




简单图片隐写术练习题

原创

椰奶冻不安全  于 2020-06-26 21:13:23 发布  1103  收藏 20

分类专栏: [杂](#) 文章标签: [信息安全](#) [安全](#)

来自 椰奶冻不安全 的博客, 复制完可要记得我吖

本文链接: https://blog.csdn.net/qq_40654505/article/details/106974557

版权



[杂](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

隐写术练习题

【题目及工具地址】: <https://github.com/RookieDrummer/Simple-picture-steganography.git>

目录

隐写术练习题

[2.png](#)

[566.gif](#)

[2010112719152853781.gif](#)

[eg_tulip.jpg](#)

[flag.exe](#)

[out.jpg](#)

[out2.jpg](#)

[rose.jpg](#)

[ta.jpg](#)

[xx.gif](#)

JPEG(jpg), 文件头: FF D8 FF E0 00 10 4A 46 49 46 文件尾: FF D9

PNG (png), 文件头: 89 50 4E 47 0D 0A 1A 0A 文件尾: 49 45 4E 44 AE 42 60 82

GIF (gif), 文件头: 47 49 46 38

Windows Bitmap (bmp), 文件头: 42 4D

Roshal ARchive (rar),文件头: 52 61 72 21

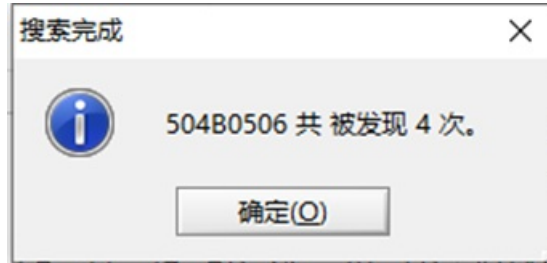
Deflate (zip), 文件头: 50 4B 03 04 14 00 00 00 08 00

