几道misc题

原创

「已注销」 于 2020-09-12 16:27:30 发布 1807 收藏 5

pdf

https://adworld.xctf.org.cn/media/task/attachments/ad00be3652ac4301a71dedd2708f78b8.pdf

下载后是一个pdf文件，将pdf转为word看看

在线工具：https://app.xunjiepdf.com/pdf2word

打开word后将图片移开，就可以得到flag

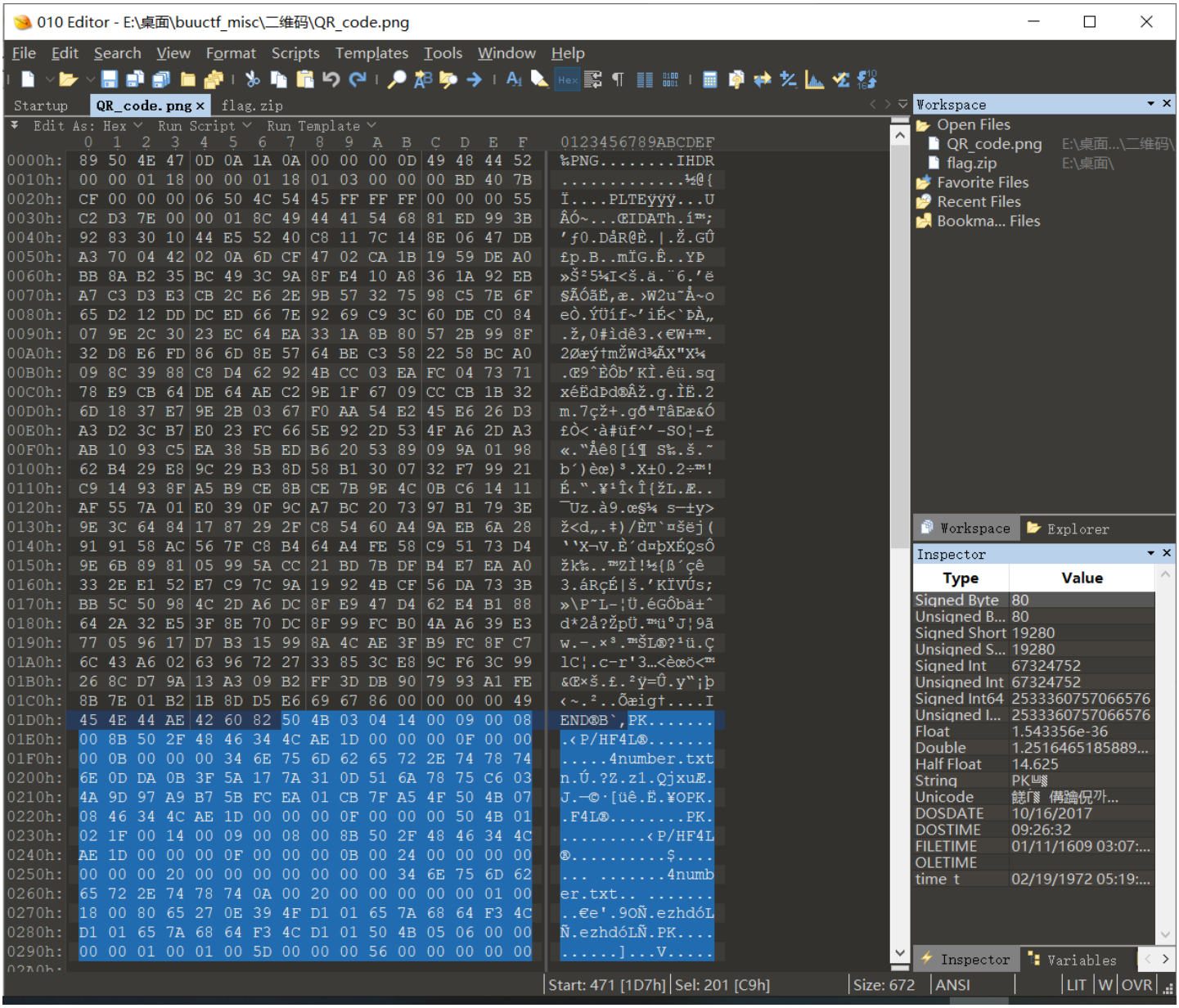
```
flag{security_through_obscurity}
```

