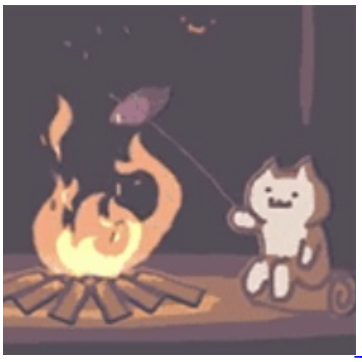
第四届2021美团网络安全 MT-CTF writeup

原创

shu天 于 2021-12-12 22:47:55 发布

分类专栏： ctf # misc 文章标签： ctf misc



ctf 同时被 2 个专栏收录

80 篇文章 4 订阅

订阅专栏

misc

7 篇文章 0 订阅

订阅专栏

第四届2021美团网络安全 MT-CTF

文章目录

MISC

Un(ix)zip


```
└─$ unzip UNZIP.zip
Archive:  UNZIP.zip
   creating: ppp/
   creating: ppp/0/
   creating: ppp/1/
 extracting: ppp/1/15
 extracting: ppp/1/18
 extracting: ppp/1/26
   creating: ppp/2/
   creating: ppp/3/
 extracting: ppp/3/6
   creating: ppp/4/
   creating: ppp/5/
   creating: ppp/6/
   creating: ppp/7/
   creating: ppp/8/
   creating: ppp/9/
 extracting: ppp/9/36
   creating: ppp/A/
   creating: ppp/B/
   creating: ppp/C/
   creating: ppp/D/
   creating: ppp/E/
   creating: ppp/F/
```

F28

	A	B	C	D
1	Column2.1	Column2.2	Column2.3	
2	ppp	Z	1	
3	ppp	m	2	
4	ppp	x	3	
5	ppp	h	4	
6	ppp	Z	5	
7	ppp	3	6	
8	ppp	t	7	
9	ppp	X	8	
10	ppp	Z	9	
11	ppp	W	10	
12	ppp	x	11	
13	ppp	j	12	
14	ppp	M	13	
15	ppp	G	14	
16	ppp	1	15	
17	ppp	I	16	
18	ppp	X	17	
19	ppp	1	18	
20	ppp	V	19	
21	ppp	u	20	
22	ppp	e	21	
23	ppp	j	22	
24	ppp	F	23	
25	ppp	w	24	
26	ppp	X	25	
27	ppp	1	26	
28	ppp	d	27	
29	ppp	v	28	


```
1  ZmxhZ3tXZWxjMG1lX1VuejFwX1dvbmRlcjR9
```

