




# PNG隐写入门赛 WP

原创

秦颖诗  于 2021-05-28 21:09:40 发布  285  收藏 3

分类专栏: [ctf wp](#) 文章标签: [安全 wp](#)

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/xiaopangding09/article/details/117370965>

版权



[ctf wp](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

一篇思路乱七八糟的wp

这个比赛是大概3月份ctfshow的一个比赛, 额, 最近在复盘之前各个比赛, 比较菜, 请见谅。

- 0、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;
- 1、所有的flag开头和结尾均为#, 中间由字母、数字或下划线组成;
- 2、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;
- 3、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;
- 4、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;
- 5、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;
- 6、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;
- 7、取得类似#abcd\_1234#的字符串后, 请计算其MD5值(包含头尾的#号);
- 8、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。

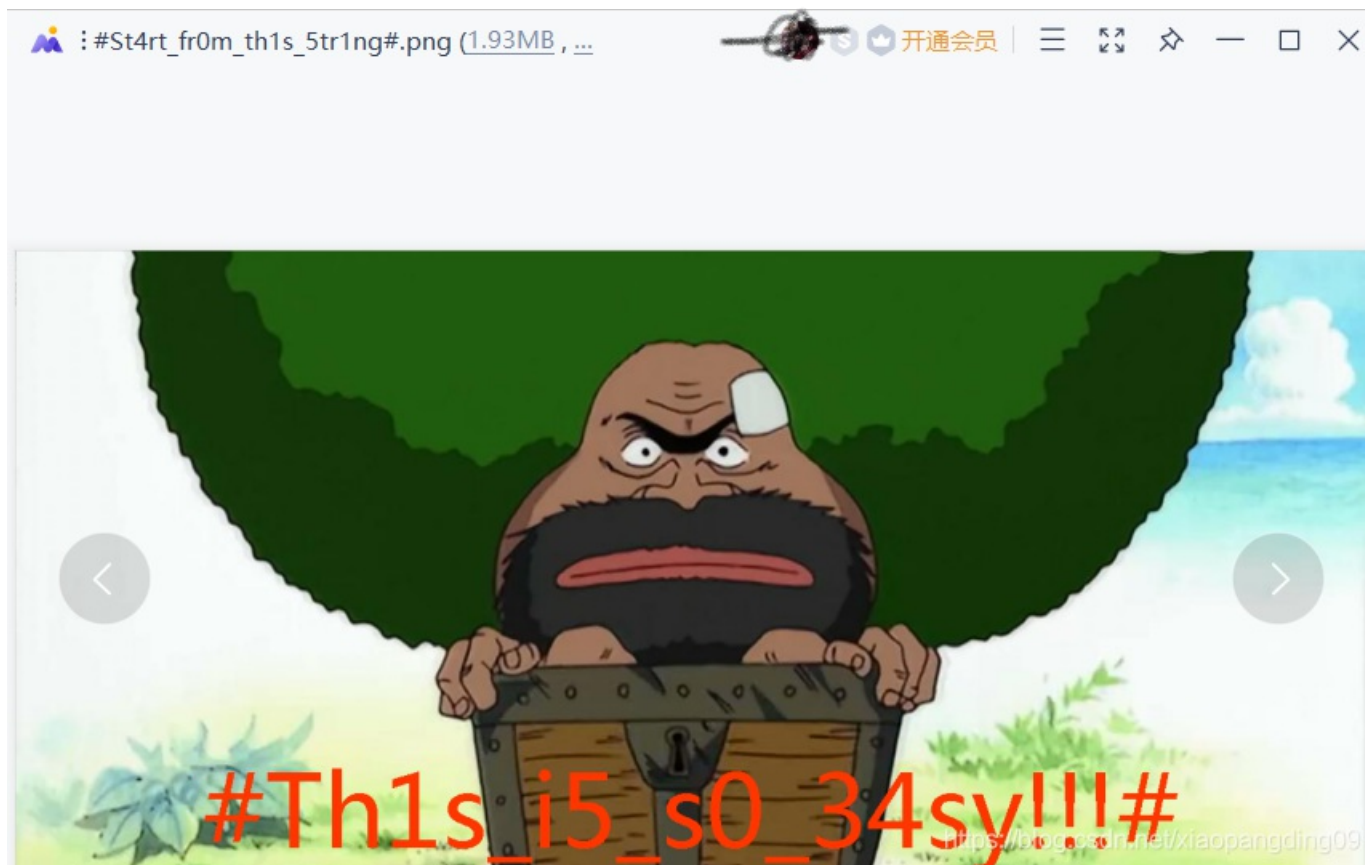
两个在线MD5网址: (有脚本的话可忽略)

