攻防世界Misc高手进阶区 3-11

原创

[飞燕草的蓝月](#) 于 2021-01-29 21:04:25 发布 448 收藏

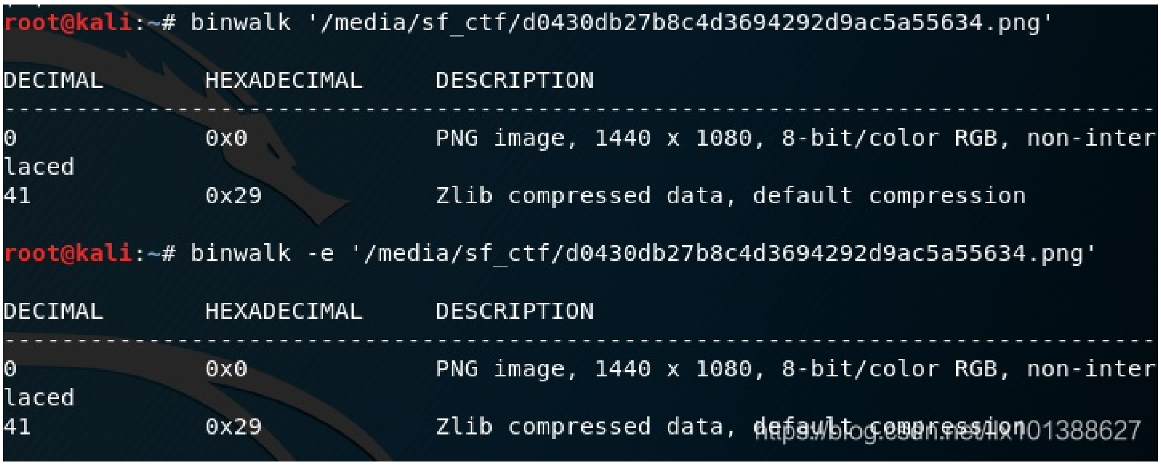
本文链接：https://blog.csdn.net/llx101388627/article/details/113406030

版权

攻防世界Misc高手进阶区 3-11

下载文件，得到一个png文件。既然是png文件，那就先用binwalk命令和stegsolve看看

首先是binwalk:

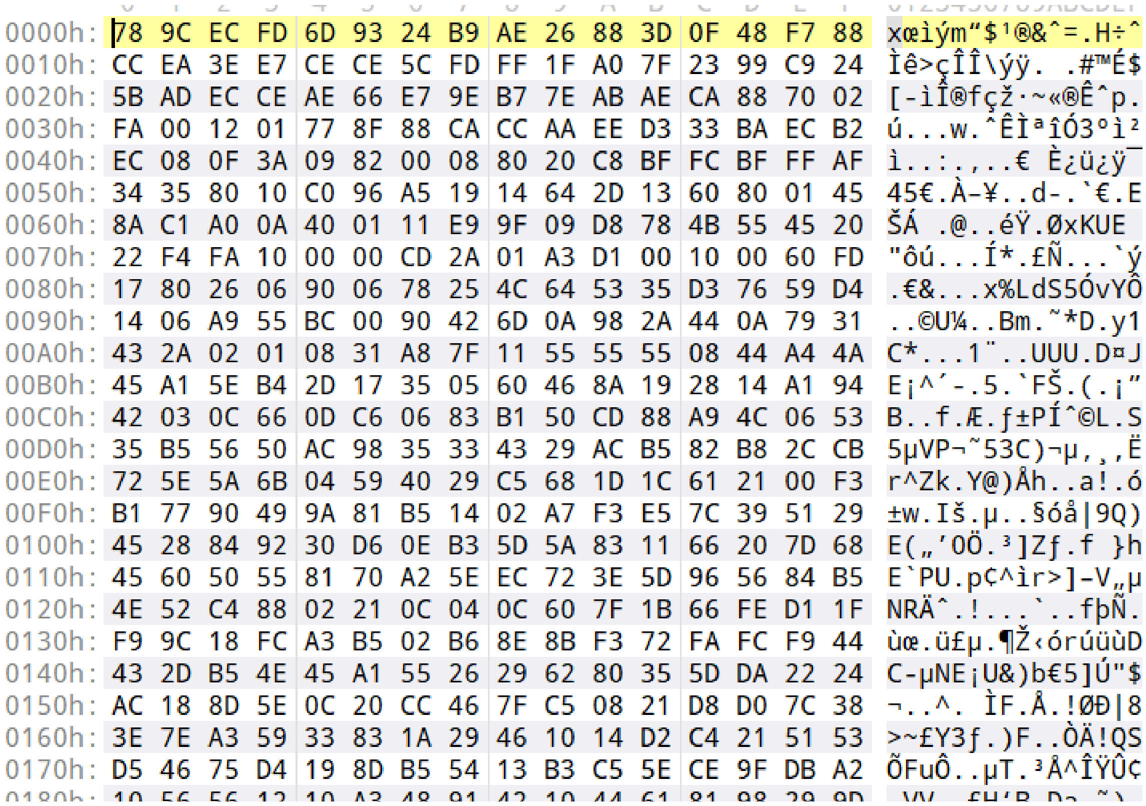


```
root@kali:~# binwalk '/media/sf_ctf/d0430db27b8c4d3694292d9ac5a55634.png'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1440 x 1080, 8-bit/color RGB, non-inter
laced
41            0x29            Zlib compressed data, default compression

root@kali:~# binwalk -e '/media/sf_ctf/d0430db27b8c4d3694292d9ac5a55634.png'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1440 x 1080, 8-bit/color RGB, non-inter
laced
41            0x29            Zlib compressed data, default compression
```