常规Base64 | CSS Base64 | DES加密/解密 | 3DES加密/解密 | AES加密/解密 | RSA加密/解密

flag{Welc0me_Unz1p_Wonder4}

오징어 게임 鱿鱼游戏

7-zip可以看到加密算法ZipCrypto Store

3.2 ZIP已知明文攻击的深入利用

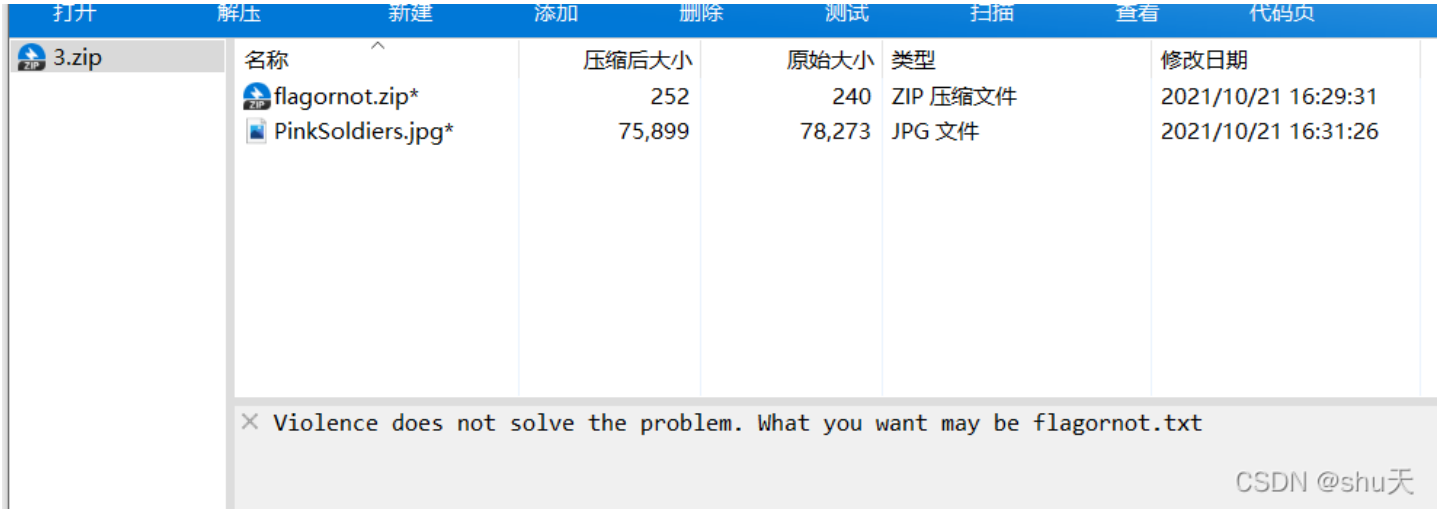
本文要探讨的攻击方法并不需要知道压缩文件中完整的明文，只需在已知加密压缩包中的少部分明文字节时即可进行攻击破解。而各类文件都有其自身固定的文件格式，结合这类格式，极大扩展了ZIP明文攻击的攻击面

破解。而各类文件都有其自身固定的文件格式，结合这类格式，极大扩展了ZIP明文攻击的攻击面。

具体要求如下：

- 至少已知明文的12个字节及偏移，其中至少8字节需要连续。
- 明文对应的文件加密方式为ZipCrypto Store

再加上备注里提示flagornot.txt，采用明文爆破



明文爆破参考：https://blog.csdn.net/q851579181q/article/details/109767425

工具下载：bkcrack：https://github.com/kimci86/bkcrack

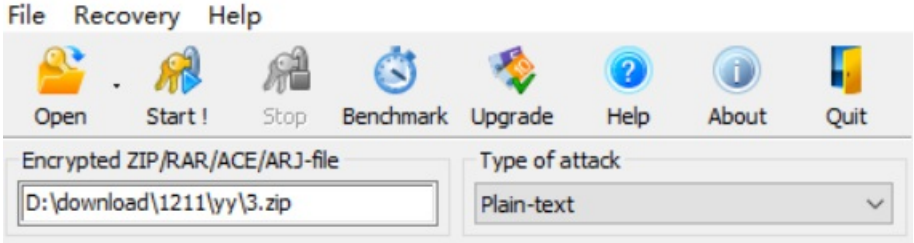
```
./bkcrack -C 3.zip -c flagornot.zip -p p.txt  -o 30  -x 0 504B0304

#Keys: 683a571e f954e70c 49da18ac
```