PDF, 文件头: 25 50 44 46

2.png



查看详细信息里正常，winhex发现有好多zip的文件头，搜索一下十六进制的zip文件头50 4B 05 06共被发现四次，说明有四个隐藏的压缩包

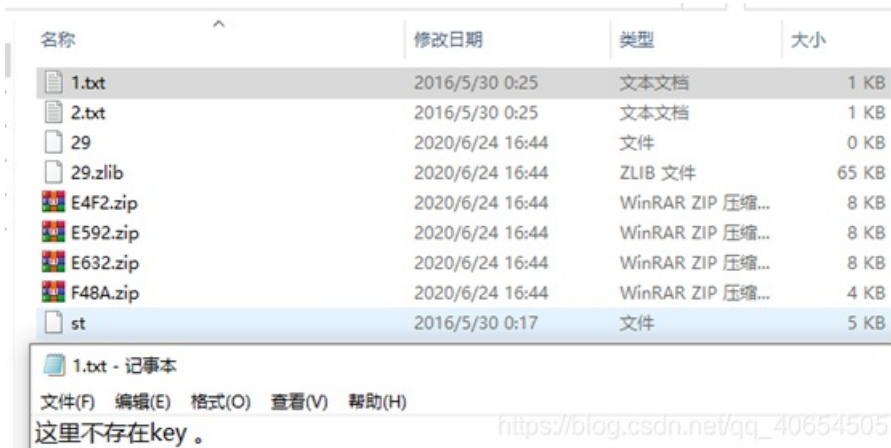


用binwalk提取一下

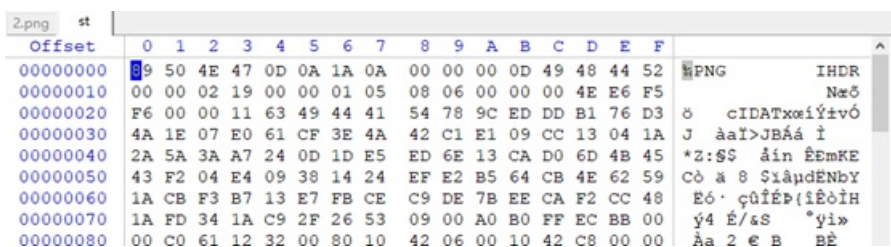
```
binwalk 2.png
```

```
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 411 x 218, 8-bit/color RGBA, non-interlaced
41          0x29        Zlib compressed data, default compression
53610       0xE4F2      Zip archive data, at least v1.0 to extract, compressed size: 16, uncompressed size: 16
name: 1.txt
53748      0xE57C      End of Zip archive, footer length: 22
53770      0xE592      Zip archive data, at least v1.0 to extract, compressed size: 16, uncompressed size: 16
name: 2.txt
53908      0xE61C      End of Zip archive, footer length: 22
53930      0xE632      Zip archive data, at least v2.0 to extract, compressed size: 3534, uncompressed size: 3534
name: st
62580      0xF474      End of Zip archive, footer length: 22
62602      0xF48A      Zip archive data, at least v2.0 to extract, compressed size: 3534, uncompressed size: 3534
name: st
66252      0x102CC     End of Zip archive, footer length: 22
```

```
binwalk -e 2.png
```



最后用winhex打开st发现了png文件头



将st重命名为st.png即得到flag

key is 3F838EFA8139F01D

566.gif



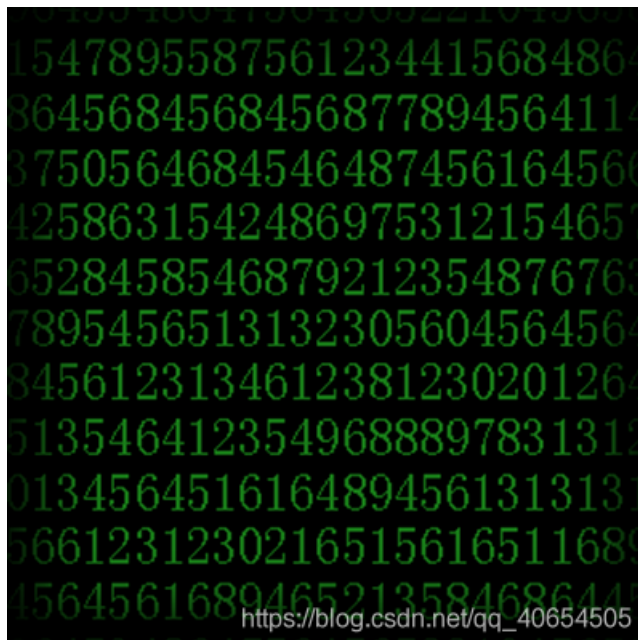
属性里的详细信息啥也没有，依旧winhex打开，文件头正常，但是在最末尾发现了东西

```
00021C00 2D 92 5A 5A F1 91 F1 82 3F 63 3F ED 5F 47 0E 3F  3'ZZn`n,?c?i_G ?
00021C10 3F 3F C8 E1 DB F6 8A D0 64 4B 1F A8 7A 74 B0 5A  ??ÈáÙóšBdK `zt"Z
