以打开工具Ziperello, 进行弱口令字典爆破得出密码:
(需要一个好的字典)



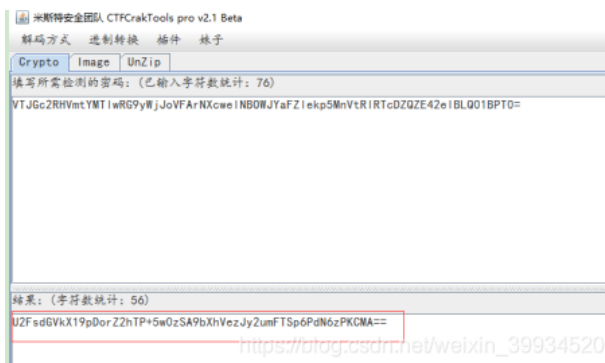
输入密码Password,打开这个文件, 发现一段说明:



贝斯即base sixfour即64

根据文字的提示说明, 知道需要用到base64解码, rabbit解码和凯撒解码, 所以将里面的字符串一步步进行解码:

Base64====>字符串



U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

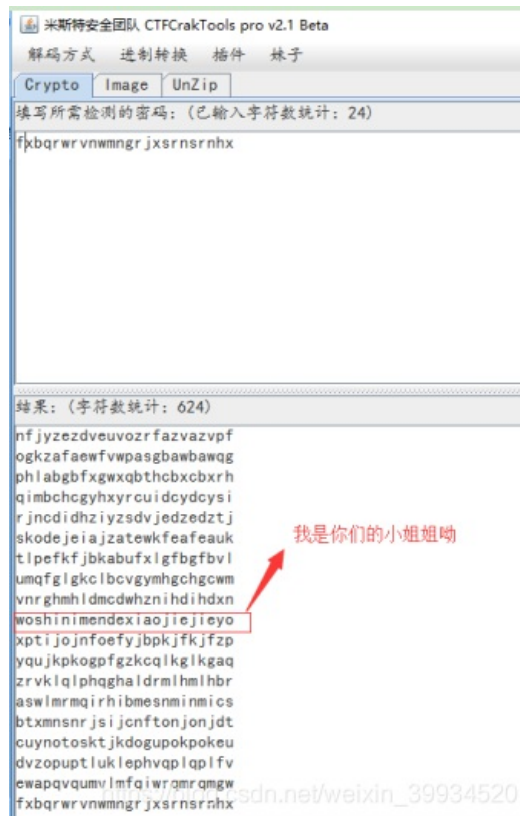
rabbit解码

https://www.sojson.com/encrypt_rabbit.html



fxbqrwrwnmngrijxsrnsrnhx

凯撒解码



最终发现flag: woshinimendexiaojiejieyo

CTF{woshinimendexiaojiejieyo}

2.guess (来源: 实验吧)

1.关卡描述

guess 分值: 10

来源: (づ〇づ)

难度: 易

参与人数: 3203人

Get Flag: 806人

答题人数: 930人

解题通过率: 87%

guess guess guess不出你就out了
flag格式:flag{xxxx}

解题链接: <http://ctf5.shiyanbar.com/misc/angrybird.jpg>

https://blog.csdn.net/weixin_3994520

2. 解题步骤

分析:

这题题目就提示了guess, 又在隐写术里, 搜索一下, 可以看到以下这一段:

Neils Provos的隐写研究是基于统计分析技术的, 他开发的Stegdetect程序主要用于分析JPEG文件。因此用Stegdetect可以检测到通过JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX和Camouflage等这些隐写工具隐藏的信息。

所以这题应该是用了OutGuess隐写。

outguess.org 用于对jpeg彩色图像添加密文, 和读取通过outguess添加在jpg图像中的密文。

outguess是一个图片隐写软件, 可以在github上下载: <https://github.com/crorvick/outguess>,

根据说明编译使用

google找到的使用方法

下载后, 在linux里cd到outguess目录下

`./configure && make && make install`

这样就可以使用outguess命令了。

自己输入个outguess -help就会显示其用法,

```
root@kali2f28:~# outguess -help
outguess: invalid option -- 'h'
OutGuess 0.2 Universal Stego (c) 1999-2001 Niels Provos

outguess [options] [<input file> [<output file>]]
-[sS] <n>      iteration start, capital letter for 2nd dataset
-[iI] <n>      iteration limit
-[kK] <key>    key
-[dD] <name>   filename of dataset
-[eE]          use error correcting encoding
-p <param>    parameter passed to destination data handler
-r           retrieve message from data
-x <n>        number of key derivations to be tried
-m          mark pixels that have been modified
-t          collect statistic information
-F[+-]       turns statistical steganalysis foiling on/off.
             The default is on.
```

看到这么一条

-r retrieve message from data

所以解答本题，只需要在angrybird.jpg所在目录下运行下面语句即可：

outguess -r angrybird.jpg outfile.txt

或者：

Kail终端命令输入git clone <https://github.com/crorvick/outguess>

安装包随即下载到文件夹。双击打开文件夹，右键点击空白区域选终端打开。（或者切换到outguess目录下）

随后输入以下命令./configure && make && make install 进行安装

```
root@kali:~# git clone https://github.com/crorvick/outguess
Cloning into 'outguess'...
remote: Enumerating objects: 217, done.
remote: Total 217 (delta 0), reused 0 (delta 0), pack-reused 217
Receiving objects: 100% (217/217), 535.91 KiB | 67.00 KiB/s, done.
Resolving deltas: 100% (72/72), done.
root@kali:~#
```