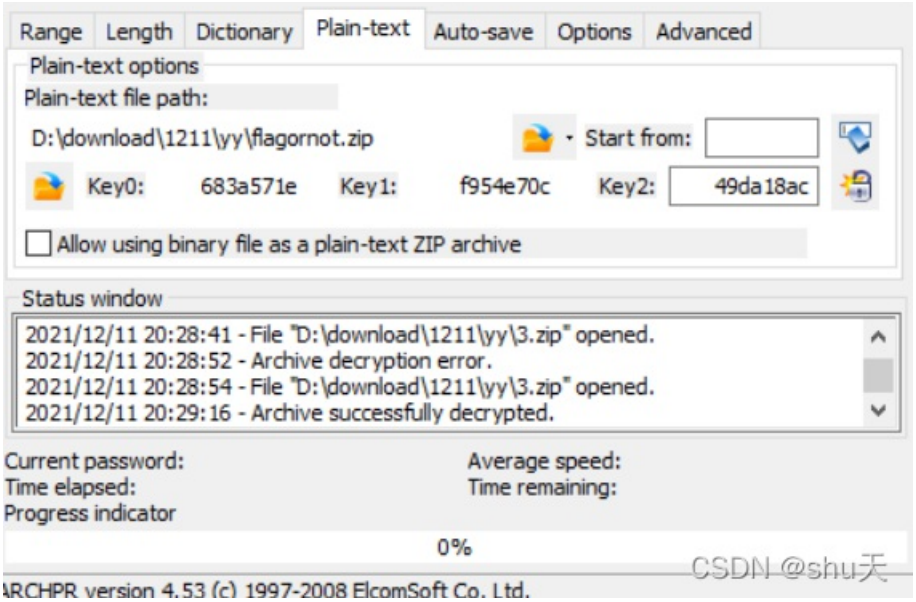
```
p3@p3-virtual-machine:~/ctftool/bkcrack-1.3.3-Linux$ ./bkcrack -C 3.zip -c flagornot.zip -p p.txt  -o 30  -x 0 504B0304
bkcrack 1.3.3 - 2021-11-08
[17:30:18] Z reduction using 5 bytes of known plaintext
100.0 % (5 / 5)
[17:30:19] Attack on 1144559 Z values at index 37
Keys: 683a571e f954e70c 49da18ac
65.7 % (752358 / 1144559)
[17:59:47] Keys
683a571e f954e70c 49da18ac
```

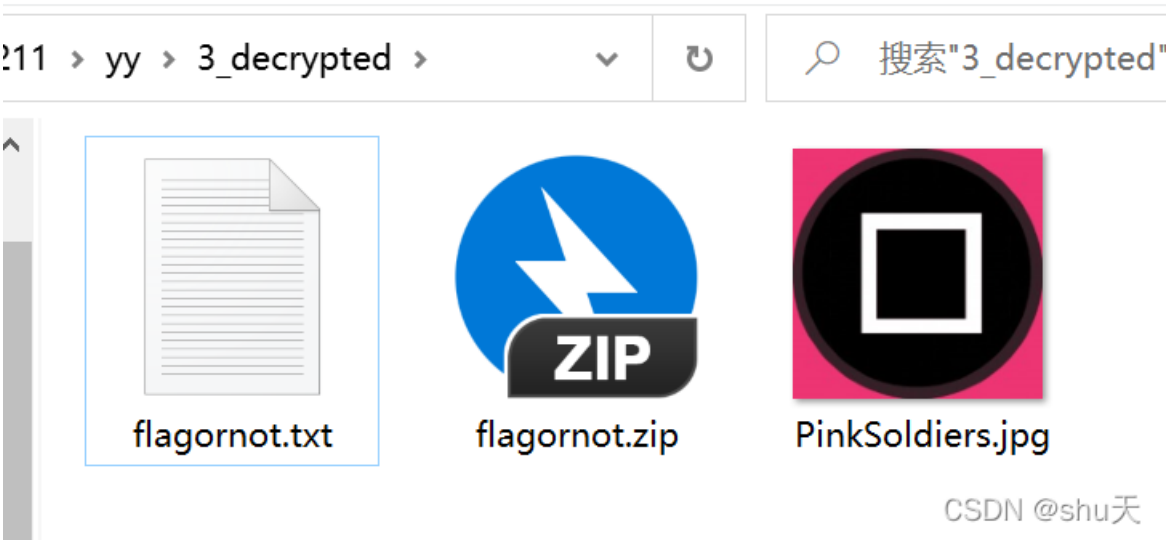


```
./bkcrack -C "/home/p3/ctftool/bkcrack-1.3.3-Linux/3.zip" -c flagornot.zip -k 683a571e f954e70c 49da18ac -d 1.zip
```