[MD5](#)

[在线MD5](#)

One PieNG 1:

附件下载后是一张照片，照片命名#St4rt\_fr0m\_th1s\_5tr1ng#.png,符合要求字符串，MD5检测为342f08112d4ffb0577f49e89a2a18fa2，和1一致，所以是flag



```
ctfshow{#St4rt_fr0m_th1s_5tr1ng#}
```

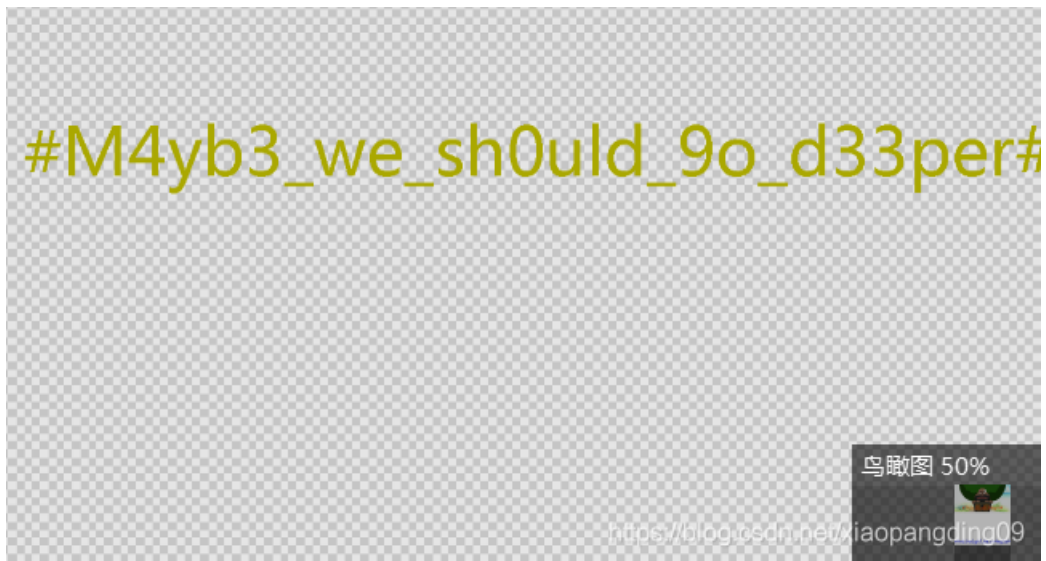
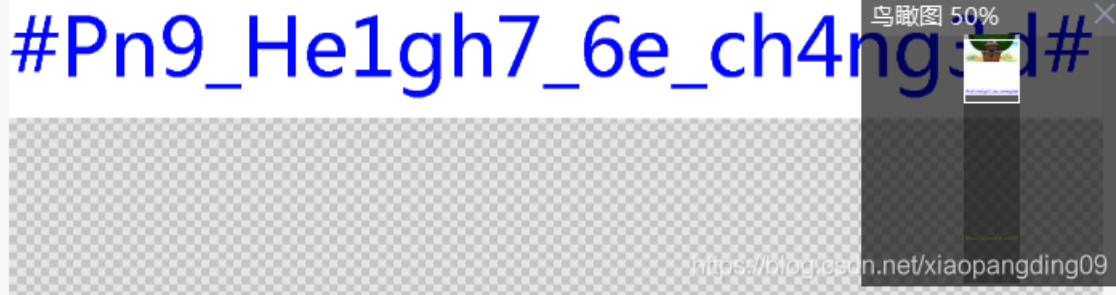
One PieNG 2:

打开图片，参照上面的图片，发现照片中有一个flag,进行MD5检测为d64fc33636dda50babdde6b775d8cf10，和2的一致。

```
ctfshow{#Th1s_i5_s0_34sy!!!#}
```

One PieNG 3 + One PieNG 4:

看属性，看图片的高和宽不相同，拖进010改高9000发现图片中又多了两个flag



分别检测MD5值，8b8bc8c6aa81e7b955660fba3575af63和c35bc750588f620f49e83493f4125bfd发现和3、4的一致。

```
One PieNG 3: ctfshow{#Pn9_He1gh7_6e_ch4ng3d#}
One PieNG 4: ctfshow{#M4yb3_we_sh0uld_9o_d33per#}
```

One PieNG 5:

图片隐写肯定少不了stegsolve，B通道最低位隐写，MD5检测91848bee27655dc0da45006f467a59fb，一致



```
ctfshow{#You_st3gs0lved_me!!!#}
```

One PieNG 6:

stegsolve的Date extract选RGB的0通道,MD5:335b63183f19e4fe1b9bd734af81403e,一致

The screenshot shows the StegSolve interface. At the top, there is a table with three columns: hex data, hex data, and ASCII characters. The hex data is: 25f31735f 763372795f653473 #LSB\_1s\_v3ry\_e4s, 96768373f 236db6db6db624ec y\_righ7? #m..m.\$., 5db6db638 e276555ab614c155 I.m..m.8 .vUZ...U, 06db6495a 92b6db6d56a56ab6 ..v.m.IZ ...mV.j., 06db6db6d b6db6db6db6db7f2 .m..m..m ..m..m.., 39237246d b6db924924924924 □.c.7\$m ...I\$.I\$, db6db9249 2492492492492492 m..m..I \$.I\$.I\$, 924924924 924924924924924 I\$.I\$.I\$.I\$.I\$.I\$.I, 16db6db92 4924924924924924 \$.I\$m... I\$.I\$.I\$, 249246db6 db9249249249246d .I\$.I\$m. ..I\$.I\$m. Below the table is a grid of bit planes for channels 'a', 'd', 'en', and 'e'. Each channel has checkboxes for bits 7 through 0. For 'd', 'en', and 'e', bit 0 is checked. To the right, the 'Order settings' panel shows 'Extract By' set to 'Column', 'Bit Order' set to 'LSB First', and 'Bit Plane Order' set to 'RGB'. A watermark 'https://blog.csdn.net/xiaopangding09' is visible at the bottom of the interface.

ctfshow{#LSB\_1s\_v3ry\_e4sy\_righ7?#}

One PieNG 7:

感觉在column可能有,尝试通道,在RG通道找到flag.MD5:e18d9aa18b35ae3a702875beab14cc86,一致

The screenshot shows the StegSolve interface. At the top, there is a table with three columns: hex data, hex data, and ASCII characters. The hex data is: 3425f67 #5omet1m es\_LSB\_g, 1723574 0es\_colo mn\_f1r5t, 0000000 #?....., 0000000 .....?...., fff3c3f .....<?, 3c003c0 ..... , 0000000 .?....., 00030cf .....V. ...j..0., aaafc3f ...UVVeY ..i<...?, 55a5555 .c.U...Z Z....ZUU. Below the table is a grid of bit planes for channels '3', '2', '1', and '0'. Each channel has checkboxes for bits 3 through 0. For channel '0', bit 0 is checked. To the right, the 'Order settings' panel shows 'Extract By' set to 'Column', 'Bit Order' set to 'LSB First', and 'Bit Plane Order' set to 'RGB'. A watermark 'https://blog.csdn.net/xiaopangding09' is visible at the bottom of the interface.