00021C20 41 26 78 98 DF A1 AE 3F 55 4B 84 79 99 E5 4A DB  A&x"š;@?UK,,y=áJÜ
00021C30 D0 3F 02 A7 AA 1E 8D 9C D2 45 3F 76 2C 6E 9C 6E  B? $* œ0E?v,non
00021C40 6C CC D9 76 54 F8 65 0F 3F 2F 5B EE DD C0 4C 30  liÛvTœe ?/[iÝÀL0
00021C50 F0 9B BA 89 FF 75 75 B3 76 EA 9A E4 8A D2 79 53  ô>°kyuu*vêšãŠôys
00021C60 81 7A 3F B7 58 3F 1E 9A 5F A4 FE E6 8C 3A BC 6A  z?.X? š _pæE:kj
00021C70 6C DD 6D 3F 3F 0F 3F 0F FA B6 37 01 3F E1 58 C8  lÝm?? ? úŸ7 ?áXÈ
00021C80 46 3F 3A AE F5 88 F6 B2 8F 62 91 B2 E0 A9 CF E7  F?:œó^ó^ b'`â@Iç
00021C90 3F BB F5 3F 38 F5 FD 55 80 76 F0 4D 57 66 D6 F0  ?»ô?8ôýÙevôMwfôô
00021CA0 CE C5 77 C7 74 44 29 A3 96 3F 65 3F A9 BE 26 A8  iÅwçTD)¿-?e?@%&"
00021CB0 BE 3F 3F 7D 8F DE F2 68 B3 79 3F E9 6B 37 86 5F  %??) bôh*y?ék7+_
00021CC0 95 40 FD C4 3F 40 01 07 8C 50 3F 5A 3F 20 67 62  •@ýÅ?@ GP?Z? qb
00021CD0 F2 6D 3F 7C 07 A3 CF FF 2D 3F 0B 3F 3F BD FE 7F  çm?| ¿Iy-? ??%p
00021CE0 3F 4D 3F E4 BF 3F 3F 6F 96 F6 24 FD EC 1F 01 50  ?M?â¿??o-ô$ýi P
00021CF0 4B 01 02 3F 20 14 20 20 20 08 20 93 9A 5E 47 12  K ? "š^G
00021D00 36 26 24 3F 20 20 3F 20 20 0A 20 24 20 20 20 20  6&$? ? $
00021D10 20 20 20 20 20 20 20 20 20 20 20 32 33 33 33 33  23333
00021D20 33 2E 67 69 66 0A 20 20 20 20 20 20 20 01 20 18  3.gif
00021D30 20 5F 33 58 20 05 13 3F 70 5A 58 20 05 13 3F 70  _3X ?pZX ?p
00021D40 5A 58 20 05 13 3F 50 4B 05 06 20 20 20 20 01 20  ZX ?DX
00021D50 01 20 5C 20 20 20 3F 20 20 20 0D 0A 0D 0A 6B 65  \ ? ke
00021D60 79 3A 36 32 66 32 34 33 35 32 38 30 65 61 35 39  y:62f2435280ea59
00021D70 63 39 20 c9
```

