

# 杂项的图片隐写题

原创

MIGENKING 于 2019-09-19 00:17:52 发布 1341 收藏 6

分类专栏: [做题](#)

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/MIGENKING/article/details/101003129>

版权



[做题](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

Challenge

7409 Solves



## 这是一张单纯的图片

### 50

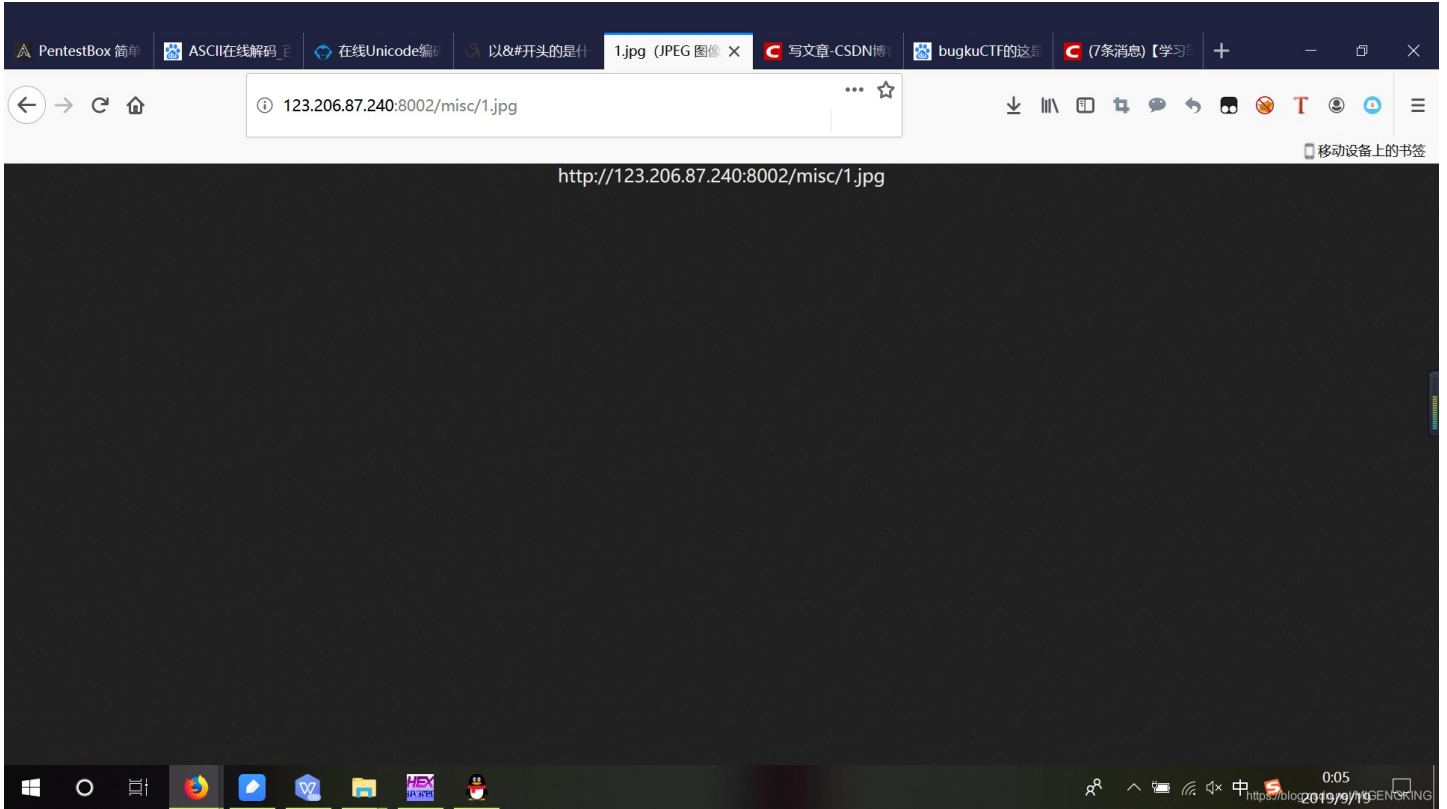
<http://123.206.87.240:8002/misc/1.jpg>

FLAG在哪里??