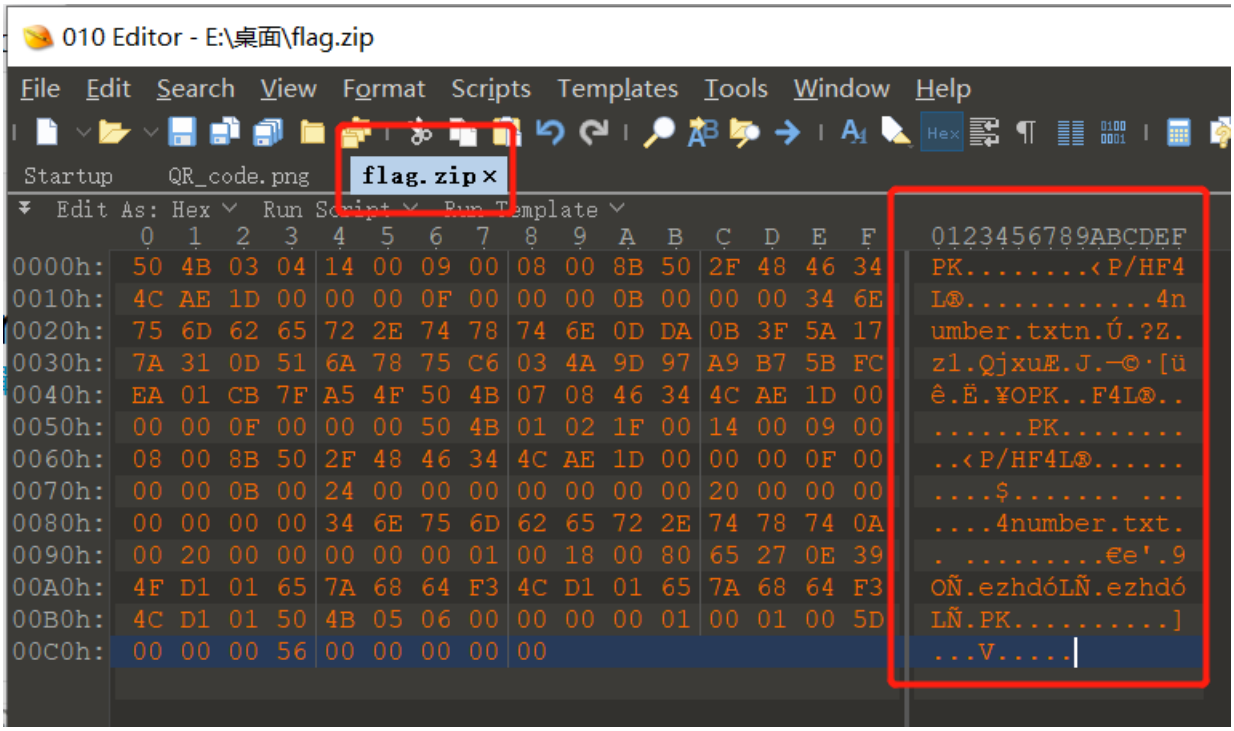
二维码

https://files.buuoj.cn/files/c611ef3b425901adf207c41810600b3c/f4571698-e6e4-41b6-8853-2aab17cef02a.zip?token=eyJ1c2VyX2lkIjoxNTA0OCwidGVhbV9pZCI6bnVsbCwiZmlsZV9pZCI6ODN9.XzttPA.Rl1WsQRj-R4TGh7b8PEmJK-PJFA