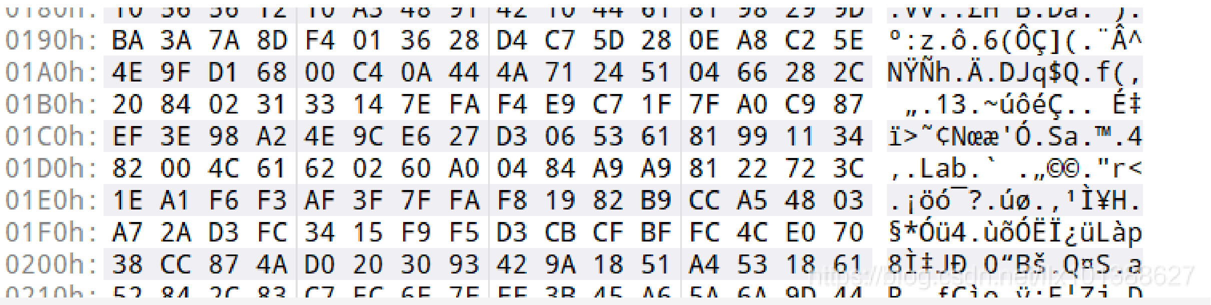
似乎是一个zlib文件。

作为一个新人，对这类文件不是很熟，但还是先提取出来看看，万一是改了后缀的其他类型文件呢

用010editor打开：



```
0000h: 78 9C EC FD 6D 93 24 B9 AE 26 88 3D 0F 48 F7 88  xœìým“$¹®&ˆ=.H÷ˆ
0010h: CC EA 3E E7 CE CE 5C FD FF 1F A0 7F 23 99 C9 24  Ìê>çÎÎ\ýÿ. .#™É$
0020h: 5B AD EC CE AE 66 E7 9E B7 7E AB AE CA 88 70 02  [-ìÎ®fçž·~«®Êˆp.
0030h: FA 00 12 01 77 8F 88 CA CC AA EE D3 33 BA EC B2  ú...w.ˆÊÌªîÓ3ºì²
0040h: EC 08 0F 3A 09 82 00 08 80 20 C8 BF FC BF FF AF  ì..:.‚..€ È¿ü¿ÿ¯
0050h: 34 35 80 10 C0 96 A5 19 14 64 2D 13 60 80 01 45  45€.À–¥..d-.`€.E
0060h: 8A C1 A0 0A 40 01 11 E9 9F 09 D8 78 4B 55 45 20  ŠÁ .@..éŸ.ØxKUE 
0070h: 22 F4 FA 10 00 00 CD 2A 01 A3 D1 00 10 00 60 FD  "ôú...Í*.£Ñ...`ý
0080h: 17 80 26 06 90 06 78 25 4C 64 53 35 D3 76 59 D4  .€&...x%LdS5ÓvYÔ
0090h: 14 06 A9 55 BC 00 90 42 6D 0A 98 2A 44 0A 79 31  ..©U¼..Bm.˜*D.y1
00A0h: 43 2A 02 01 08 31 A8 7F 11 55 55 55 08 44 A4 4A  C*...1¨..UUU.D¤J
00B0h: 45 A1 5E B4 2D 17 35 05 60 46 8A 19 28 14 A1 94  E¡^´-.5.`FŠ.(.¡”
00C0h: 42 03 0C 66 0D C6 06 83 B1 50 CD 88 A9 4C 06 53  B..f.Æ.ƒ±PÍˆ©L.S
00D0h: 35 B5 56 50 AC 98 35 33 43 29 AC B5 82 B8 2C CB  5µVP¬˜53C)¬µ‚¸,Ë
00E0h: 72 5E 5A 6B 04 59 40 29 C5 68 1D 1C 61 21 00 F3  r^Zk.Y@)Åh..a!.ó
00F0h: B1 77 90 49 9A 81 B5 14 02 A7 F3 E5 7C 39 51 29  ±w.Iš.µ..§óå|9Q)
0100h: 45 28 84 92 30 D6 0E B3 5D 5A 83 11 66 20 7D 68  E(„’0Ö.³]Zƒ.f }h
0110h: 45 60 50 55 81 70 A2 5E EC 72 3E 5D 96 56 84 B5  E`PU.p¢^ìr>]–V„µ
0120h: 4E 52 C4 88 02 21 0C 04 0C 60 7F 1B 66 FE D1 1F  NRÄˆ.!...`..fþÑ.
0130h: F9 9C 18 FC A3 B5 02 B6 8E 8B F3 72 FA FC F9 44  ùœ.ü£µ.¶Ž‹óruüùD
0140h: 43 2D B5 4E 45 A1 55 26 29 62 80 35 5D DA 22 24  C-µNE¡U&)b€5]Ú"$
0150h: AC 18 8D 5E 0C 20 CC 46 7F C5 08 21 D8 D0 7C 38  ¬..^. ÌF.Å.!ØÐ|8
0160h: 3E 7E A3 59 33 83 1A 29 46 10 14 D2 C4 21 51 53  >~£Y3ƒ.)F..ÒÄ!QS
0170h: D5 46 75 D4 19 8D B5 54 13 B3 C5 5E CE 9F DB A2  ÕFuÔ..µT.³Å^ÎŸÛ¢
```