ctfshow{#5omet1mes\_LSB\_g0es\_co1omn\_f1r5t#}

One PieNG 8:

R,G,B,A通道7通道都能看到左上角有异常，

The screenshot displays the PieNG 8 interface. At the top, the title bar reads "Extract Preview". Below it is a hex dump with the following content:

```
7465675f64 6f33355f6e6f375f #zsteg_d o35_no7_  
3479735f77 30726b23fffffffff alw4ys_w 0rk#....  
fffffffffff ffffffffffffffff .....
```

The interface is divided into several sections:

- Planes:** A section with four rows, each representing a color channel (Alpha, Red, Green, Blue). Each row has checkboxes for bit planes 7 through 0. All checkboxes for bit planes 7 through 0 are checked for all channels.
- Order settings:** A section with two main options: "Extract By" (Row or Column) and "Bit Order" (MSB First or LSB First). "Column" and "MSB First" are selected. Below this is a "Bit Plane Order" section with options: RGB, GRB, RBG, BRG, GBR, and BGR. "GBR" is selected.
- View Settings:** A section at the bottom left with a checkbox "Include Hex Dump In Preview" which is checked.

A watermark URL is visible at the bottom right: <https://blog.csdn.net/xiaopangding09>

MD5检测8d4ae0eed967e9936ee5373f0f58829c和8一致

```
ctfshow{#zsteg_do35_no7_a1w4ys_w0rk#}
```

One PieNG 9:

看0通道的左上角的LSB隐写长度，发现1、2通道明显长

0:



1、2:



**Extract Preview**

```

04b030414000000 080088714c529664 PK..... .qLR.d
eca31000002f00 0000060000007077 ..1.../. .....pw
e747874530ecf30 2989372c8e37cb2c .txtS..0 ).7,.7.,
937284a492d8a37 c94b89af34288d4f .7(JI-.7 .K..4(.O
6c98bf709768a4f 32cc4b3129498c2f 6...v.O 2.K1)I./
937500600504b01 021f001400000008 .7P..PK. ....
088714c5296642e ca310000002f0000 ..qLR.d. .1.../..
006002400000000 0000002000000000 ...$. ... ..
0000070772e7478 740a002000000000 ...pw.tx t. ....
001001800b7e72a 030601d70146499b .....* .....FI.

```

**Bit Planes**

Alpha  7  6  5  4  3  2  1  0

Red  7  6  5  4  3  2  1  0

Green  7  6  5  4  3  2  1  0

Blue  7  6  5  4  3  2  1  0

**Order settings**

Extract By  Row  Column

Bit Order  MSB First  LSB First

Bit Plane Order

RGB  GRB

1、2通道提取PK文件

解压的txt:



<https://blog.csdn.net/xiaopangding09>

MD5检测 9734a5d18504ef6a31c2c104b224f0df与9一致

```
ctfshow{#Wh4t_1s_6it_Order_4nd_y0u_c4n_LSB_b1nd4ta_to0#}
```

One PieNG 10:

用010打开在文本头发现

```
44 52 %PNG.....IHDR
21 2A ...V...p.....«!*
74 00 S....tEXtArtist.
23 7F #A_k3y_1n_exif#.
3A 63 uAa...>iTtXML:c
00 00 om.adobe.xmp....
```

MD5检测 cec1969402261bd550f1b3d0c0ccc655和10一致

```
ctfshow{#A_k3y_1n_exif#}
```

One PieNG 11 + One PieNG 12:

EXIF查看: [EXIF查看](#)

又多了两个flag

## XMP-photoshop

DocumentAncestors	23415F6B65795F6672306D5F50683074307368307023
城市	b58/3AjtPrXQJuhFwguK7nqu4ZpsqMLwU