扫码提示：secret is here

把图片拖进010editor，发现压缩包，提取到flag.zip


010 Editor - E:\桌面\buuctf_misc\二维码\QR_code.png
File Edit Search View Format Scripts Templates Tools Window Help
Startup
QR_code.png
flag.zip
Edit As: Hex Run Script Run Template
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 ‰PNG........IHDR
0010h: 00 00 01 18 00 00 01 18 01 03 00 00 00 BD 40 7B ....½@{
0020h: CF 00 00 00 06 50 4C 54 45 FF FF FF 00 00 00 55 Ï....PLTEÿÿÿ...U
0030h: C2 D3 7E 00 00 01 8C 49 44 41 54 68 81 ED 99 3B ÂÓ~...ŒIDATh.í™;
0040h: 92 83 30 10 44 E5 52 40 C8 11 7C 14 8E 06 47 DB ’ƒ0.DåR@È.|.Ž.GÛ
0050h: A3 70 04 42 02 0A 6D CF 47 02 CA 1B 19 59 DE A0 £p.B..mÏG.Ê..YÞ
0060h: BB 8A B2 35 BC 49 3C 9A 8F E4 10 A8 36 1A 92 EB »Š²5¼I<š.ä.¨6.’ë
0070h: A7 C3 D3 E3 CB 2C E6 2E 9B 57 32 75 98 C5 7E 6F §ÃÓãË,æ.›W2u˜Å~o
0080h: 65 D2 12 DD DC ED 66 7E 92 69 C9 3C 60 DE C0 84 eÒ.ÝÜíf~’iÉ<`ÞÀ„
0090h: 07 9E 2C 30 23 EC 64 EA 33 1A 8B 80 57 2B 99 8F .ž,0#ìdê3.‹€W+™.
00A0h: 32 D8 E6 FD 86 6D 8E 57 64 BE C3 58 22 58 BC A0 2Øæý†mŽWd¾ÃX"X¼
00B0h: 09 8C 39 88 C8 D4 62 92 4B CC 03 EA FC 04 73 71 .Œ9ˆÈÔb’KÌ.êü.sq
00C0h: 78 E9 CB 64 DE 64 AE C2 9E 1F 67 09 CC CB 1B 32 xéËdÞd®Âž.g.ÌË.2
00D0h: 6D 18 37 E7 9E 2B 03 67 F0 AA 54 E2 45 E6 26 D3 m.7çž+.gðªTâEæ&Ó
00E0h: A3 D2 3C B7 E0 23 FC 66 5E 92 2D 53 4F A6 2D A3 £Ò<·à#üf^’-SO¦-£
00F0h: AB 10 93 C5 EA 38 5B ED B6 20 53 89 09 9A 01 98 «.“Åê8[í¶ S‰.š.˜
0100h: 62 B4 29 E8 9C 29 B3 8D 58 B1 30 07 32 F7 99 21 b´)èœ)³.X±0.2÷™!
0110h: C9 14 93 8F A5 B9 CE 8B CE 7B 9E 4C 0B C6 14 11 É.“.¥¹Î‹Î{žL.Æ..
0120h: AF 55 7A 01 E0 39 0F 9C A7 BC 20 73 97 B1 79 3E ¯Uz.à9.œ§¼ s—±y>
0130h: 9E 3C 64 84 17 87 29 2F C8 54 60 A4 9A EB 6A 28 ž<d„.‡)/ÈT`¤šëj(
0140h: 91 91 58 AC 56 7F C8 B4 64 A4 FE 58 C9 51 73 D4 ‘‘X¬V.È´d¤þXÉQsÔ
0150h: 9E 6B 89 81 05 99 5A CC 21 BD 7B DF B4 E7 EA A0 žk‰..™ZÌ!½{ß´çê
0160h: 33 2E E1 52 E7 C9 7C 9A 19 92 4B CF 56 DA 73 3B 3.áRçÉ|š.’KÏVÚs;
0170h: BB 5C 50 98 4C 2D A6 DC 8F E9 47 D4 62 E4 B1 88 »\P˜L-¦Ü.éGÔbä±ˆ
0180h: 64 2A 32 E5 3F 8E 70 DC 8F 99 FC B0 4A A6 39 E3 d*2å?ŽpÜ.™ü°J¦9ã
0190h: 77 05 96 17 D7 B3 15 99 8A 4C AE 3F B9 FC 8F C7 w.–.×³.™ŠL®?¹ü.Ç
01A0h: 6C 43 A6 02 63 96 72 27 33 85 3C E8 9C F6 3C 99 lC¦.c–r'3…<èœö<™
01B0h: 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE &Œ×š.£.²ÿ=Û.y“¡þ
01C0h: 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 ‹~.²..Õæigt....I
01D0h: 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END®B`‚PK.....
01E0h: 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 0F 00 00 .‹P/HF4L®.....
01F0h: 00 0B 00 00 00 34 6E 75 6D 62 65 72 2E 74 78 74 .....4number.txt
0200h: 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n.Ú.?Z.z1.QjxuÆ.
0210h: 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J.—©·[üê.Ë.¥OPK.
0220h: 08 46 34 4C AE 1D 00 00 00 0F 00 00 00 50 4B 01 .F4L®.....PK.
0230h: 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C .....‹P/HF4L
0240h: AE 1D 00 00 00 0F 00 00 00 0B 00 24 00 00 00 00 ®.....$....
0250h: 00 00 00 20 00 00 00 00 00 00 00 34 6E 75 6D 62 ... .4numb
0260h: 65 72 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 er.txt.. .....
0270h: 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C ..€e'.9OÑ.ezhdóL
0280h: D1 01 65 7A 68 64 F3 4C D1 01 50 4B 05 06 00 00 Ñ.ezhdóLÑ.PK....
0290h: 00 00 01 00 01 00 5D 00 00 00 56 00 00 00 00 00 ......]...V.....
Workspace
Open Files
QR_code.png E:\桌面...\二维码\
flag.zip E:\桌面\
Favorite Files
Recent Files
Bookma... Files
Workspace Explorer
Inspector
Type Value
Signed Byte 80
Unsigned B... 80
Signed Short 19280
Unsigned S... 19280
Signed Int 67324752
Unsigned Int 67324752
Signed Int64 2533360757066576
Unsigned I... 2533360757066576
Float 1.543356e-36
Double 1.2516465185889...
Half Float 14.625
String PK
Unicode
DOSDATE 10/16/2017
DOSTIME 09:26:32
FILETIME 01/11/1609 03:07:...
OLETIME
time_t 02/19/1972 05:19:...
Inspector Variables
Start: 471 [1D7h] Sel: 201 [C9h]
Size: 672 ANSI
LIT W OVR