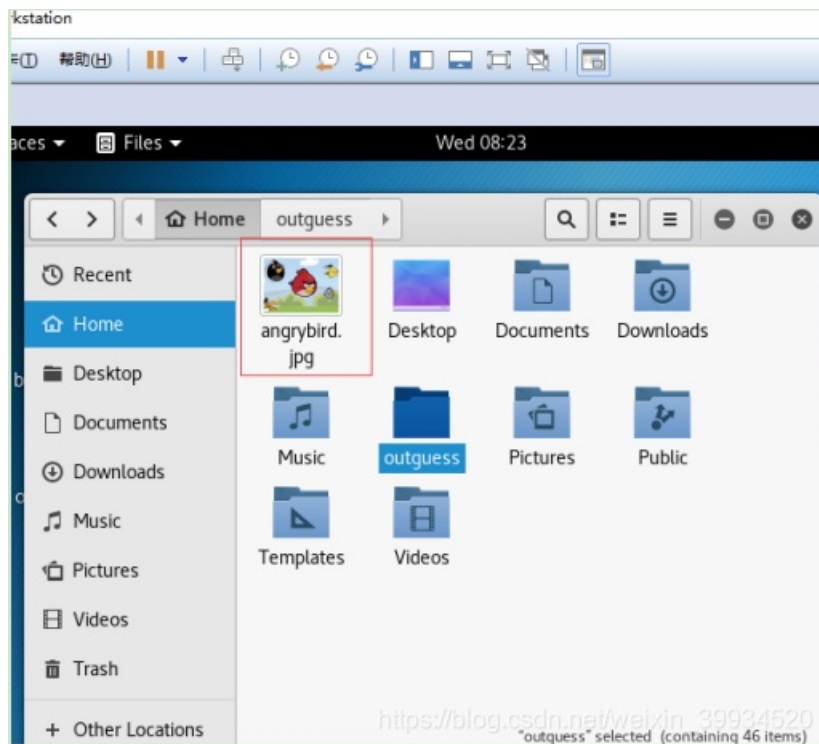
```
root@kali:~# ls
Desktop  Downloads  outguess  Public  Videos
Documents  Music  Pictures  Templates
root@kali:~# cd outguess/
root@kali:~/outguess#
root@kali:~/outguess# ./configure && make && make install
creating cache ./config.cache
checking for gcc... gcc
checking whether the C compiler (gcc ) works... yes
checking whether the C compiler (gcc ) is a cross-compiler... no
checking whether we are using GNU C... yes
checking whether gcc accepts -g... yes
checking if the compiler understands -pipe -Wall -funroll-all-loops... yes
checking for a BSD compatible install... /usr/bin/install -c
checking whether make sets ${MAKE}... yes
checking how to run the C preprocessor... gcc -pipe -Wall -funroll-all-loops -E
checking for ANSI C header files... yes
checking for fcntl.h... yes
checking for unistd.h... yes
https://blog.csdn.net/weixin_39934520
```

输入命令outguess -help 即可获得使用格式如下图

```
root@kali:~/outguess# outguess -help
outguess: invalid option -- 'h'
OutGuess 0.2 Universal Stego (c) 1999-2001 Niels Provos

outguess [options] [<input file> [<output file>]]
  -[sS] <n>      iteration start, capital letter for 2nd dataset
  -[iI] <n>      iteration limit
  -[kK] <key>    key
  -[dD] <name>   filename of dataset
  -[eE]          use error correcting encoding
  -p <param>    parameter passed to destination data handler
  -r            retrieve message from data
  -x <n>        number of key derivations to be tried
  -m           mark pixels that have been modified
  -t           collect statistic information
  -F[+-]       turns statistical steganalysis foiling on/off.
                The default is on.
https://blog.csdn.net/weixin_39934520
root@kali:~/outguess#
```

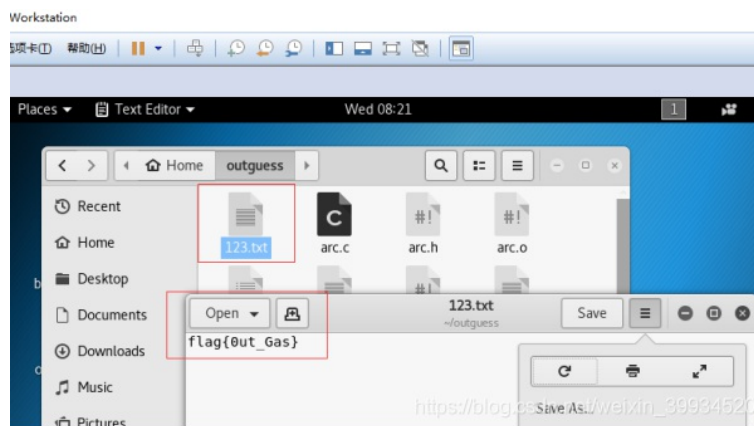
把图片放到根目录下：



对图片信息进行破解的命令如下：**outguess -r /root/angrybird.jpg -t 123.txt**

```
root@kali:~/outguess# outguess -r /root/angrybird.jpg -t 123.txt
Reading /root/angrybird.jpg...
Extracting usable bits: 36252 bits
Steg retrieve: seed: 152, len: 14
root@kali:~/outguess#
```

解密信息如下：



flag{0ut_Gas}



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)