第一个:16进制转字符:

加密或解密字符串长度不可以超过10M

1	23415F6B65795F6672306D5F50683074307368307023
---	--

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

## 服务器租用低至5.9折

小鸟云服务器,纯SSD架构,弹性扩容,免费5G防御,0元免费备案,

1 #A\_key\_fr0m\_Ph0t0sh0p#

<https://blog.csdn.net/xiaopangding09>

MD5检测 fba2e6b912ab1a308c6b1438da31fbb8和12一致

第二个: base58

转换前:

3AjtPrXQJuhFwguK7nqu4ZpsqMLwU

编码Base58>

解码Base58>

转换后:

#An0th3r\_key\_1n\_3xif#

<https://blog.csdn.net/xiaopangding09>

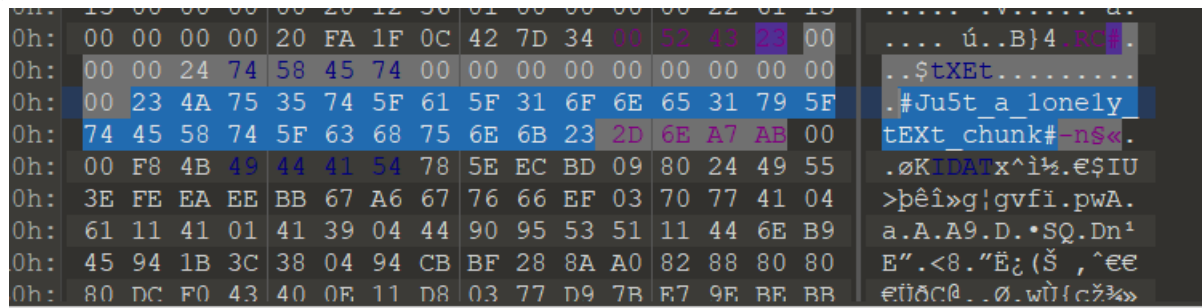
MD5检测3e703086b0e2585eff041cbd186f1bd4和11一致



One PieNG 12: ctfshow{#An0th3r\_key\_1n\_3xf#}  
 One PieNG 11 :ctfshow{#A\_key\_fr0m\_Ph0t0sh0p#}

One PieNG 13:

010变量窗口



果 - PNG.bt

名称	值	开始	大小	颜色	注释
ct PNG_SIGNATURE sig		0h	8h	Fg: Bg:	
ct PNG_CHUNK chunk[0]	IHDR (Critic...	8h	19h	Fg: Bg:	
ct PNG_CHUNK chunk[1]	tEXt (Ancil...	21h	22h	Fg: Bg:	
ct PNG_CHUNK chunk[2]	iTXt (Ancil...	43h	24Ah	Fg: Bg:	
ct PNG_CHUNK chunk[3]	IDAT (Critic...	28Dh	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[4]	IDAT (Critic...	10299h	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[5]	IDAT (Critic...	202A5h	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[6]	IDAT (Critic...	302B1h	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[7]	IDAT (Critic...	402BDh	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[8]	IDAT (Critic...	502C9h	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[9]	IDAT (Critic...	602D5h	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[10]	IDAT (Critic...	702E1h	1000Ch	Fg: Bg:	
ct PNG_CHUNK chunk[11]	IDAT (Critic...	802EDh	2652h	Fg: Bg:	
ct PNG_CHUNK chunk[12]	tXEt (Ancil...	8293Fh	30h	Fg: Bg:	
ct PNG_CHUNK chunk[13]	IDAT (Critic...	8296Fh	F857h	Fg: Bg:	
ct PNG_CHUNK chunk[14]	IDAT (Critic...	921C6h	10000h	Fg: Bg:	
ct PNG_CHUNK chunk[15]	IDAT (Critic...	A21C6h	10000h	Fg: Bg:	

MD5检测 23e4464f1b458a062fb13e155a72f999和13一致

ctfshow{#Ju5t\_a\_l0nely\_tEXt\_chunk#}

One PieNG 14:

检查IDAT块

用PNGdebugger跑了一下



使用tweakpng删掉前面出错的9个IDAT块.,保存

#St4rt\_fr0m\_th1s\_5tr1ng#.png (C:\Users\17120\Desktop\ctf题) - Tw...