解压flag.zip，发现要密码，提示：4number

直接用软件爆破得到密码：7639

其它方法：
把flag.zip拖进kali进行爆破

```
fcrackzip -b -l 4-4 -c 1 -p 0000 flag.zip
```

> Fcrackzip——简介、安装、使用

得到：

```
possible pw found: 0149 ()
possible pw found: 0690 ()
possible pw found: 1106 ()
possible pw found: 1358 ()
possible pw found: 1739 ()
possible pw found: 1786 ()
possible pw found: 1801 ()
possible pw found: 2316 ()
possible pw found: 2389 ()
possible pw found: 2773 ()
possible pw found: 2845 ()
possible pw found: 2988 ()
possible pw found: 3149 ()
possible pw found: 3151 ()
possible pw found: 3717 ()
possible pw found: 3720 ()
possible pw found: 3757 ()
possible pw found: 3854 ()
possible pw found: 4281 ()
possible pw found: 4363 ()
possible pw found: 4560 ()
possible pw found: 4884 ()
possible pw found: 4985 ()
possible pw found: 6207 ()
possible pw found: 6246 ()
possible pw found: 6325 ()
possible pw found: 6326 ()
possible pw found: 6398 ()
possible pw found: 6851 ()
possible pw found: 6962 ()
possible pw found: 6985 ()
possible pw found: 7127 ()
possible pw found: 7639 ()
possible pw found: 7803 ()
possible pw found: 8409 ()
possible pw found: 8430 ()
possible pw found: 8522 ()
```