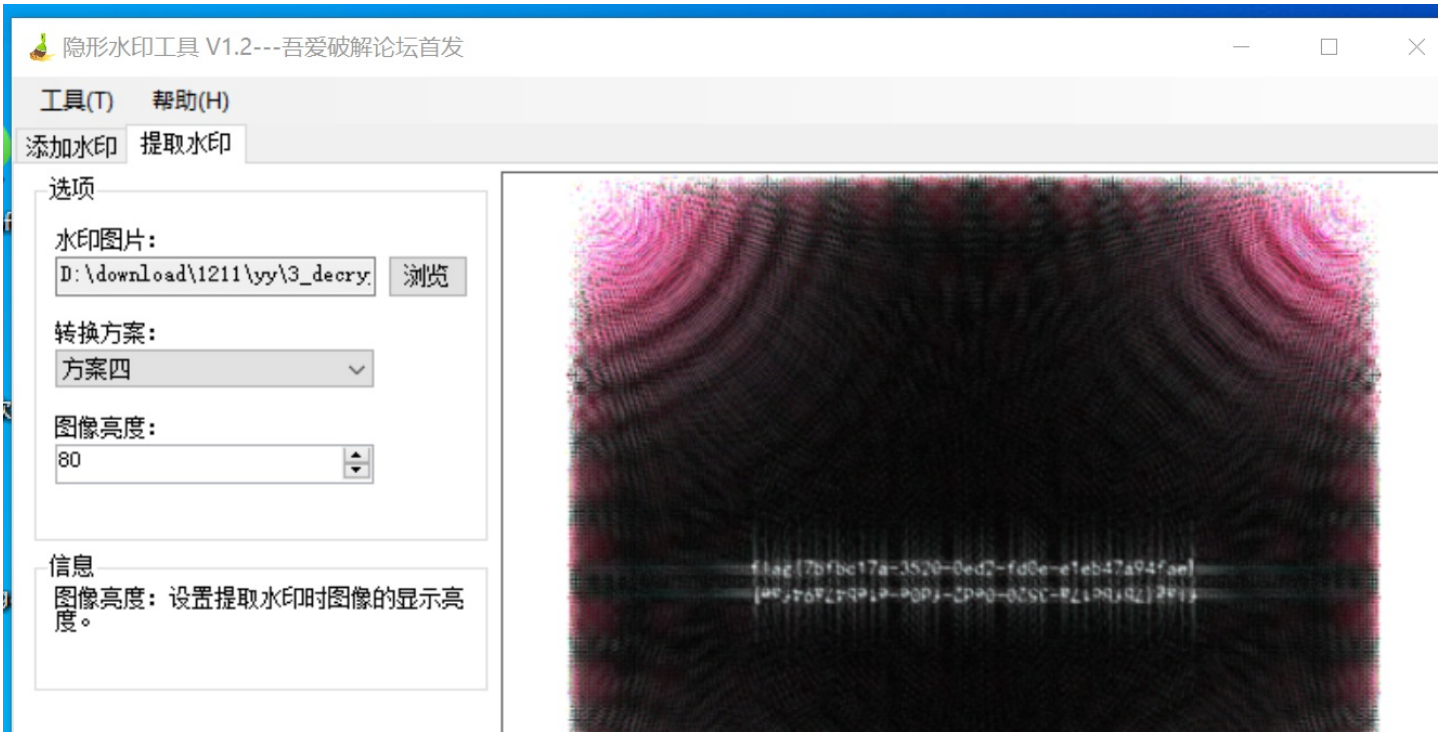
```
p3@p3-virtual-machine:~/ctftool/bkcrack-1.3.3-Linux$ ./bkcrack -C "/home/p3/ctftool/bkcrack-1.3.3-Linux/3.zip" -c flagornot.zip -k
683a571e f954e70c 49da18ac -d 1.zip
bkcrack 1.3.3 - 2021-11-08
[18:52:46] Writing deciphered data 1.zip (maybe compressed)
Wrote deciphered data.
```