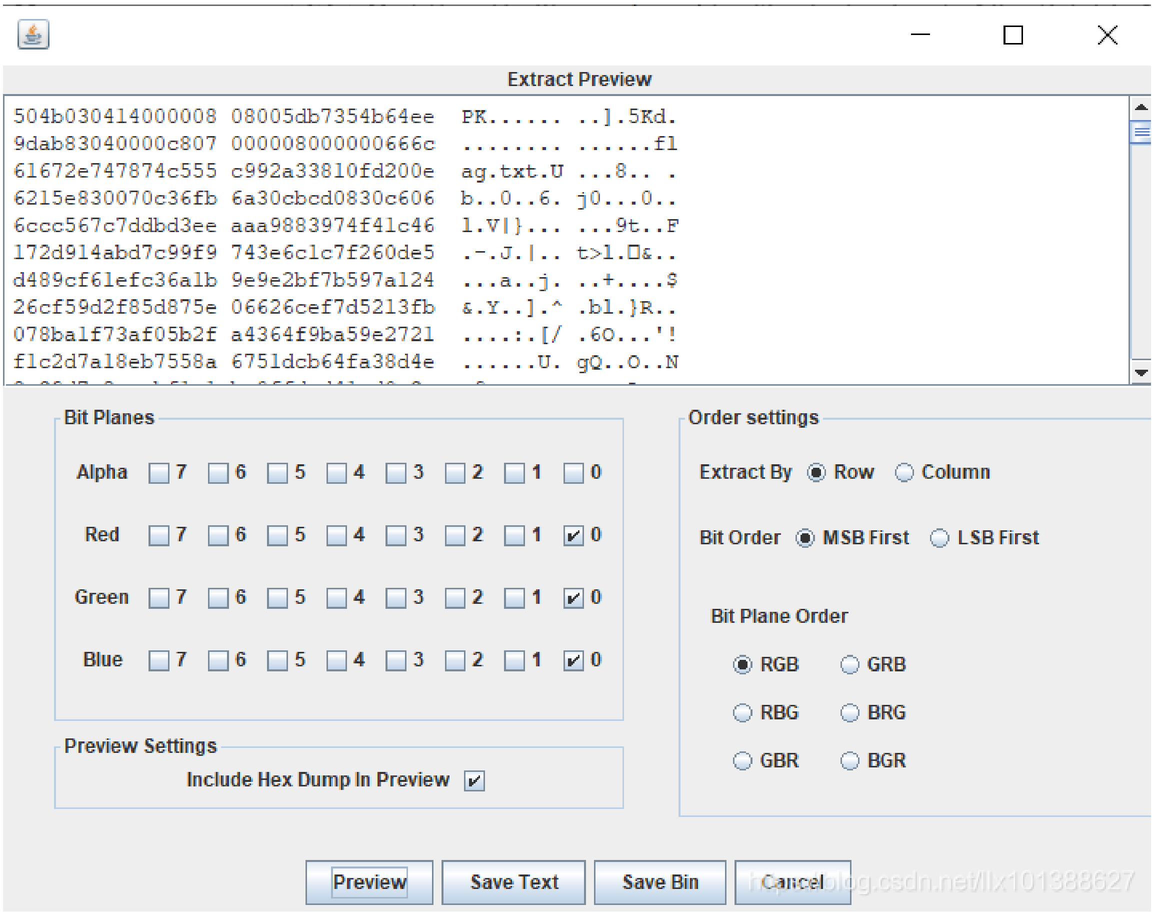


```
0190h: BA 3A 7A 8D F4 01 36 28 D4 C7 5D 28 0E A8 C2 5E  º:z.ô.6(ÔÇ](.¨Â^
01A0h: 4E 9F D1 68 00 C4 0A 44 4A 71 24 51 04 66 28 2C  NŸÑh.Ä.DJq$Q.f(,
01B0h: 20 84 02 31 33 14 7E FA F4 E9 C7 1F 7F A0 C9 87   „.13.~úôéÇ.. É‡
01C0h: EF 3E 98 A2 4E 9C E6 27 D3 06 53 61 81 99 11 34  ï>˜¢Nœæ'Ó.Sa.™.4
01D0h: 82 00 4C 61 62 02 60 A0 04 84 A9 A9 81 22 72 3C  ‚.Lab.` .„©©."r<
01E0h: 1E A1 F6 F3 AF 3F 7F FA F8 19 82 B9 CC A5 48 03  .¡öó¯?.úø.‚¹Ì¥H.
01F0h: A7 2A D3 FC 34 15 F9 F5 D3 CB CF BF FC 4C E0 70  §*Óü4.ùõÓËÏ¿üLàp
0200h: 38 CC 87 4A D0 20 30 93 42 9A 18 51 A4 53 18 61  8Ì‡JÐ 0“Bš.Q¤S.a
```