一个一个尝试，最后得到解压密码：7639
解压后得到 4number.txt：

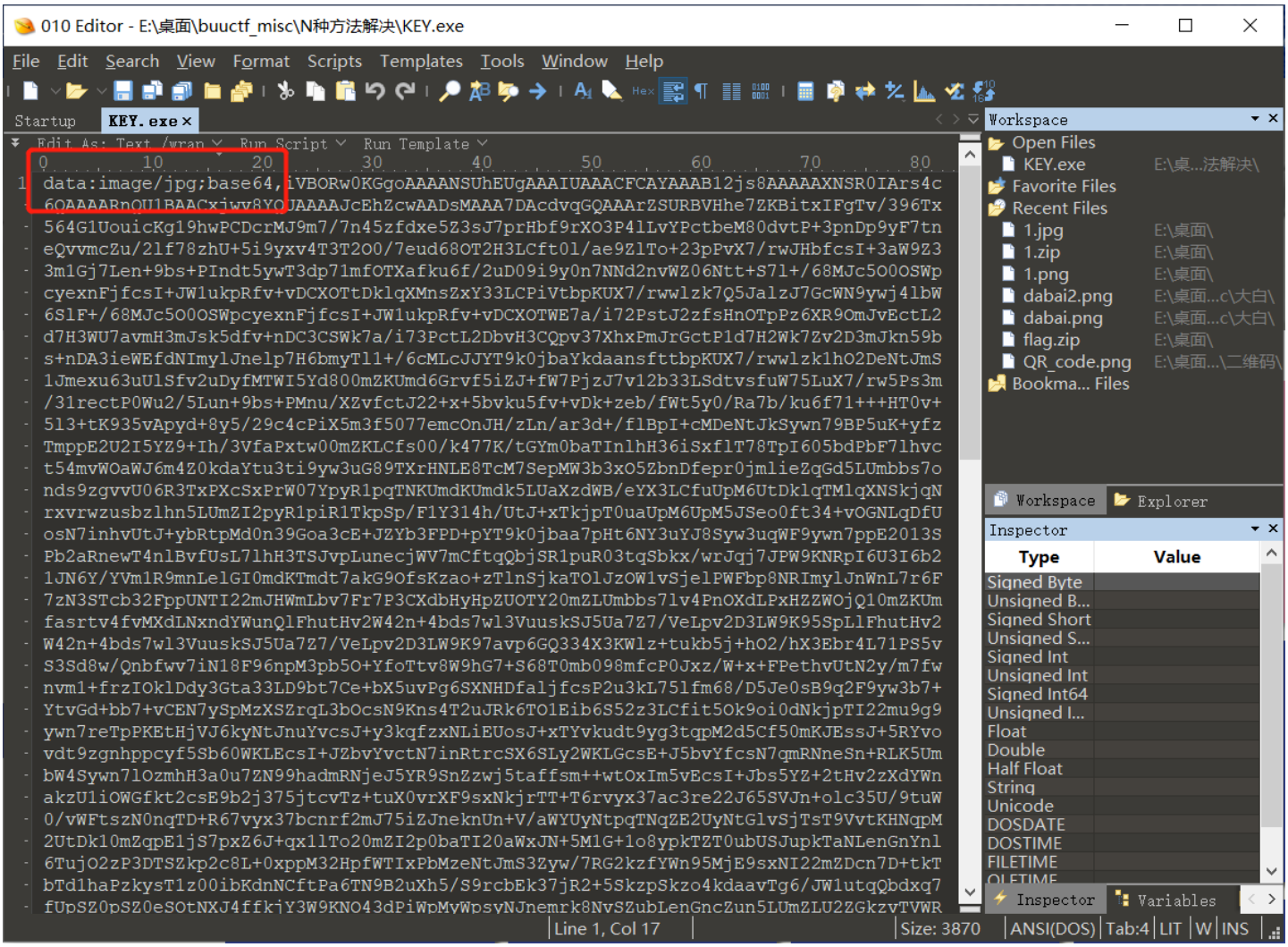
```
CTF{vjpw_wnoei}
```

N种方法解决

https://files.buuoj.cn/files/eda1929c94839b4aed936e3fa75fa8d6/f64ca6fa-1113-4ebe-8dbe-5e2d2db41ae1.zip?token=eyJ1c2VyX2lkIjoxNTA0OCwidGVhbV9pZCI6bnVsbCwiZmlsZV9pZCI6ODh9.Xzu42g.DbvGPHGhiNoGSfPm-A0rQXut3kU

