# IDF-CTF-图片里的英语 writeup

转载

weixin_30477293 于 2015-06-13 20:15:00 发布 58 收藏
原文链接：http://www.cnblogs.com/renzongxian/p/4574033.html

题目链接：http://ctf.idf.cn/index.php?g=game&m=article&a=index&id=34

> 一恒河沙中有三千世界，一张图里也可以有很多东西。
> 不多说了，答案是这个图片包含的那句英文的所有单词的首字母。
> 首字母中的首字母要大写，答案格式是wctf{一坨首字母}
> 加油吧少年！看好你哦~

**思路：**
信息隐藏在图片（*这是小李，会不会是小李说过的什么话呢，脑洞中……*）中，使用cat, strings命令查看没有什么有效的字符串。回想以前做过wechall中一个把信息隐藏在图片像素中的题，然后使用Stegsolve.jar工具查看，依然没有看到字符串……

然后就没有思路了，就点了提示（*扣分就扣分吧，不会啊……*），提示“文件拆分，百度一下”。立即百度之，结果发现都是大文件拆分上传之类的，没啥有用的信息……

好歹看到一个有提到Linux工具binwalk的，“后门分析利器”，我擦这难道是一个隐藏在图片中的后门？联想到提示“图片拆分”，完全有可能是把一个什么玩意放进图片里了（这样答案可能就不是小李说的话了，小李我错怪你了……），那么接下来用binwalk看看这图片里有什么幺蛾子。

使用`binwalk 547f180022db2.png`，显示结果

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 266 x 205, 8-bit/color RGBA, non-interlaced
80            0x50            Zlib compressed data, default compression
30977         0x7901          Zlib compressed data, default compression
40459         0x9E0B          Zlib compressed data, default compression
82718         0x1431E         Zlib compressed data, compressed
88477         0x1599D         Zlib compressed data, default compression
99782         0x185C6         Zlib compressed data, compressed
100097        0x18701         RAR archive data
100352        0x18800         Zlib compressed data, compressed
126310        0x1ED66         Zlib compressed data, default compression
162596        0x27B24         Zlib compressed data, compressed
```

原来图片里面有个rar，那么用dd命令提取出来，`dd if=547f180022db2.png of='2.rar' bs=1 skip=100097`，其中if=输入文件名，of=输出文件名，bs=一次读写的最大字节数，skip=跳过的数据块数，将得到的rar文件解压后……尼玛又是一张图片，文件名是flag.jpg，这次换成赵本山了，看文件名应该离答案不远了。

然后用cat, strings查看这张图片，没看出啥，用Stegwalk.jar依旧没看出啥……总不会这张图片里又隐藏了一个文件吧，用binwalk看，没有隐藏……尼玛要疯了……

想到之前的脑洞，不会就是图中人物说的话吧？用谷歌图片搜索发现这是电影《大笑江湖》的一幕，那答案是台词？搜搜它的经典台词，竟然有一句英语“May the force be with you”,那么按首字母提交flag{MTFBWY}，错了……难道大小写不对吗，看看题目要求“首字母中的首字母要大写”（**这句话请读三遍！**），好吧，提交flag{Mtfbwy}，通过了！

转载于:https://www.cnblogs.com/renzongxian/p/4574033.html