Chunk	Length	CRC	Attributes	Contents
IHDR	13	692a1...	critical	PNG image header: 1366×663, 8 bits/sampl
tEXt	22	7fac3...	ancillary, safe to c...	text, key="Artist" (nonstandard): "#A_k3y_1n
iTXt	574	d915b...	ancillary, safe to c...	text (international), key="XML:com.adobe.xn
IDAT	65536	94f555...	critical	PNG image data
IDAT	65536	ba240...	critical	PNG image data
IDAT	65536	cd6a5...	critical	PNG image data
IDAT	65536	9ec19...	critical	PNG image data
IDAT	65536	1d1c5...	critical	PNG image data
IDAT	65536	d41fca...	critical	PNG image data
IDAT	65536	655d5...	critical	PNG image data
IDAT	65536	cb187...	critical	PNG image data
IDAT	9798	19fe70...	critical	PNG image data

<https://blog.csdn.net/xiaopangding09>



MD5检测 d325d41389ddb0c3fdec30e51565fda3和14一致

ctfshow{#eXtr4\_IDAT\_of\_an0th3r\_Pn9#}

One PieNG 15:

拖到kali2020中binwalk发现有东西, binwalk -e分离

翻分离的东西



MD5检测ad9d95f270d91aed3ba2203487bf01cd和15一致

```
ctfshow{#IDAT_i5_a_z1ib_p4cka9e#}
```

One PieNG 16:

这个是真的没看出来, 看了大佬的WP才明白, 是之前出错的IDAT都是00开头, 后面几乎都是6, 并且是16进制, 转ASCII

加密或解密字符串长度不能超过10M

```
1 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

**服务器租用低至5.9折**  
小鸟云服务器,纯SSD架构,弹性扩容,免费5G防御,0元免费备案,7\*24H技术运

```
1 #H1de_h3xd47a_1n_chunk_CRC#
```

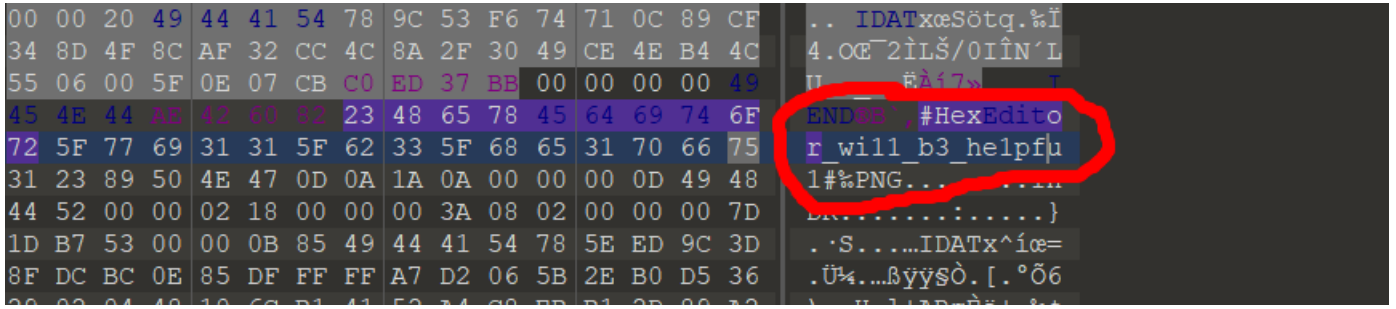
<https://blog.csdn.net/xiaopangding09>

MD5:7dc6506ac3d4c7a99587c9b3cbf43798与16一致