解压得到一个名为KEY.exe的程序，无法运行

拖进010editor分析



使用网站http://tool.chinaz.com/tools/imgtobase转化为图片，扫码得到

```
KEY{dca57f966e4e4e31fd5b15417da63269}
```

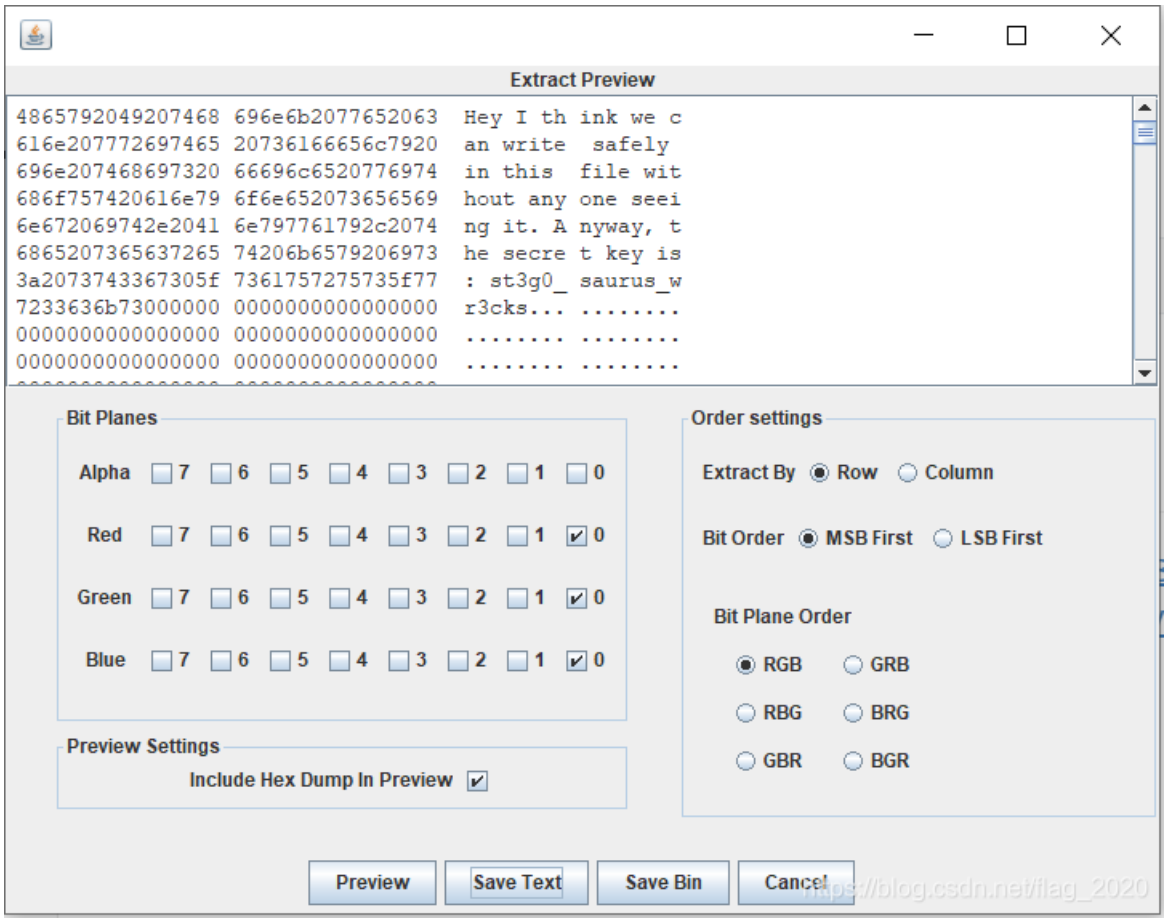
flag为

```
flag{dca57f966e4e4e31fd5b15417da63269}
```