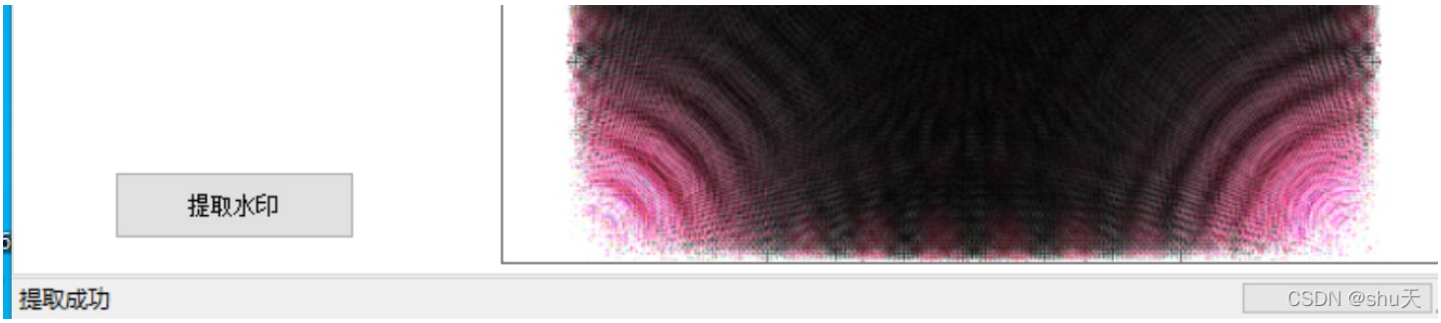






然后是图片盲水印提取，比赛的时候没做出来





Boom

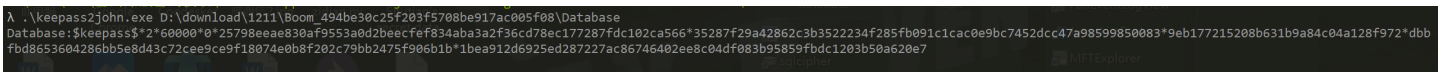

```
shen@DESKTOP-4R7ESOT:/mnt/d/download/1211/Boom_494be30c25f203f5708be917ac005f08$ file Database
Database: Keepass password database 2.x KDBX
```

发现是 Keepass的数据库

Hashcat进行Keepass密码爆破：https://luxswf.github.io/2020/05/14/Hashcat%E7%88%86%E7%A0%B4/
https://www.rubydevices.com.au/blog/how-to-hack-keepass

1.利用John the Ripper 解析出Hash值

```
keepass2john.exe Database
# $keepass$*2*60000*0*25798eeae830af9553a0d2beecfef834aba3a2f36cd78ec177287fdc102ca566*35287f29a42862c3b3522234f285fb091c1cac0e9bc7452dcc47a98599850083*9eb177215208b631b9a84c04a128f972*dbbfbd8653604286bb5e8d43c72cee9ce9f18074e0b8f202c79bb2475f906b1b*1bea912d6925ed287227ac86746402ee8c04df083b95859fbdc1203b50a620e7:
```

