ctfshow - PNG隐写入门赛

原创

H3rmesk1t 于 2021-09-13 13:58:31 发布 217 收藏 1

分类专栏： Misc 文章标签： ctfshow Misc PNG 隐写 LSB

ctfshow - PNG隐写入门赛

前言

> - 题目下载链接

1. 本场比赛共有18题，但只有1个附件文件（见第1题），所有flag均可以从附件中获取；
2. 所有的flag开头和结尾均为#，中间由字母、数字或下划线组成；
3. 本场比赛不使用任何*可以*设置密码的隐写方法，包括可以将密码留空的隐写方法；
4. 原理类似的隐写方法在确保不互相干扰的前提下可能会以多种方式使用；
5. 如果从附件提取的隐写信息为字符串形式，可能需要转码得到指定格式的结果；
6. 如果从附件提取的隐写信息为另一张图片，该图片不会再包含隐写信息，即不存在套娃隐写；
7. 所使用的字体均为微软雅黑，若有字符无法分辨，请与字体对比查看；
8. 取得类似#abcd_1234#的字符串后，请计算其MD5值（包含头尾的#号）；
9. 每道题目都给出了一段MD5值，请找到MD5值匹配的题目后，将flag包上ctfshow{}格式提交。

One PieNG 1

- 图片的名字就是 `One PieNG 1` 的 Flag： `ctfshow{#St4rt_fr0m_th1s_5tr1ng#}`

One PieNG 2

- 图片上面直接给出了 `One PieNG 2` 的 Flag： `ctfshow{#Th1s_i5_s0_34sy!!!#}`

One PieNG 3

- 用蜂蜜浏览器查看图片时发现载入失败，猜测图片的宽高可能有问题，将图片修复后拿到 `One PieNG 3` 的 Flag： `ctfshow{#Pn9_He1gh7_6e_ch4ng3d#}`