镜子里的世界

https://files.buuoj.cn/files/5c368ac212141c544e817f9dff395de1/a74988d1-9df2-4e96-9fbd-45f4594b3e34.zip?token=eyJ1c2VyX2lkIjoxNTA0OCwidGVhbV9pZCI6bnVsbCwiZmlsZV9pZCI6ODZ9.XzzLSg.BSjm81Gkz76CByEaNpJ2mjbsKs4

根据图片名称**steg.png**，用**StegSolve**工具看一下LSB隐写



所以flag为：

```
flag{st3g0_saurus_wr3cks}
```

神奇的二维码

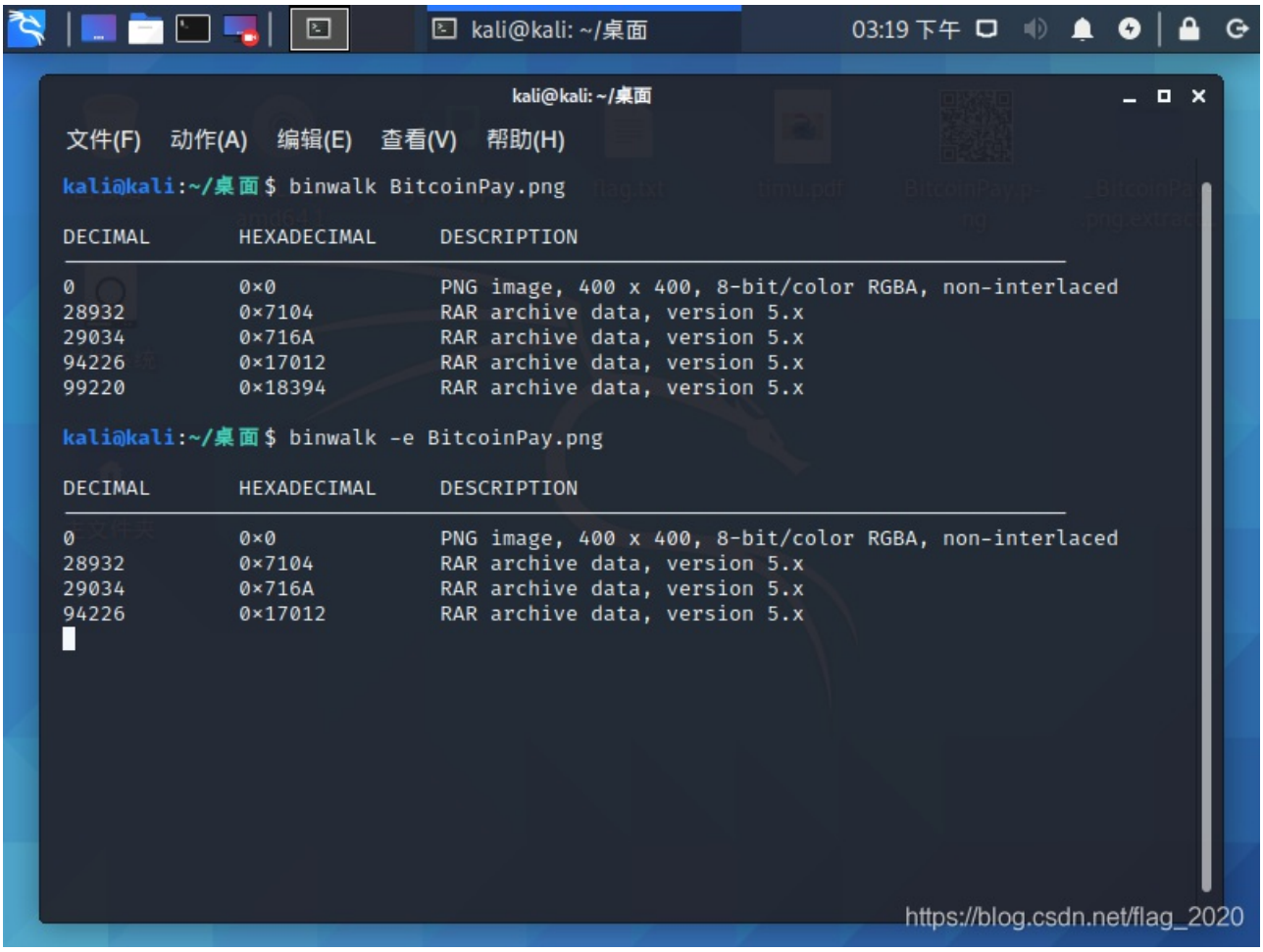
https://files.buuoj.cn/files/b7160092c20e47b7e9a4ddc641b37622/attachment.rar?token=eyJ1c2VyX2lkIjoxNTA0OCwidGVhbV9pZCI6bnVsbCwiZmlsZV9pZCI6Nzl1fQ.X1xz_w.eG9Z-GGww78n6mxnPSx9CJ382Ng