https://blog.csdn.net/qq_40654505

emmmmmm 结束

2010112719152853781.gif



详细信息正常，文件头正常，binwalk发现里面居然还有一个rar，之前用binwalk居然没发现，害，提取吧

```
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          GIF image data, version "89a", 300 x 300
184854      0x2D216      RAR archive data, version 4.x, first volume type: MAIN_HEAD
```

binwalk -e 2010112719152853781.gif

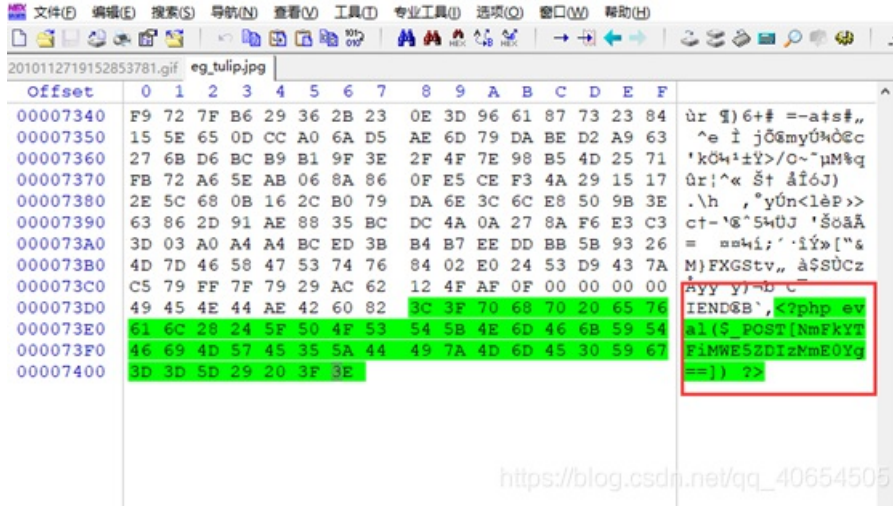
得到压缩包，在里面找到flag



eg_tulip.jpg



winhex打开发现文件头是png，文件末尾发现一句话木马

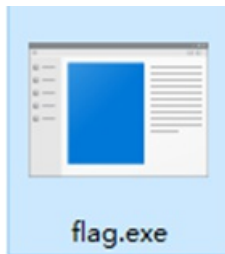


flag应该是这个base64加密后的密文

NmFkYTFiMWE5ZDIzNmE0Yg==

网上找个在线base64解密网站搞定

flag.exe



winhex打开发现是个png，给文件重命名变成了二维码



扫码得到flag

out.jpg



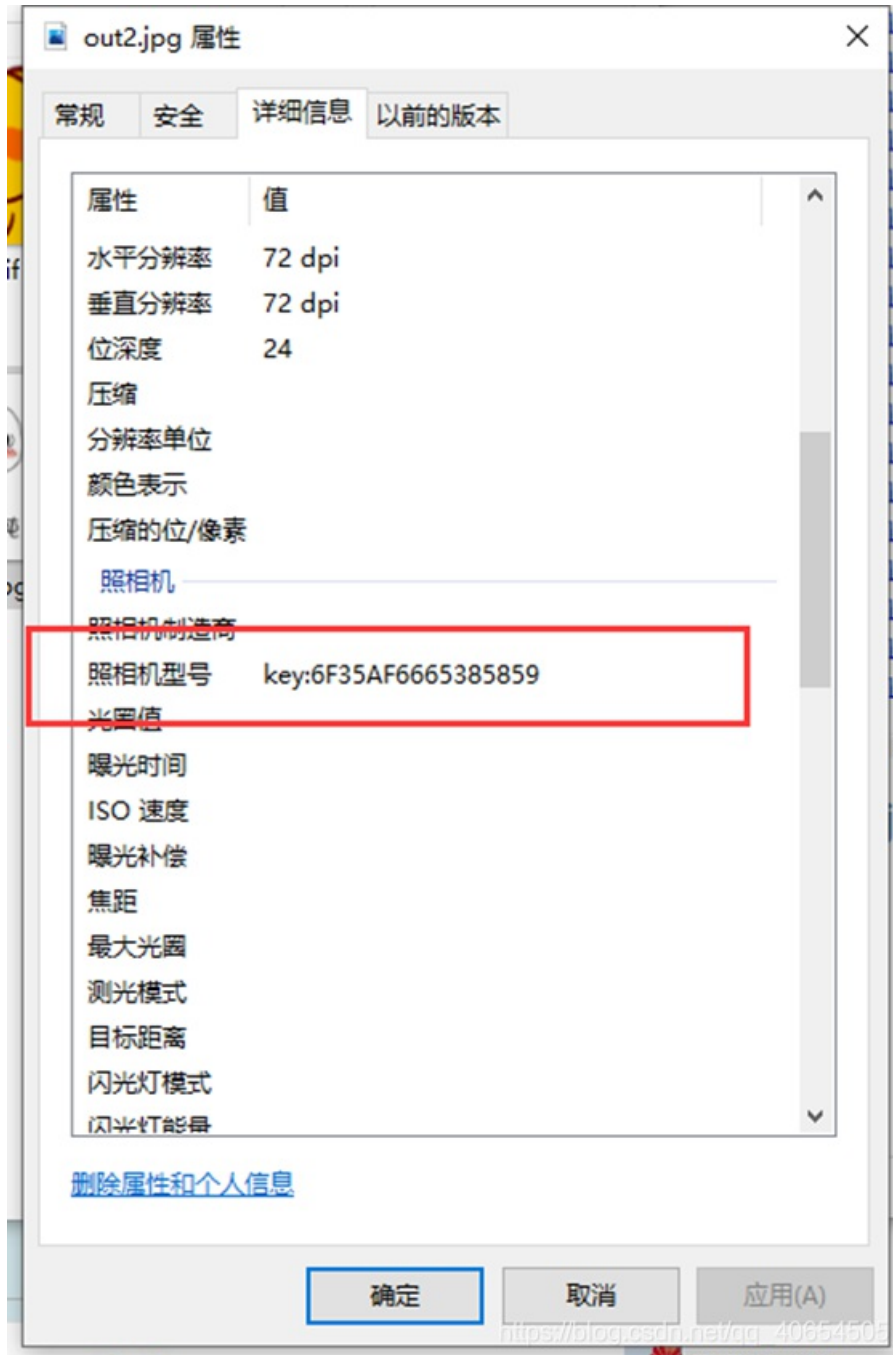
winhex打开在文件末尾找到这个。。。。目测是两张图片，需要分离，不过这都这么明显了，就算了吧

```
00001E00 9D 1B 82 A4 F0 6A C2 A2 A2 05 03 80 38 A2 8A 00  ,=0jÃcç €8cŠ
00001E00 F2 CD 4E 3F ED FF 00 8C D7 5E 19 BE 67 3A 53 69  òîN?iy Gx^ *g:Si
00001E10 A9 2C 91 46 DB 0C 84 30 7C 33 0E 71 9E C3 1C 71  @,'F0 „013 qžÃ q
00001E20 5E 93 A7 69 76 3A 75 AA C3 63 6B 0D AC 59 2D B2  ^"šiv:u*Ãck -Y-²
00001E30 04 08 32 7A 9E 3B D1 45 24 36 CB 22 31 B8 9D C4  2zž;NE$6E"1, Å
00001E40 E6 A4 55 0A 31 45 14 C4 3A 8A 28 A0 02 8A 28 A0  æ=U 1E Å:Š( Š(