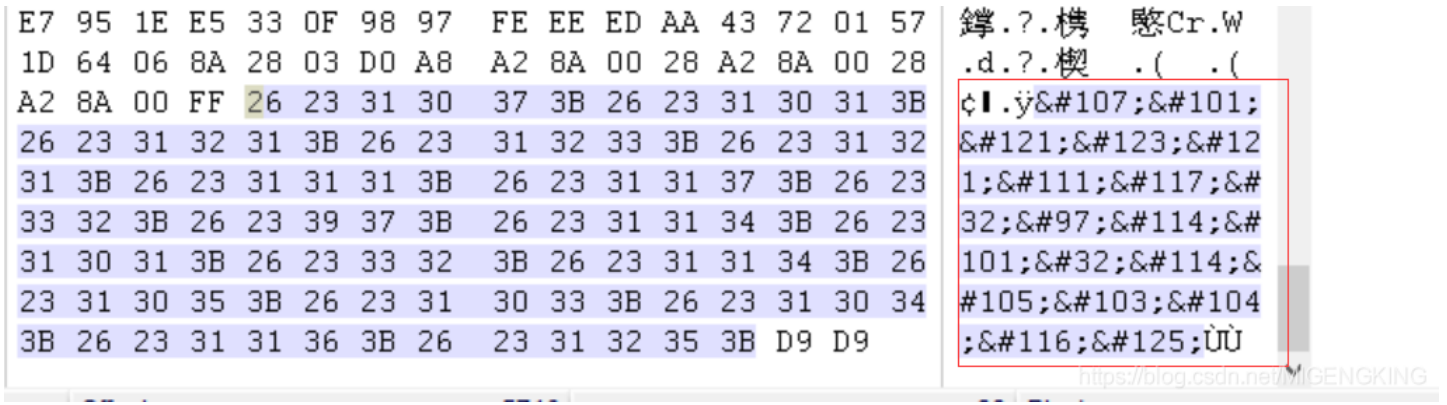
Flag

Submit

<https://blog.csdn.net/MIGENKING>



题目显示为".jpg"文件，打开题目为一张什么都没有的图片，要联想到图片隐写，，，，  
 下载图片后，用winhex软件（因为题目显示为.jpg文件）打开文件后，  
 发现一组明显的加密编码，，，，



由“&#+ASCII+;”组成上网查了是  
 网页中&#开头的是HTML实体，一些字符在 HTML 中是预留的，拥有特殊的含义  
 汉字的HTML实体由三部分组成，“&#+ASCII+;”即可。  
 字符实体有三部分：一个和号 (&)，一个实体名称，或者 # 和一个实体编号，以及一个分号 (?  
 然后就试着去解码：

# 在线Unicode编码解码

[全屏显示](#)[获取代码](#)[URL网址](#)[UTF-8](#)[Unicode](#)[ASCII](#)

文字:

key{you are right}

编码 >

< 解码

Unicode:

&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;

<https://blog.csdn.net/MIGENKING>

Unicode（统一码、万国码、单一码）是一种在计算机上使用的字符编码。Unicode是为了解决传统的字符编码方案的局限而产生的，它为每种语言中的每个字符设定了统一并且唯一的二进制编码，以满足跨语言、跨平台进行文本转换、处理的要求