#Pn9_He1gh7_6e_ch4ng3d#

One PieNG 4

- 尝试将图片的高度再拉大点，发现了 `One PieNG 4` 的 Flag：`ctfshow{#M4yb3_we_sh0uld_9o_d33per#}`

#Pn9_He1gh7_6e_ch4ng3d#

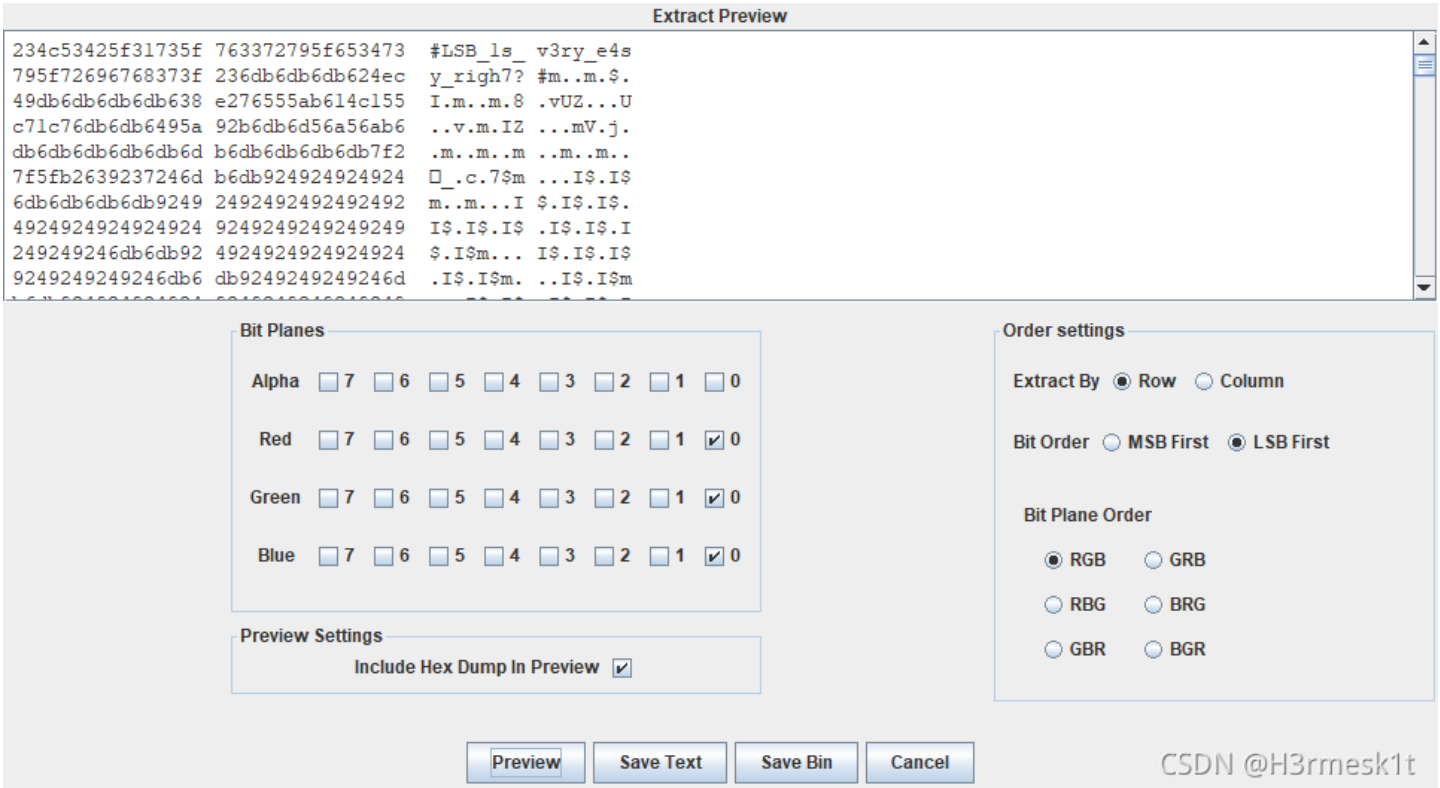