好，看不懂，下一个stegsolve：

先把各个通道（？）下的图片看一下，发现没什么异常

那么接下来看一下是否存在LSB隐写：



Extract Preview

```
504b030414000008 08005db7354b64ee  PK...... ..].5Kd.
9dab83040000c807 000008000000666c  ........ ......fl
61672e747874c555 c992a33810fd200e  ag.txt.U ...8.. .
6215e830070c36fb 6a30cbcd0830c606  b..0..6. j0...0..
6ccc567c7ddbd3ee aaa9883974f41c46  l.V|}... ...9t..F
172d914abd7c99f9 743e6c1c7f260de5  .-.J.|.. t>l.□&..
d489cf61efc36a1b 9e9e2bf7b597a124  ...a..j. ..+....$
26cf59d2f85d875e 06626cef7d5213fb  &.Y..].^ .bl.}R..
078ba1f73af05b2f a4364f9ba59e2721  ....:.[/ .6O...'!
f1c2d7a18eb7558a 6751dcb64fa38d4e  ......U. gQ..O..N
```

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

Preview Settings

Include Hex Dump In Preview ☑

Order settings

Extract By ● Row ○ Column

Bit Order ● MSB First ○ LSB First

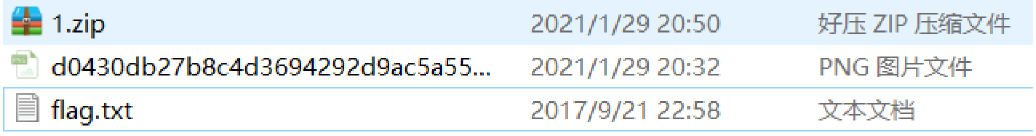
Bit Plane Order

● RGB ○ GRB

○ RBG ○ BRG

○ GBR ○ BGR

得到的代码开头是504b0304（zip文件头），看来有点东西，Save Bin保存代码成zip格式，然后成功解压，得到一个名为flag.txt的文件：



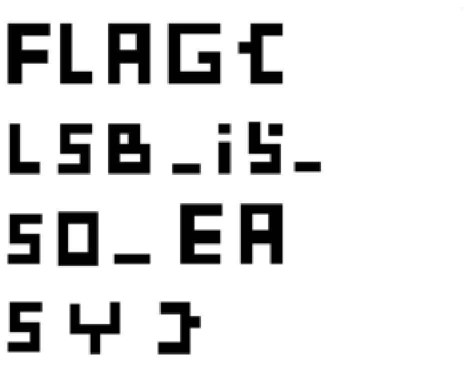
1.zip	2021/1/29 20:50	好压 ZIP 压缩文件
d0430db27b8c4d3694292d9ac5a55...	2021/1/29 20:32	PNG 图片文件
flag.txt	2017/9/21 22:58	文本文档

打开查看这个txt文件，得到以下内容：

iVBORw0KGgoAAAANSUhEUgAAAPoAAAD6CAYAAACI7Fo9AAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAAJc
EhZcwAAEnQAABJ0Ad5mH3gAAAVqSURBVHhe7d1bTuRGAEDRlftfK1tlxgNRJNlNbpff9xzJmvlpP6q5KpeB5u3v334Bt/bX57/Aj
QkdAoQOAUKHAKFDgNAhQOgQIHQlEDoECB0ChA4BQocLe39///zf9/xSCwSY0SFA6BAgdAgQOgQIHQKEDgGLv7329vb2+b
/1PDqVZ8dZ67uCe13HV1sc95GRcRo9x7GRcRo9x7XeI8aZ0SFA6BAgdAgQOgR4GLdw/99d/5xz2/pWo2CX3NN3jrIJbuf/T6t76
uNVzhHJnHrTsECB0ChM6fW/RHG/chdAgQOgQIHQJO8330Z6fx7DhrfytbYtni7XonHPb+rpe8YHHHGOjDGjX9AU5twNJkLnzwz9aO
M+hA4BQocAoUQA0CHAb68N7B+o1z7zaJ9r72+v1tizHzM6BAgdAoQOAZddo8/107mMrEQ3oO3aBt6Lrcoo/ZiBIUDoECB0CB

