Bugku writeup（杂项）2【隐写2】

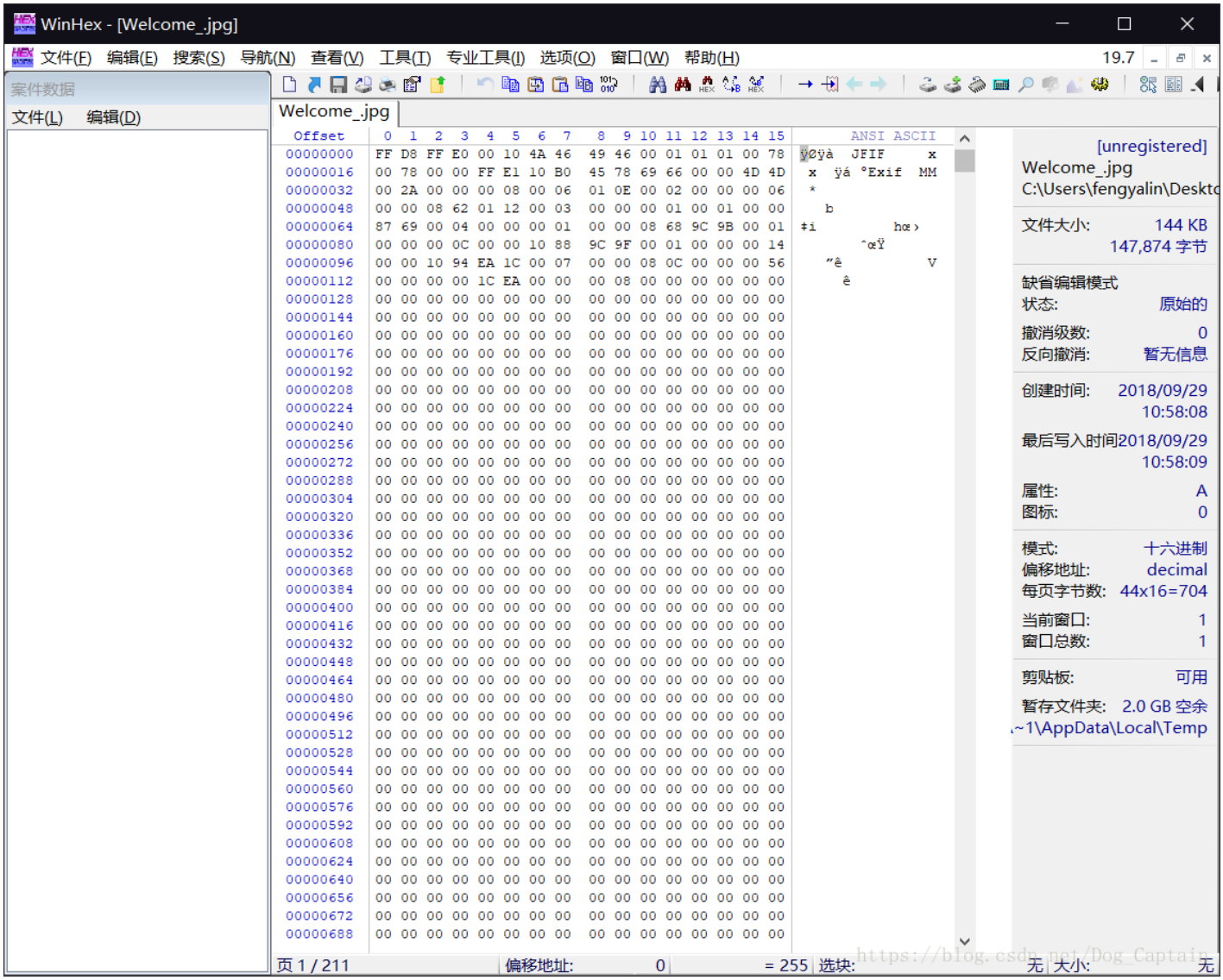
原创

Sn1Per_395 于 2018-09-29 11:43:19 发布 1140 收藏 2
分类专栏： ctf解题思路 文章标签： ctf writeup bugku