#M4yb3_we_sh0uld_9o_d33per#

One PieNG 5

- 用 `stegsolve` 查看图片，在 Blue 通道的最低位发现 Flag：`ctfshow{#You_st3gs0lved_me!!!#}`

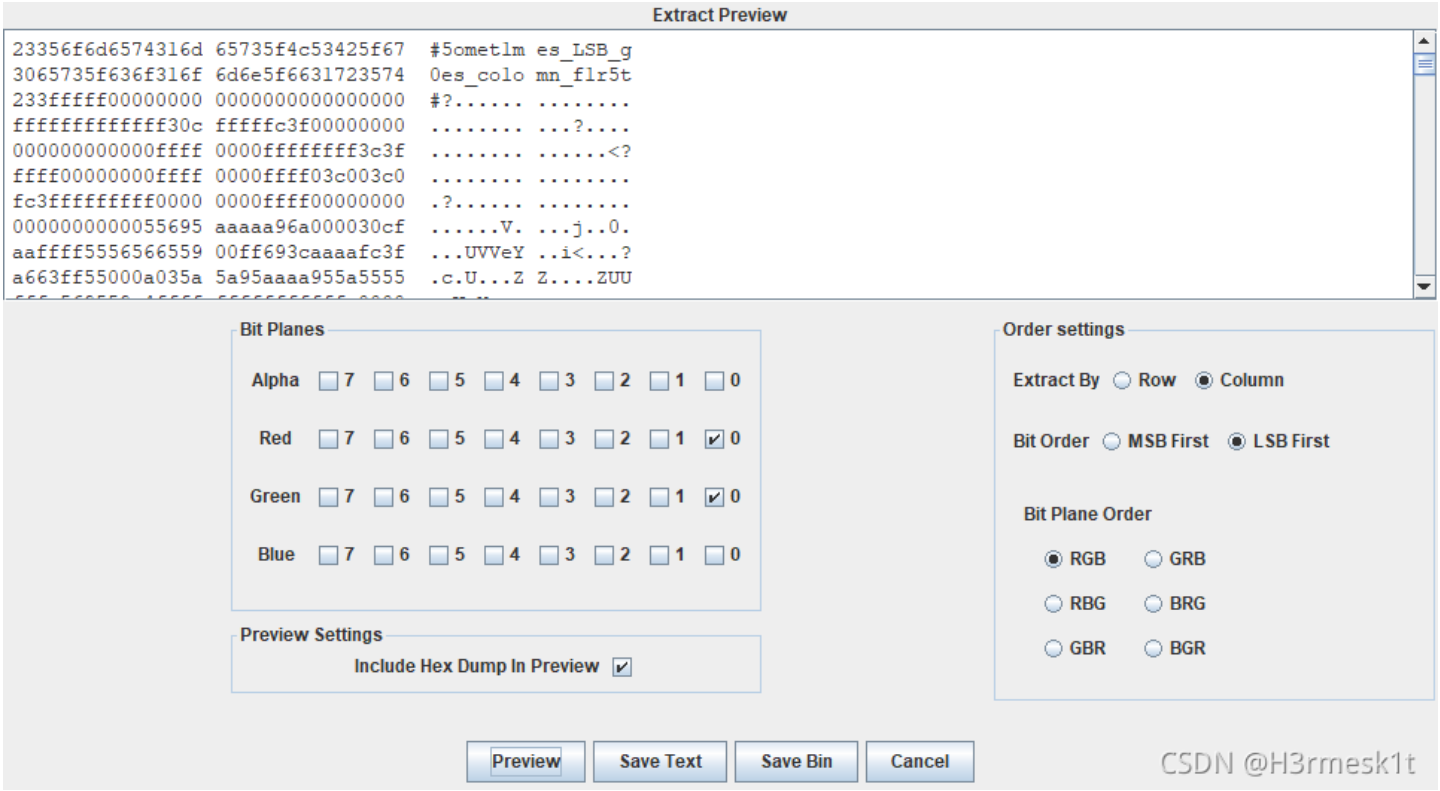
One PieNG 6

- 用 `stegsolve` 查看图片，在 RGB 