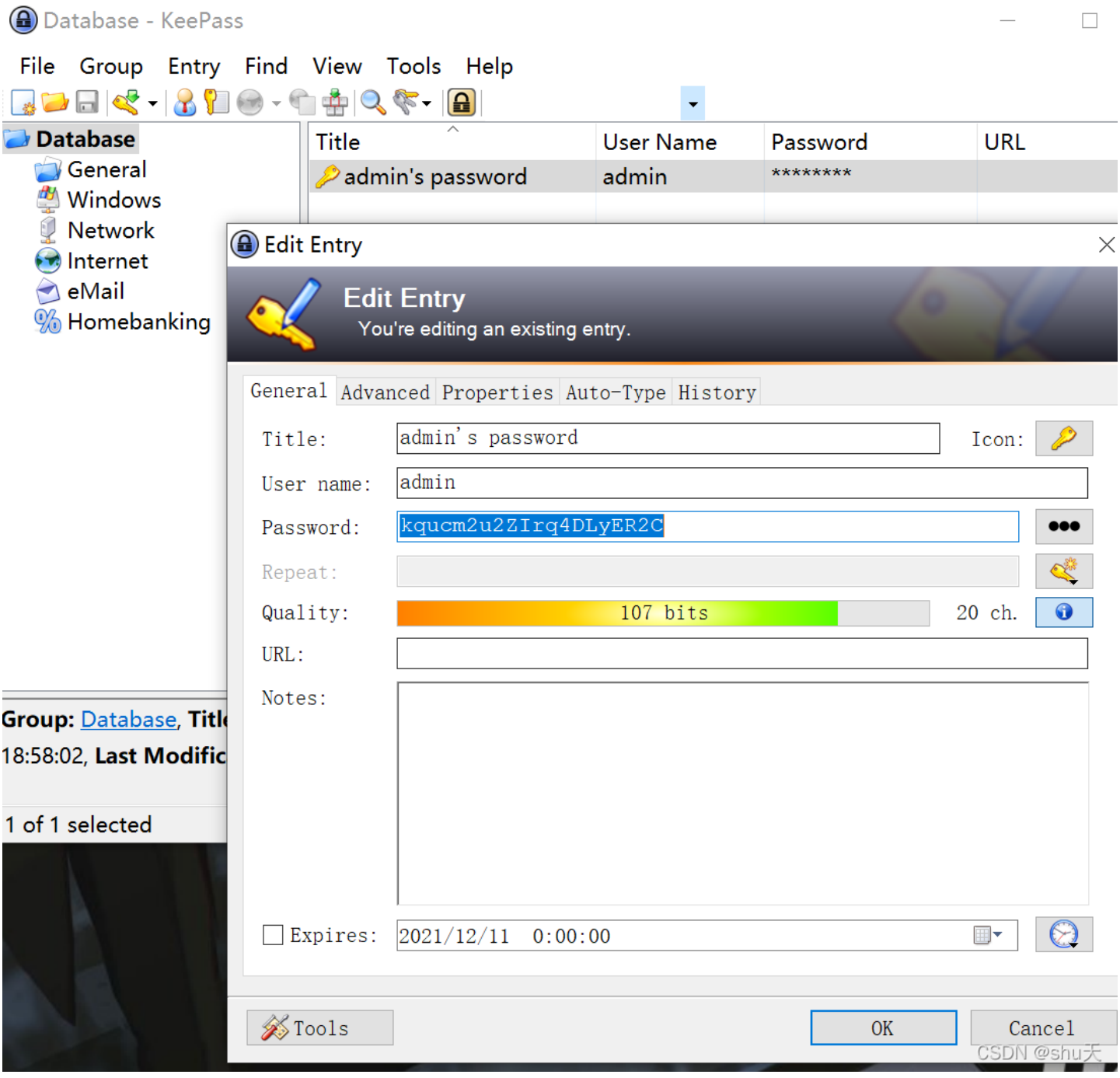


Hashcat破解Hash值

```
Hashcat64.exe -m 13400 hash.txt -a0 wordlist.dic -o found.txt
```

```
$keepass$*2*60000*0*25798eeae830af9553a0d2beecfef834aba3a2f36cd78ec177287fdc
102ca566*35287f29a42862c3b3522234f285fb091c1cac0e9bc7452dcc47a98599850083*9
eb177215208b631b9a84c04a128f972*dbbfbd8653604286bb5e8d43c72cee9ce9f18074e0
b8f202c79bb2475f906b1b*1bea912d6925ed287227ac86746402ee8c04df083b95859fbdc
1203b50a620e7:
```


发现密码是个换行符(*￣m￣)