M+hA4BQocAoUOA0CHAb68N7P+6127zaJ9f72+yTtzHzM6BAgdAoQOAZdd08/107mMrEO3eO3aRt6Lrcee/ZjRtOD0ECB0CB
A6BAgdAhY/dQeuw4wOAUKHAKFDgNAhQOgQIHQIEDoECB0ChA4BQocAoUOA0CFA6BAgdAgQOgQIHQKEDgFChwAfJcV
DI3+cgvMZCv3RF8PaXwhb/7WQO/81kpFY5772u/E789jUuHWHAKFDgNAhQOgQcMmHcWseY/Sh09rXexaj4zK569hckRmdIVP
MzzbOQ+gQIHQIEPqNTevnRxs9t/7JuDnnssUX/InWp8+ubY9xOcsY8MGMDgFChwChQ4DQIeD0D+PmWnoulw+sJmcag69Gr22u
M48BH8zoECB0CBA6BKy+Rp/rLOvEkWt45izr09E1+Ibv75L9nmVMr+rUoY9GuMcxHnllSJcef+Ta5p7fVu/vkv2+Mqb8n1t3CBA6B
AgdAoTO7qb19qsbY4YexgHXYEaHAKFDgNAhQOgQIHQIEDoECB0ChA4BQocAoUOA0CFA6BAgdAgQOgT4NdWTOeoz7I46
Lvswo0OA0CFA6BBw6jX62uvGK6wZrdHZwmF/wGHy06GFvo451/3suCPv0RXGu0LoJ3NUOEK/N2t0CBA6BAgdAIZfo6+5LhvZ/
9bntpWj1rzPjvvTMY86X15jRocAoUOAW/eT+e5WeImR8Rp1hfGuMKNDwOqhTzPDnA3YjxkdAoQOAUKHAKFDwC6/j/7o4ducwy
593WTktUf67kHIluf/7LhL36fJFca7wowOAUKHAKFDwOVCn9aDczbgP4sfxo3GNPKQZ6mfjrnW8UYeQu19zf96dtyR92IkHFiXW3
cIEDoECB0ChA4Bu/xk3FJHPZiCuzI16MA63LpDgNAhQOgQIHQIEDoECB0ChA4BQocAoUOA0CFA6BAgdAgQOgQIHQKEDg
FChwChQ8DQJ8yMftTTWT7c5tF1rH1uI2PIQ4AYdckZfYrm6wY859YdAoQOAUKHgNUfxu3x4Gjt4+5xHSPPEfYYU+5N6L8ddR2P
nOIcuA+37hcwxf91g1cIHQKEDgGH/WTcmdbUa+9vxNwxPer8uKbbhL42oXMnbt0hQOgXMM3eXzd4hdAhYGiNPtfaD7tqa3QzOK
MuGfpcV4xG6GzBrTsECB0ChA4Bi9foow/ESmv0K4wV92ZGhwChQ4DQIUDoELDLD8wcxcM4+HDr0IEPbt0hQOgQIHQIEDoE
CB0ChA4BQocAoUOA0CFA6BAgdAgQOgQIHQKEDgFChwChQ4DQIUDoECB0CBA6BAgdAoQOAUKHAKFDgNAhQOgQIH
QIEDoECB0ChA4BQocAoUOA0CFA6BAgdAgQOgQIHQKEDgFChwChQ4DQIUDoECB0CBA6BAgdAoQOAUKHAKFDgNAh
QOgQIHQIEDoECB0ChA4BQocAoUOA0CFA6BAgdAgQOgQIHQKEDgFChwChw+39+vUPmuaZZgm+XxcAAAAASUVORK5C
YII=

根据结尾的=号判断，应该是base64编码，又因为开头的代码为iVBORw0K，猜测应该是base64编码的图片，那么解码后可以得到：



这样就得到了flag:
FLAG{LSB_i5_SO_EASY}