```
ctfshow{#H1de_h3xd47a_1n_chunk_CRC#}
```

One PieNG 17:

用010打开在文本尾发现

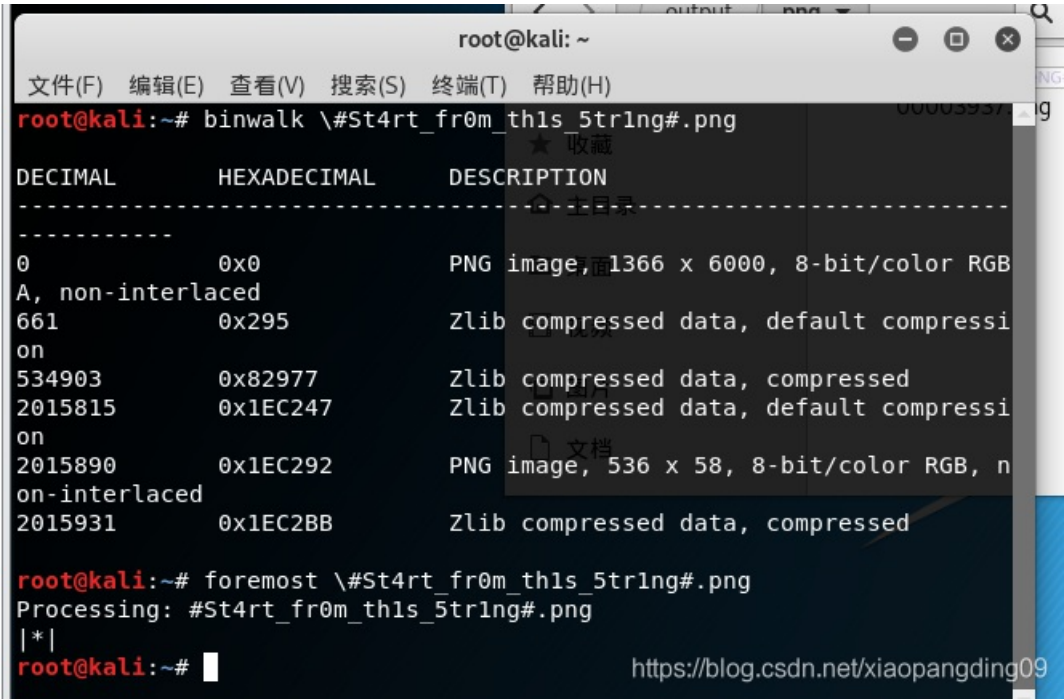


MD5检测170cee5e9bd6dd81021d8533490a4b8b与17一致

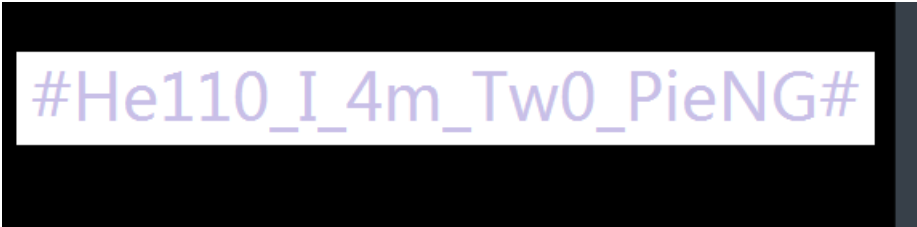
```
ctfshow{#HexEditor_wi11_b3_he1pfu1#}
```

One PieNG 18:

拖到kali2019中binwalk发现有东西, foremost分离



发现是一张图片



MD5: 5f6b859726bd17bd5fb4905c4420b269, 一致

```
ctfshow{#He110_I_4m_Tw0_PieNG#}
```

One PieNG问卷调查

ctfshow{套娃终有报，天道好轮回。不信抬头看，苍天饶过谁。}