三通道最低位发现 Flag：`ctfshow{#LSB_1s_v3ry_e4sy_righ7?#}`



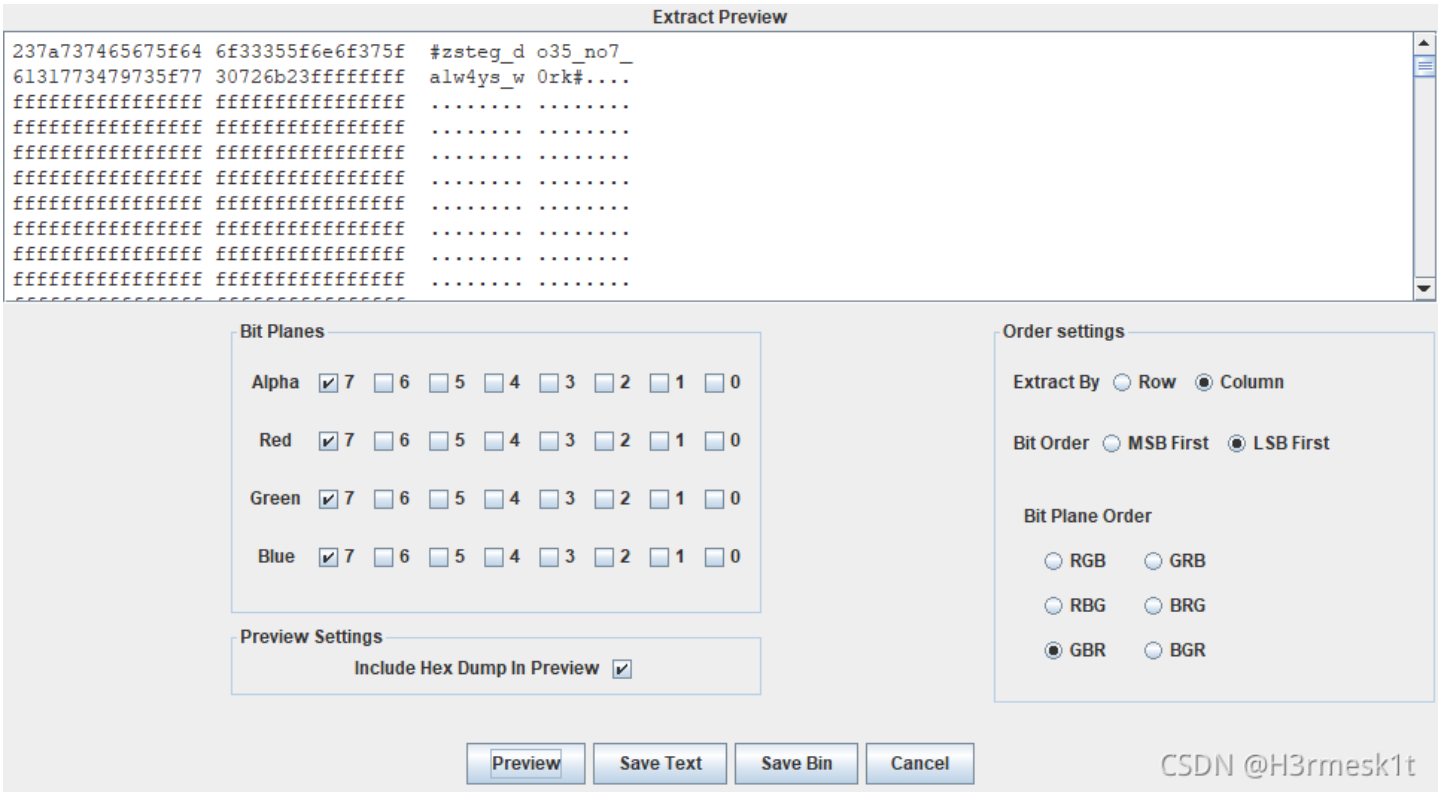
One PieNG 7

- 用 `stegsolve` 查看图片，在 RG 两通道最低位发现 Flag：`ctfshow{#5omet1mes_LSB_g0es_co1omn_f1r5t#}`