图片隐写二：

Challenge

5485 Solves

×

# 隐写 50

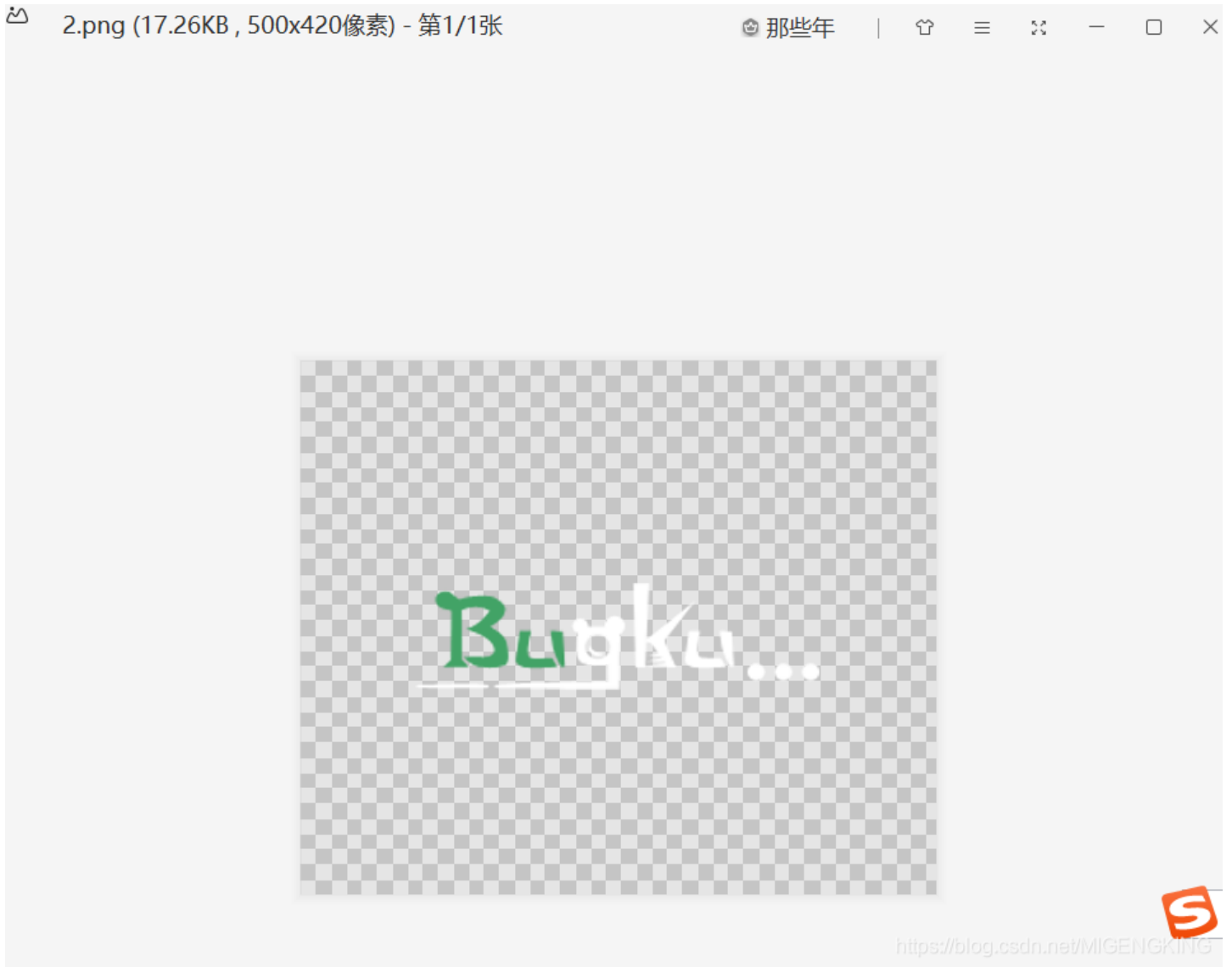
2.rar

Flag

Submit

<https://blog.csdn.net/MIGENKING>

下载好文件后是一张图片：



因为是“.png”文件，一般这种情况图片的隐写很有可能，于是把图片放进“winhex”,“HxD”查看图片代码

HxD - [D:\2\2\2.png]

