

# 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](#)

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/Dog\\_Captain/article/details/82895311](https://blog.csdn.net/Dog_Captain/article/details/82895311)

版权



[ctf解题思路](#) 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

## 【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。

WinHex - [Welcome\_.jpg]

文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

19.7

案件数据

文件(L) 编辑(D)

Welcome\_.jpg

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	78
00000016	00	78	00	00	FF	E1	10	B0	45	78	69	66	00	00	4D	4D
00000032	00	2A	00	00	00	08	00	06	01	0E	00	02	00	00	00	06
00000048	00	00	08	62	01	12	00	03	00	00	00	01	00	01	00	00
00000064	87	69	00	04	00	00	00	01	00	00	08	68	9C	9B	00	01
00000080	00	00	00	0C	00	00	10	88	9C	9F	00	01	00	00	00	14
00000096	00	00	10	94	EA	1C	00	07	00	00	08	0C	00	00	00	56
00000112	00	00	00	00	1C	EA	00	00	00	08	00	00	00	00	00	00
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000528	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000544	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000576	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000592	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000608	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000624	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000656	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000672	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000688	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

ANSI ASCII

ÿÿà JFIF x

x ýá °Exif MM

\*

b

±i            hœ>

^œÿ

"é

è

V

[unregistered]

Welcome\_.jpg

C:\Users\fengyalin\Desktop

文件大小: 144 KB

147,874 字节

缺省编辑模式

状态: 原始的

撤销级数: 0

反向撤销: 暂无信息

创建时间: 2018/09/29 10:58:08

最后写入时间: 2018/09/29 10:58:09

属性: A

图标: 0

模式: 十六进制

偏移地址: decimal

每页字节数: 44x16=704

当前窗口: 1

窗口总数: 1

剪贴板: 可用

暂存文件夹: 2.0 GB 空余

~1\AppData\Local\Temp

页 1 / 211      偏移地址: 0      = 255 选块:      无 | 大小: 无

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, compressed size: 6732, uncompressed size: 6732, name: flag.rar
59264	0xE780	End of Zip archive
147852	0x2418C	End of Zip archive

[https://blog.csdn.net/Dog\\_Captain](https://blog.csdn.net/Dog_Captain)



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

[https://blog.csdn.net/Dog\\_Captain](https://blog.csdn.net/Dog_Captain)

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

[https://blog.csdn.net/Dog\\_Captain](https://blog.csdn.net/Dog_Captain)

```

23 E4 67 D4 FF D9 20 20 20 20 66 31 40 67 7B 65 #ägÛÜ 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 2t1ciE=}
1A

```

用winhex打开

```

> atob('eTB1IEFyZSBhIGhAY2t1ciE=')
< "you Are a h@cker!"

```

得到的flag为base64，解码可得到flag

将fl@g改为flag，即可得到答案。