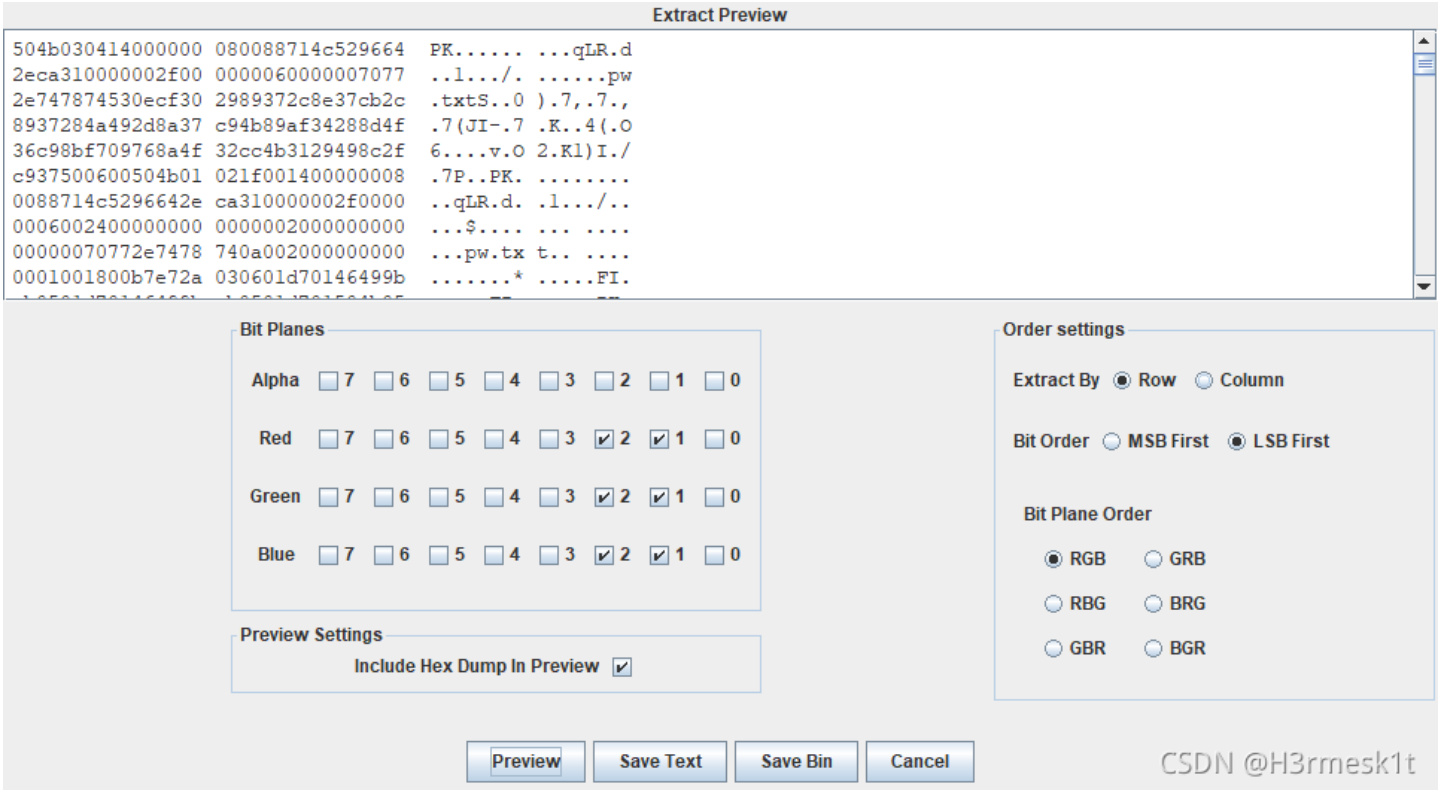
One PieNG 8

- 用 `stegsolve` 查看图片，发现 R,G,B,A 通道都能看到左上角有问题，在最高位发现
  Flag：`ctfshow{#zsteg_do35_no7_a1w4ys_w0rk#}`



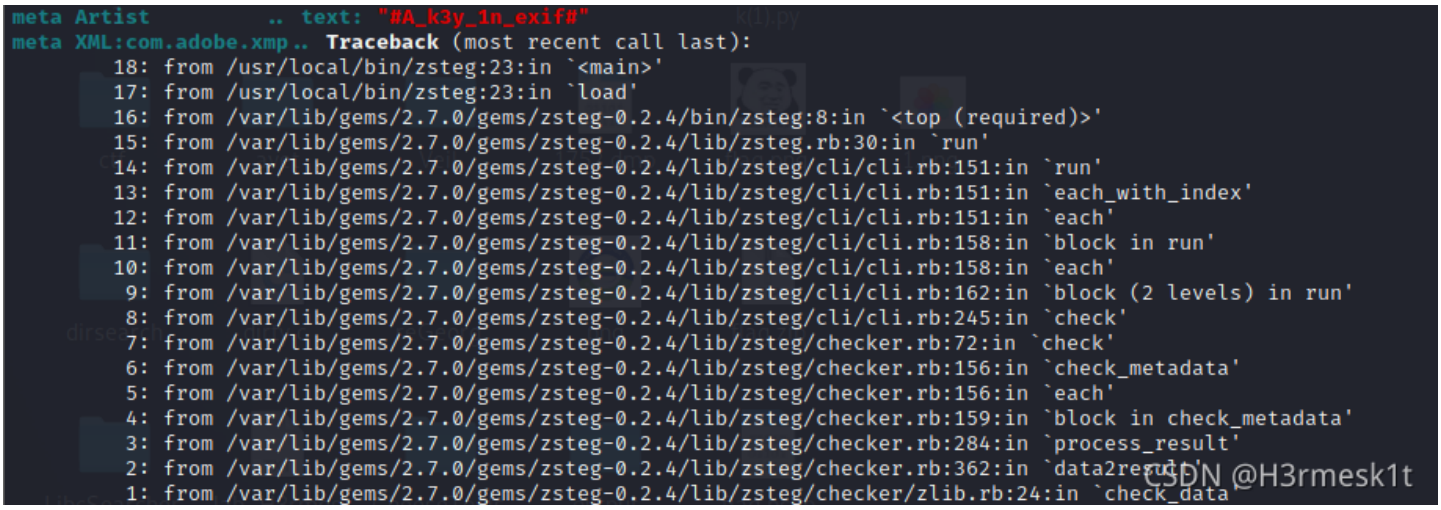
One PieNG 9

- 用 `stegsolve` 查看图片，提取 RGB 的 1,2 通道，得到一个压缩包，将其 `save bin` 保存下来后打开发现
  Flag：`ctfshow{#Wh4t_1s_6it_0rder_4nd_y0u_c4n_LSB_b1nd4ta_to0#}`