本文链接：https://blog.csdn.net/Dog_Captain/article/details/82895311

【隐写2】

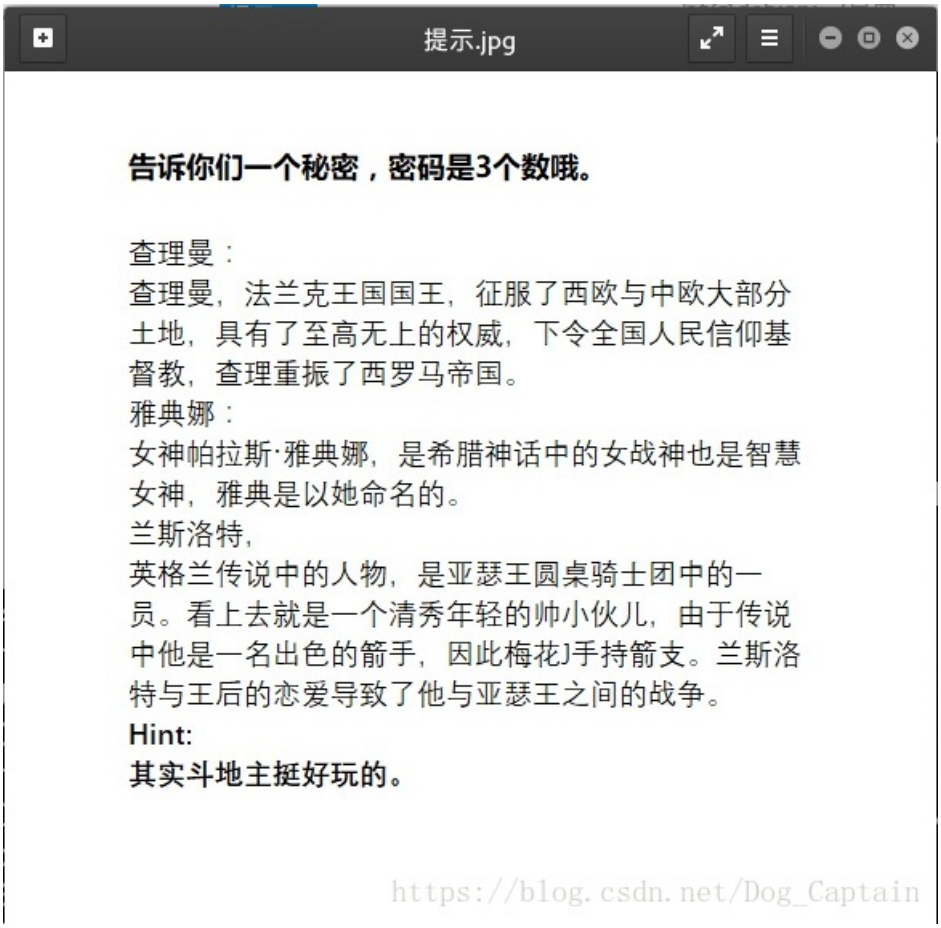
拿到题目，是一张图片，老套路，用winhex打开，但并没有发现什么有用信息。



再把图片放到kali中，用binwalk提取

```
root@debian:~/桌面# binwalk Welcome_.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
4444          0x115C          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
4900          0x1324          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:li xml:lang="x-default">hint:</rdf:li></rdf:Alt>
52516         0xCD24          Zip archive data, at least v1.0 to extract, compre
ssed size: 6732, uncompressed size: 6732, name: flag.rar
59264         0xE780          End of Zip archive
147852        0x2418C         End of Zip archive
```

红桃k里的国王是建立查理曼帝国的查理大帝。

方块k里的国王是古罗马的恺撒大帝。

梅花k里的画像是亚历山大，曾一手缔造了地跨欧、亚、非三大洲的亚历山大帝国。

黑桃k是公元前10世纪以色列国王索洛蒙的父亲戴维。黑桃q是希腊智慧和战争女神帕拉斯·阿西娜。

红桃q名叫朱尔斯，她嫁给英国斯图尔特王朝的查尔斯一世。

梅花q寓意着这样一个故事：英国的兰开斯特王族皇后。方块q是莱克尔皇后，她是雅各布的女儿。

黑桃j为查尔斯一世的侍从霍克拉。

方块j为查尔斯一世的侍从洛兰。

红桃j为查尔斯七世的侍从拉海亚。

梅花j是阿瑟王故事中的著名骑士兰斯洛特

通过百度，知道三个人分别代表的扑克牌，通过观察键盘KJQ代表871

或者用ARCHPR爆破，得到密码871

解压得到

用winhex打开

```
23 E4 67 D4 FF D9 20 20  20 20 66 31 40 67 7B 65 | #ägÔÿÙ    fl@g{e
54 42 31 49 45 46 79 5A  53 42 68 49 47 68 41 59 | TB1IEFyZSBhIGhAY
32 74 6C 63 69 45 3D 7D  20 20 20 20 20 0D 0A 20 | 2tlciE=}
1A
```


得到的flag为base64，解码可得到flag

```
> atob('eTB1IEFyZSBhIGhAY2tlciE=')
< "y0u Are a h@cker!"
```


将fl@g改为flag，即可得到答案。