00001E50 02 8A 28 A0 02 AB 5D D8 C3 7B 18 49 83 15 07 38  Š( «)0Ã{ If 8
00001E60 07 14 51 40 15 DF 48 B7 70 37 34 87 1D 39 1D 4F  Q0 BH·p74† 9 0
00001E70 53 D2 86 D1 ED 9D FC DC C8 1F 9E 41 1D FA F6 A2  S0†Ñi uÜÈ ŽA úoc
00001E80 8A 00 0E 8F 6C 48 DC D2 1F A3 63 D7 D0 7B FE 94  Š 1HU0 Łc×D{p"
00001E90 BF D8 F6 B8 39 0E 73 8E F8 FC 78 A2 8A 00 4F EC  ž0ö,9 sž0uxçŠ oi
00001EA0 8B 63 BB E6 93 9E 0F 23 91 C7 B7 B5 5D 86 25 86  <c>æ"ž #'Ç·µ|†††
00001EB0 14 89 49 2A 8A 00 C9 E6 8A 28 03 FF D9 50 4B 03  †I*Š ÉæŠ( ýÜPK
00001EC0 04 0A 00 00 00 00 00 BA 65 6D 47 48 CF EE 50 14  °emGHİİP
00001ED0 00 00 00 14 00 00 00 07 00 00 00 6B 65 79 2E 74  key.txt
00001EE0 78 74 6B 65 79 3A 42 34 34 41 43 39 33 41 43 35  xtkey:B44AC93AC5
00001EF0 42 34 42 36 43 36 50 4B 01 02 3F 00 0A 00 00 00  B4B6C6PK ?
00001F00 00 00 BA 65 6D 47 48 CF EE 50 14 00 00 00 14 00  °emGHİİP
00001F10 00 00 07 00 24 00 00 00 00 00 00 00 20 00 00 00  $
00001F20 00 00 00 00 6B 65 79 2E 74 78 74 0A 00 20 00 00  key.txt
00001F30 00 00 00 01 00 18 00 BA 0E 3D 2C CE 1D D1 01 42  ° =,î Ñ B
00001F40 06 67 1E CE 1D D1 01 42 06 67 1E CE 1D D1 01 50  g î Ñ B g î Ñ P
00001F50 4B 05 06 00 00 00 01 00 01 00 59 00 00 00 39  K Y 9
00001F60 00 00 00 00 00
```