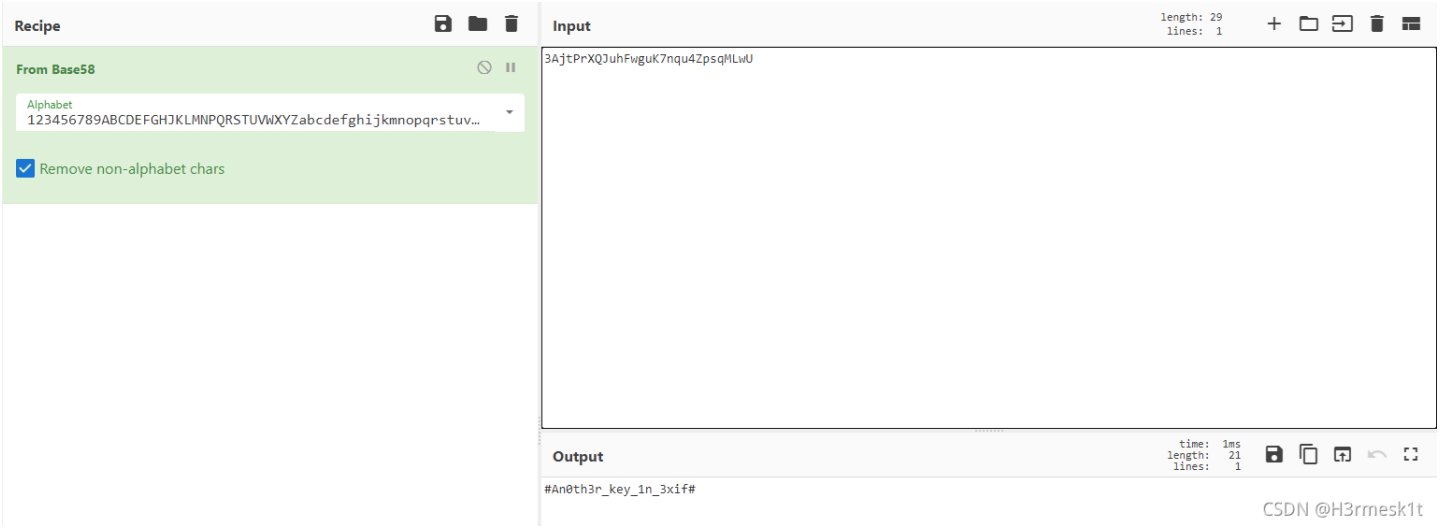
One PieNG 10

- 用 `zsteg` 查看图片发现 `One PieNG 10` 的 Flag：`ctfshow{#A_k3y_1n_exif#}`



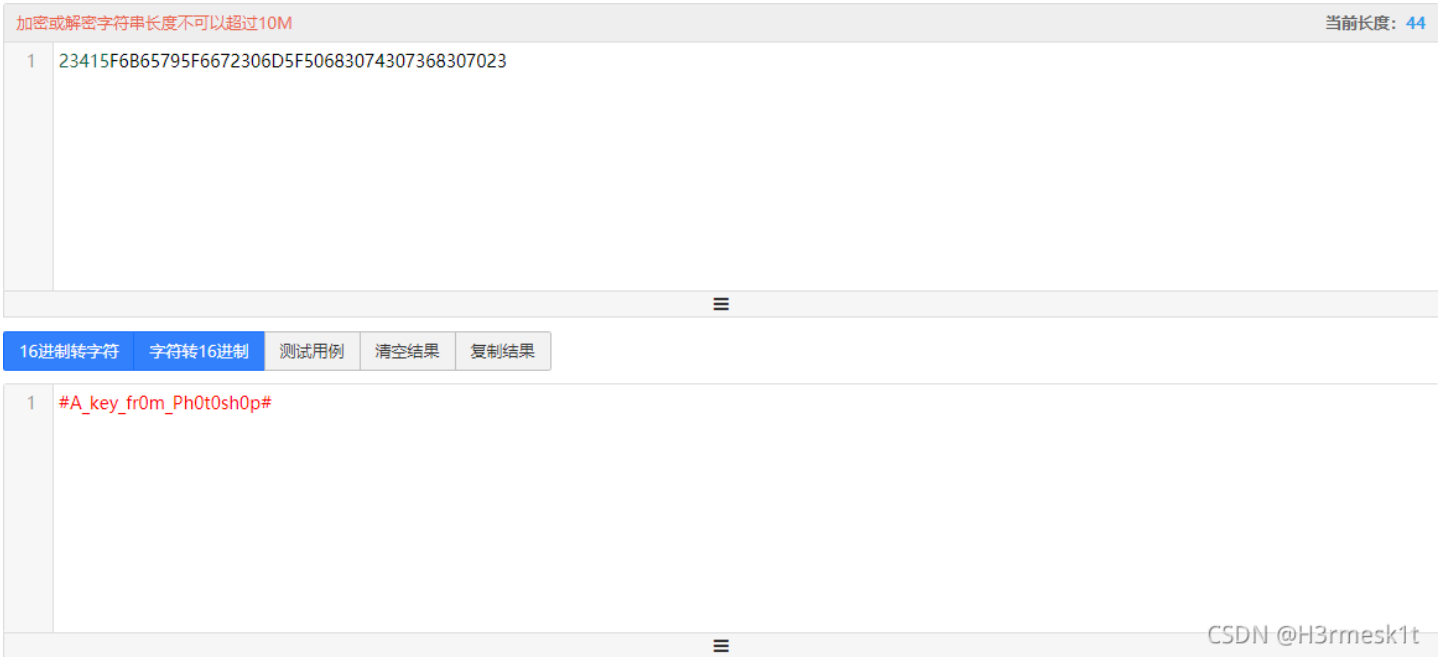
One PieNG 11

- 根据 `One PieNG 10` Flag 内容的提示，查看一下图片的 EXIF，将 `City` 选项 base58 解密拿到 `One PieNG 11` 的 Flag：`ctfshow{#An0th3r_key_1n_3xif#}`



One PieNG 12

- 根据 `One PieNG 10` Flag 内容的提示，查看一下图片的 EXIF，将 `Document Ancestors` 选项十六进制转字符串拿到 `One PieNG 12` 的 Flag：`ctfshow{#A_key_fr0m_Ph0t0sh0p#}`



One PieNG 13

- 用 010editor 打开，查看每一个块，发现 `One PieNG 13` 的 Flag：`ctfshow{#Ju5t_a_1one1y_tEXt_chunk#}`

One PieNG 14

- 由于 `zsteg` 提示数据块异常，用 `pngdebuger` 跑一下，发现九个出错的数据块，先将其提取出来，将图片的这九个数据块删去，拿到 `One PieNG 14` 的 Flag： `ctfshow{#eXtr4_IDAT_of_an0th3r_Pn9#}`

```
>> (CRC CHECK)  crc-computed=0xD915B16A        =>     CRC OK!

0x0000028D      chunk-length=0x00010000 (65536)
0x00000291      chunk-type='IDAT'
0x00010295      crc-code=0x00234831
>> (CRC CHECK)  crc-computed=0x94F55588        =>     CRC FAILED

0x00010299      chunk-length=0x00010000 (65536)
0x0001029D      chunk-type='IDAT'
0x000202A1      crc-code=0x0064655F
>> (CRC CHECK)  crc-computed=0xBA2406E1        =>     CRC FAILED

0x000202A5      chunk-length=0x00010000 (65536)
0x000202A9      chunk-type='IDAT'
0x000302AD      crc-code=0x00683378
>> (CRC CHECK)  crc-computed=0xCD6A57C7        =>     CRC FAILED

