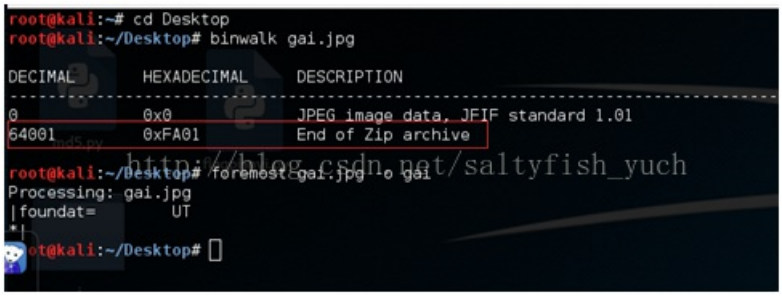
实验吧隐写术部分writeup（1）

原创

saltyfishy 于 2017-09-10 19:07:27 发布 1145 收藏 1
文章标签： ctf

题目：Spamcarver

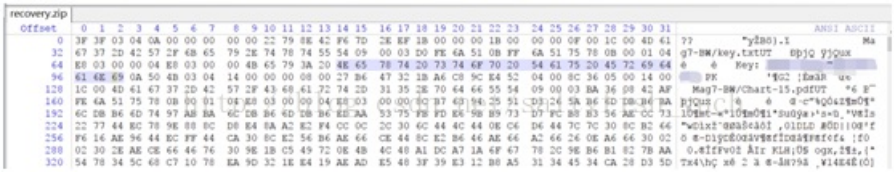
下载得到图片直接丢进kali里binwalk，发现压缩文件尾



于是foremost打开zip即为flag

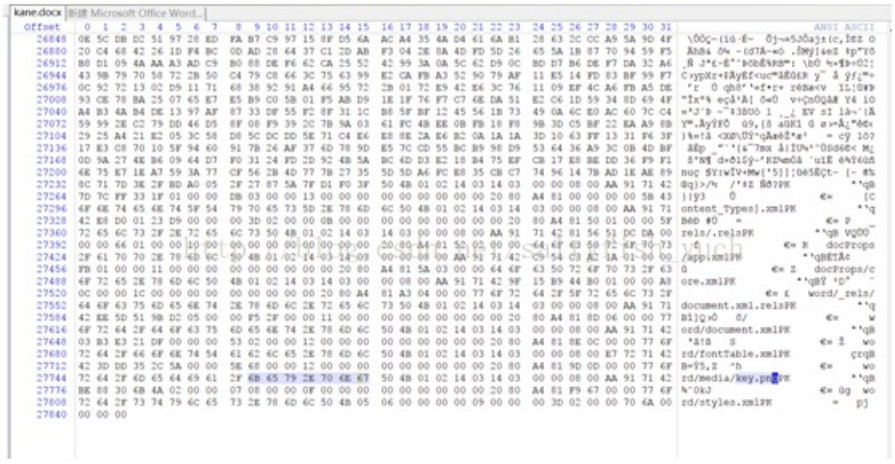
题目：NAVSAT

压缩包下载，无法解压，于是丢进winhex发现key,这里因为压缩包里还有一张地图，根据key还以为要在地图找信息，没想到就是flag

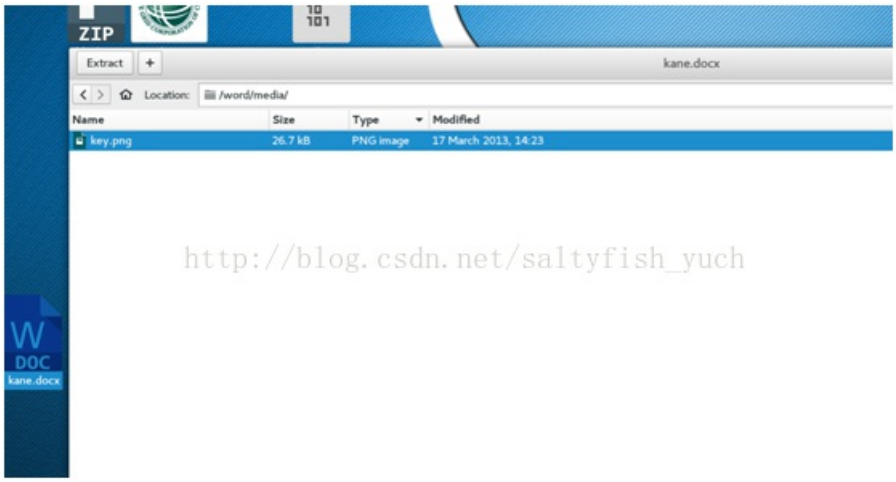


题目：In Hex,No One Can Hear You Complain

直接丢进winhex，在末尾发现png

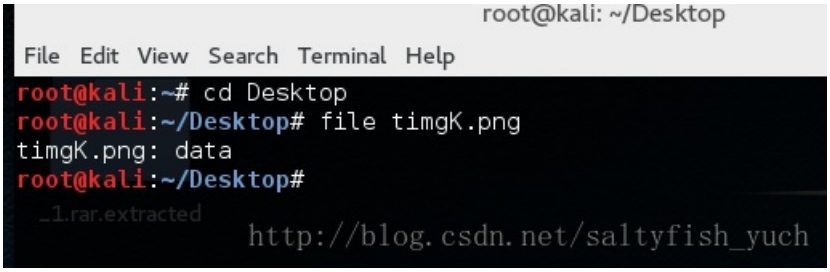


直接在kali中打开，打开图片即为flag



题目：越光宝盒

将图片下载下来直接丢进虚拟机显示文件残缺



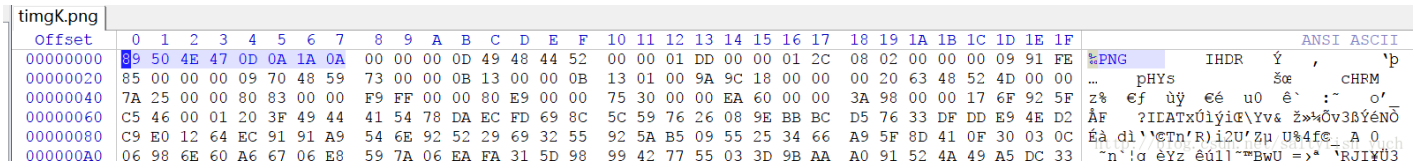
用winhex打开图片判断为文件头残缺，于是百度png文件头

PNG的文件结构

对于一个PNG文件来说，其文件头总是由位固定的字节来描述的：

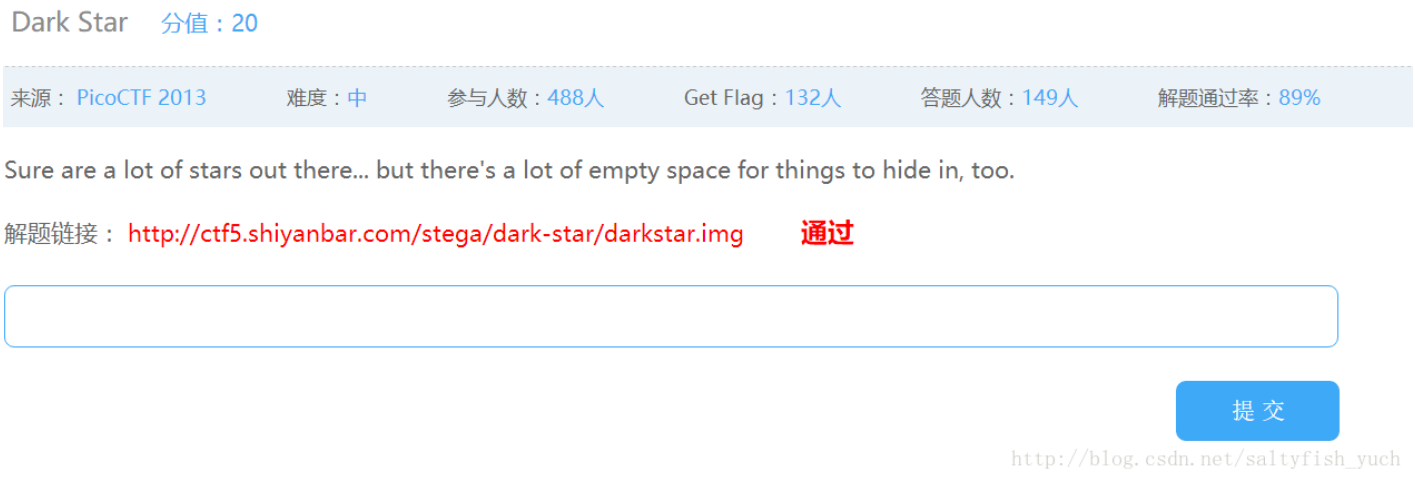
十进制数	137 80 78 71 13 10 26 10
十六进制数	89 50 4E 47 0D 0A 1A 0A

将正确的文件头写入



保存，打开即为flag

题目：Dark Star



文件下载之后发现无法打开，于是丢入虚拟机binwalk一下发现图片

```
oot@kali:~/Desktop# binwalk darkstar.img

ECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
3146752       0x300400        PNG image, 192 x 56, 8-bit/color RGBA, non-interl
ed
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-Pac
ard Company"
4738048       0x484C00        JPEG image data, JFIF standard 1.01
4738346       0x484D2A        Copyright string: "Copyright 1999 Adobe Systems I
corporated"
4740040       0x4853C8        JPEG image data, JFIF standard 1.02
4743332       0x4860A4        Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"
<rdf:Description rdf:about="" xmlns:tiff="http://ns.adobe.com/tiff/1.0/" xmlns
:exif="htt
```

于是分离出图片

```
root@kali:~/Desktop# foremost darkstar.img -o darkstar
Processing: darkstar.img
|*|
```


分离出的图片即可找到flag

持续施工中。。。