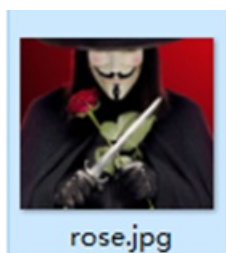
out2.jpg



不枉我每次都查看详细信息，果然出现了



rose.jpg



详细信息正常，十六进制正常，binwalk正常，不过用Stegdetect检测到了隐写

```
命令: stegdetect.exe -tjopif -s 10.0 xxx.jpg
```

```
\\rose.jpg : jphide(*)
```

使用stegbreak用字典爆破密码

```
stegbreak.exe -r rules.ini -f 123.txt -t p xxx.jpg
```

得到密码123456

使用 steghide info xxx.jpg, 输入密码即可提取隐藏文件得到flag

ta.jpg



用winhex打开搜索jpg的文件头，共发现两次，是两个图片拼接的

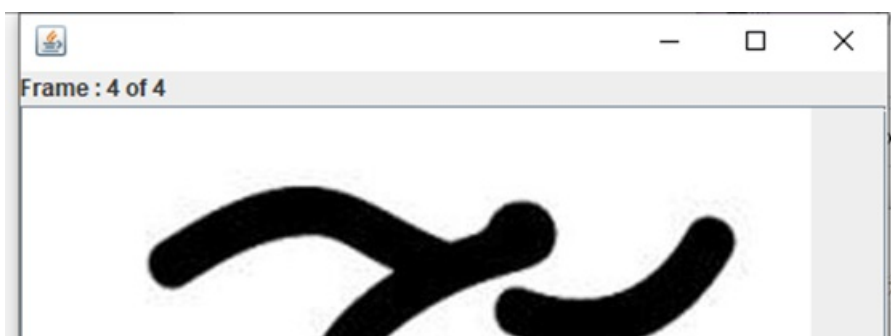
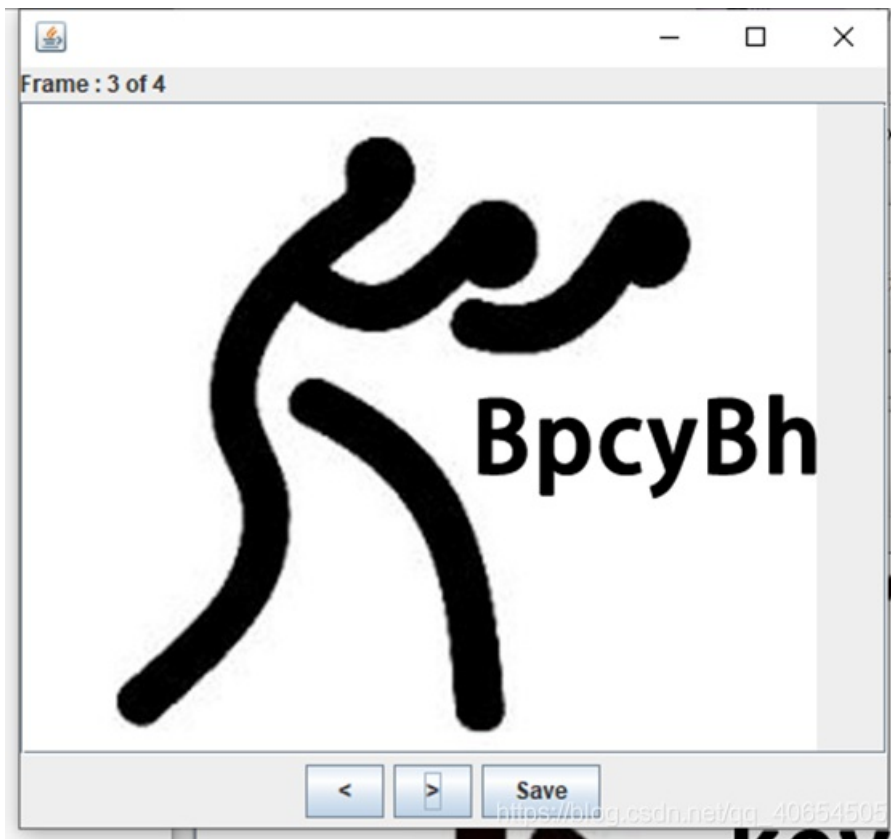


截取第二个文件头到末尾新建一个文件保存为.jpg，则成功得到flag

```
-----  
=====  
key:578FDB505ACA5187  
=====  
-----
```

https://blog.csdn.net/qq_40654505

xx.gif





key is:dGhpcyBpcyBhIGdpZg== 格式很明显是base64, 转码后得到flag: this is a gif