

# FIVE1 writeup

原创

太阳已经起床了  于 2019-04-03 16:37:14 发布  5749  收藏

分类专栏: [CTF隐写](#)

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/qq\\_42105549/article/details/88998926](https://blog.csdn.net/qq_42105549/article/details/88998926)

版权



[CTF隐写 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

为了证明我不是铁five, 做了这道题。

题目:

图片内藏有5位数密码, 你能找出来吗?

flag格式: flag{xxx}

解题链接: [<http://ctf5.shiyanbar.com/stega/FIVE1/1111110000000000.jpg>](javascript:?)

打开连接, 得到一张图片:



按照常规操作, 先查看图片的属性, 一无所获。

用binwalk查看

```
python binwalk -e 1.jpg
```

发现其中有一个压缩文件, 应该也是一张图片, 打开需要解压密码。这个密码我找了好长时间都没发现, 后来看别人的write up才知道, 原来在下载这个图片文件的时候, 文件名是: 1111110000000000.jpg

这是段二进制数!!!!

当时我为了方便之间将文件名改为1.jpg...

看来做CTF的题不能漏过一丝一毫的信息。

将这段二进制数转化为十六进制: FC00。输入, 成功解压压缩包。得到另一张图片:



这张图片的名字没有什么信息量（吃一堑长一智），然后用各种软件进行分析，通过winhex和stegsolve都可以发现这个图片中藏有一段字符。其中stegsolve显示的格式更为清晰：



```
-----  
Ascii  
echo "L S0uLi4gI  
C4tICAuL i4uLiAgL  
S0uLi4gI C4tICAuL  
i4uLiAgL i0gIC0tL  
i4uICAuL i4uLSAgL  
i4uLS0gI C0tLS4uI  
CAtLS0tL iAgLi4uL  
i0gIC4tI CAtLS0tL  
SAgLiAg" >1.txt  
OK
```

可以大约估计一下，这应该是BASE64编码，大致说一下其编码特点：

**\*\*字符串只可能包含A-Z, a-z, 0-9, +, /, =字符\*\***

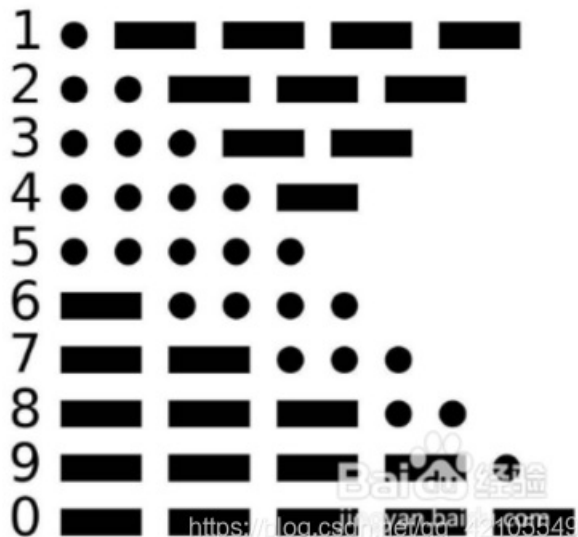
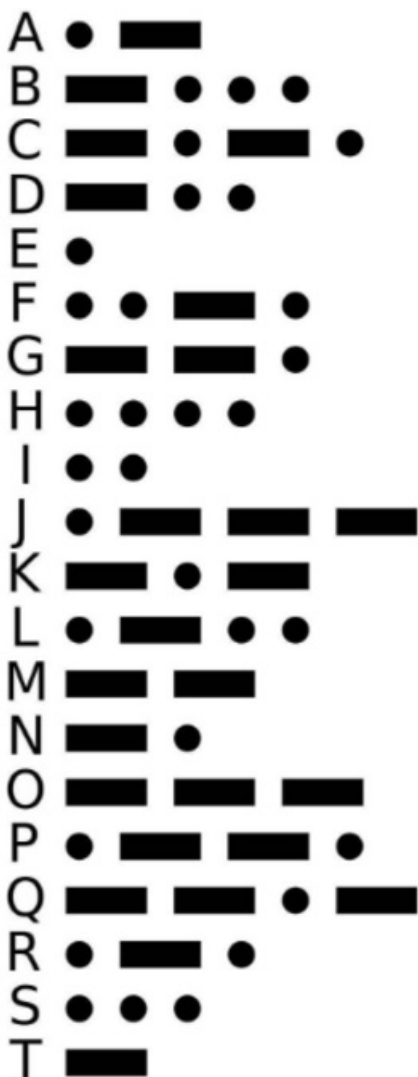
**\*\*字符串长度是4的倍数\*\***

**=只会在字符串最后，可能没有或者一个等号或者两个等号**

解码后，得到：

-----

这就很清晰了，这应该是摩斯密码，但是一般的在线破解摩斯密码的网站都只能翻译出英文字母，而不能翻译出数字（这些网站的制造者太懒了。。）我只能手动翻译：



得到：

7A57A5A743894A0E

这是啥???

看来我的密码学并没有学好，对很多类型的密码并不是很敏感。

分析发现它只有16位同时还是十六进制，很有可能是md5加密后的结果，



The screenshot shows a web interface for MD5 decryption. At the top, there is a dark blue header bar containing a text input field with the value "7A57A5A743894A0E", a dropdown menu set to "自动", and a "[帮助]" link. Below the header are two buttons: "查询" (Query) in orange and "加密" (Encrypt) in blue. Underneath is a white box with the text "查询结果:" followed by "admin". In the bottom right corner of the interface, there is a URL: [https://blog.csdn.net/cq\\_42105549](https://blog.csdn.net/cq_42105549).

很好，得到最终结果：**flag{admin}**