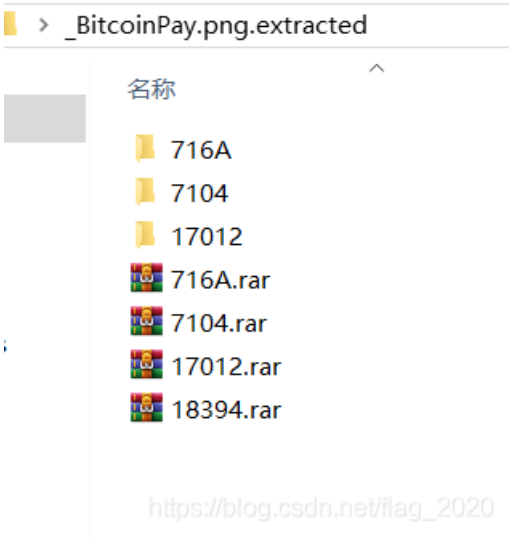
扫码后得到

```
swpuctf{flag_is_not_here}
```

拉到kali下查看，发现有4个压缩包

-e 提取出来





压缩包18394.rar是加密的

716A打开后有个加密的压缩包

> 看看flag在不在里面-.rar

密码为7104里的encode.txt

> YXNkZmdoamtsMTIzNDU2Nzg5MA==

用base64解密后为

> asdfghjkl1234567890

打开后是一张图片

emmmm，好像没什么用

17012里有一个flag.doc，里面很长一段

使用base64解码20次就可以得到

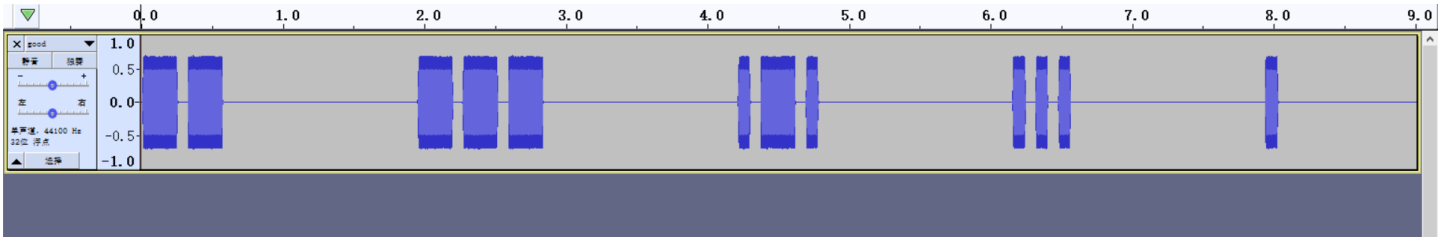
> comEON_YOuAreSOSoS0great

作为密码解压最后一个压缩包

然后得到一个good.mp3

打开一听，觉得像摩斯密码

将文件拉到Audacity



得到电码为

> – — .-. … . … … …- . .-. -.-- …- . .-. -.-- . .- … -.–

通过网站解密，得到flag

```
flag{morseisveryveryeasy}
```