文件(F) 编辑(E) 搜索(S) 视图(V) 分析(A) 工具(T) 窗口(W) 帮助(H)

16 Windows (Alt) 十六进制

2.png

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52
00000010	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DE
00000020	8A	00	00	09	70	48	59	73	00	09	12	74	00	00	12	
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A

规定八个字节为png的文件头      四个字节，字母‘D’为十六进制的13代表数据长度

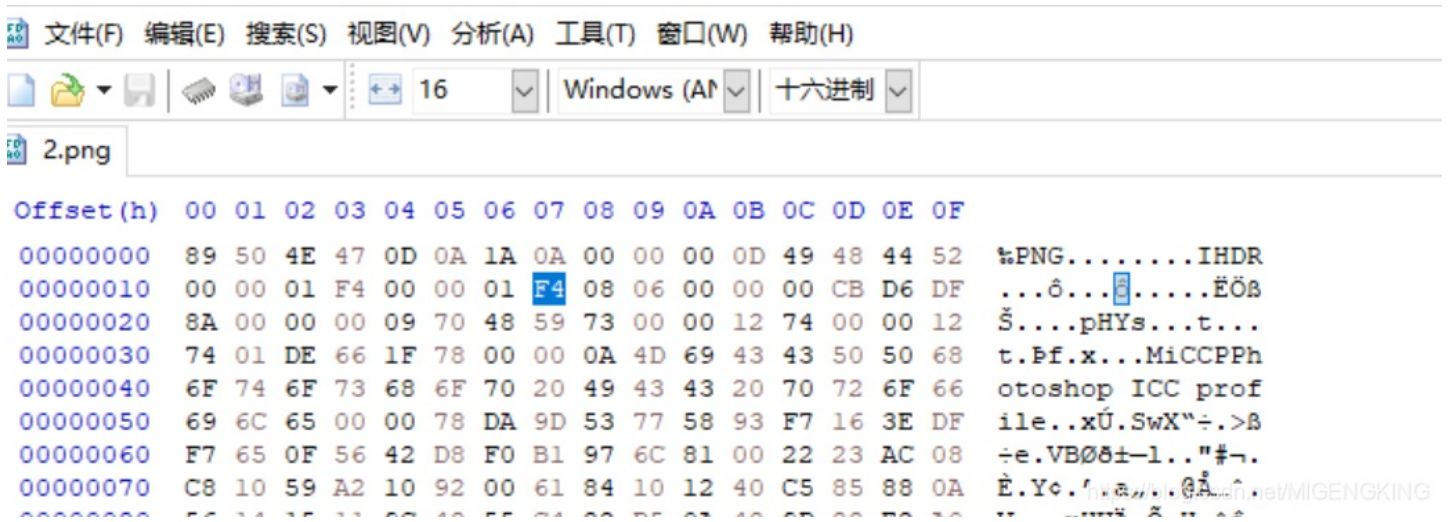
图片的宽      图片的高

PNG.....IHDR  
 ...ô...¸.....ËÖß  
 Š...pHYs...t...  
 t.¸f.x...MiCCPPh  
 otoshop ICC prof  
 ile...xÛ.SwX"÷.>ß  
 ÷e.VBØð±-1.."#-.  
 È.Ye.¸.a...@Ä.../MIGENKING

- (固定) 八个字节89 50 4E 47 0D 0A 1A 0A为png的文件头
- (固定) 四个字节00 00 00 0D 代表数据块的长度为13
- (固定) 四个字节49 48 44 52 (即为ASCII码的IHDR) 是文件头数据块的标示 (IDCH)
- (可变) 13位数据块 (IHDR)

- 前四个字节代表该图片的宽 00 00 01 F4
- 后四个字节代表该图片的高 00 00 01 A4

因为图片可能是高度不够 (做题经验) 所以直接把图片的高改成和宽度一样再保存 (图片如果是只读文件要在图片属性上去掉)



改好保存，图片就出现flag