0x000302B1      chunk-length=0x00010000 (65536)
0x000302B5      chunk-type='IDAT'
0x000402B9      crc-code=0x00643437
>> (CRC CHECK)  crc-computed=0x9EC196CD        =>     CRC FAILED

0x000402BD      chunk-length=0x00010000 (65536)
0x000402C1      chunk-type='IDAT'
0x000502C5      crc-code=0x00615F31
>> (CRC CHECK)  crc-computed=0x1D1C51CC        =>     CRC FAILED

0x000502C9      chunk-length=0x00010000 (65536)
0x000502CD      chunk-type='IDAT'
0x000602D1      crc-code=0x006E5F63
>> (CRC CHECK)  crc-computed=0xD41FCAD9        =>     CRC FAILED

0x000602D5      chunk-length=0x00010000 (65536)
0x000602D9      chunk-type='IDAT'
0x000702DD      crc-code=0x0068756E
>> (CRC CHECK)  crc-computed=0x655D563D        =>     CRC FAILED

0x000702E1      chunk-length=0x00010000 (65536)
0x000702E5      chunk-type='IDAT'
0x000802E9      crc-code=0x006B5F43
>> (CRC CHECK)  crc-computed=0xCB1875FD        =>     CRC FAILED

0x000802ED      chunk-length=0x00002646 (9798)
0x000802F1      chunk-type='IDAT'
0x0008293B      crc-code=0x00524323
>> (CRC CHECK)  crc-computed=0x19FE70D3        =>     CRC FAILED

0x0008293F      chunk-length=0x00000024 (36)
0x00082943      chunk-type='tXEt'
0x0008296B      crc-code=0x2D6EA7AB
>> (CRC CHECK)  crc-computed=0x2D6EA7AB        =>     CRC OK!
```


One PieNG 15

- 由于 `binwalk` 发现了异常数据块，将其分离出来查看，发现 `One PieNG 15` 的 Flag： `ctfshow{#IDAT_i5_a_z1ib_p4cka9e#}`

```
 kali@kali  ~/Desktop/_1.png.extracted  ls
1EC247  1EC247.zlib  1EC2BB  1EC2BB.zlib  295  295.zlib  82977  82977.zlib
 kali@kali  ~/Desktop/_1.png.extracted  cat 1EC247
#IDAT_i5_a_z1ib_p4cka9e#%
 kali@kali  ~/Desktop/_1.png.extracted
```

One PieNG 16

- 发现前面提取出来的出错的 CRC 数据块拼接起来和之前的十六进制很像，转一下拿到 `One PieNG 16` 的 Flag： `ctfshow{#H1de_h3xd47a_1n_chunk_CRC#}`

加密或解密字符串长度不可以超过10M 当前长度：54

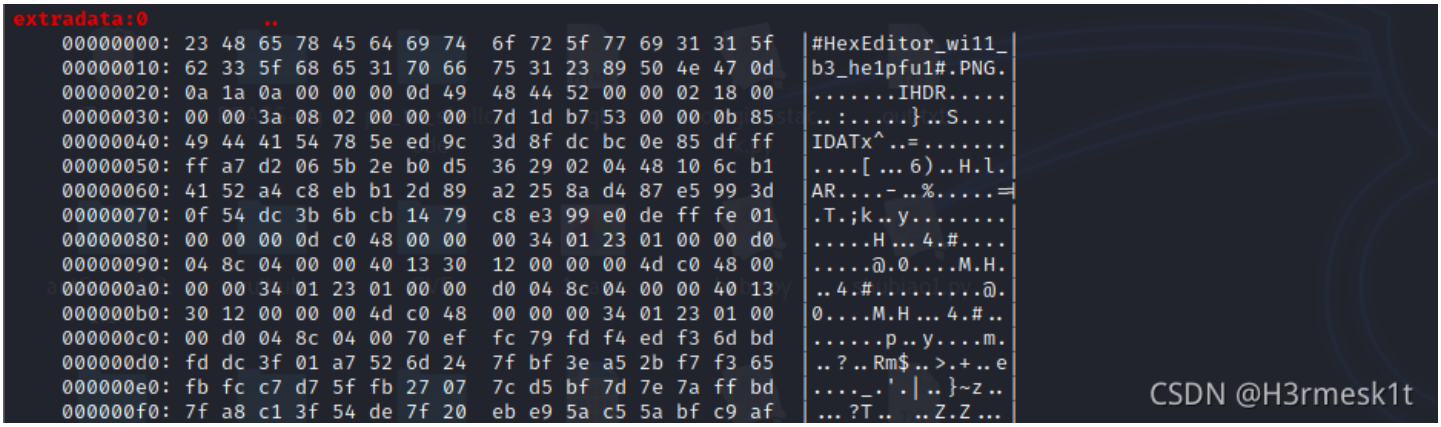
```
23483164655F683378643437615F316E5F6368756E6B5F43524323
```

16进制转字符 | 字符转16进制 | 测试用例 | 清空结果 | 复制结果

```
#H1de_h3xd47a_1n_chunk_CRC#
```


One PieNG 17

- 用 `zsteg` 查看图片发现 `One PieNG 17` 的 Flag：`ctfshow{#HexEditor_wi11_b3_he1pfu1#}`



One PieNG 18

- `binwalk` 发现还有一张图片，分离出来上面的内容就是 `One PieNG 18` 的 Flag：`ctfshow{#He110_I_4m_Tw0_PieNG#}`

#He110_I_4m_Tw0_PieNG#

One PieNG问卷调查

> - 没意思

ctfshow{套娃终有报，天道好轮回。不信抬头看，苍天饶过谁。}