解压密码kqucm2u2ZIrq4DLyER2C，解压得到flag.png

zsteg分析png隐写

```
zsteg -a [png图片]
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ zsteg -a  /home/kali/Desktop/flag.png
[?] 27109 bytes of extra data after image end (IEND), offset = 0x20290
extradata:0         ..
    00000000: 00 00 00 00 1a 07 01 00  12 7a c7 73 0b 01 05 07  |.........z.s....|
    00000010: 00 06 01 01 d6 d2 81 00  74 27 b9 59 5d 02 03 3c  |........t'.Y]..<|
    00000020: c0 d1 01 04 e3 9e 02 20  a9 86 ae 7e 80 03 00 0e  |....... ...~....|
    00000030: 66 69 6e 61 6c 2f 66 6c  61 67 2e 70 6e 67 30 01  |final/flag.png0.|
    00000040: 00 03 0f 04 bb 00 50 16  09 47 c4 11 05 0c e0 29  |......P..G.....)|
    00000050: aa e3 be e5 f1 4a 7c 0d  af 25 d4 86 33 d4 fb 82  |.....J|..%..3...|
    00000060: f7 97 47 3c 39 73 a5 ee  8b 3c c2 8d 54 6f 82 0a  |..G<9s...<..To..|
    00000070: 03 02 bf dc 64 bd ba de  d7 01 d9 3e 73 62 e4 a4  |....d......>sb..|
    00000080: 57 ae 50 24 10 58 80 0d  5f b6 8f a1 2f 93 8b ba  |W.P$.X.._.../...|
    00000090: 17 eb a2 7a 4e bd 23 25  72 bb fd 7c d9 af 2d 5f  |...zN.#%r..|..-_|
    000000a0: 01 62 35 5f f0 8d 53 c4  c6 62 8e 28 10 4b 6c 25  |.b5_..S..b.(.Kl%|
    000000b0: 23 1d 04 fc 32 fe c3 82  6b 89 55 a4 03 19 e0 c4  |#...2...k.U.....|
    000000c0: fe 3d f8 21 31 c9 53 26  83 7e 63 8e bc ff 01 1f  |•=.!1.S&.~c.....|
    000000d0: 45 d5 34 13 f6 10 4f 07  e2 c8 d7 77 81 d8 f0 e2  |E.4...O....w....|
    000000e0: d6 a8 88 0b 53 c9 92 22  a6 fc 6d 2a 0f 3d 7f c0  |....S.."..m*•=..|
    000000f0: 23 6a 14 02 32 76 de 89  d6 35 63 90 b0 11 4a 27  |#j..2v...5c...J'|
imagedata           ..  text: "HNW@PR$+,"
b2,b,lsb,xy         ..  file: amd 29k coff prebar executable
b3,bgr,lsb,xy       ..  file: PGP Secret Sub-key -
b4,g,msb,xy         ..  text: "wW}ww7=s"
b2,rgb,msb,xy,prime ..  file: SVr4 curses screen image, big-endian
b3,bgr,lsb,yx       ..  file: PGP Secret Sub-key -
b4,rgb,msb,YX       ..  text: "wwwUefUuw"
b4,bgr,msb,YX,prime ..  text: "w733sww'"
b1,bgr,lsb,Xy       ..  text: "?6%.n\"ffl"
b2,r,lsb,Xy         ..  text: "Vs\\\\]V{jGJzVL|{POkFwBv3TCZwMx"
b4,b,msb,Xy         ..  text: "s;7{s;7;"
b1,bgr,lsb,Xy,prime ..  text: "#NYWk7xL_"
b4,bgr,msb,Xy,prime ..  text: ";;;{w7;7"
b4,rgb,msb,yX       ..  text: "wWUfVUwww"
b2,r,lsb,yX,prime   ..  file: AIX core file fulldump 32-bit
b2,g,lsb,yX,prime   ..  file: AIX core file fulldump 32-bit
b2,b,lsb,yX,prime   ..  file: AIX core file fulldump 32-bit
```

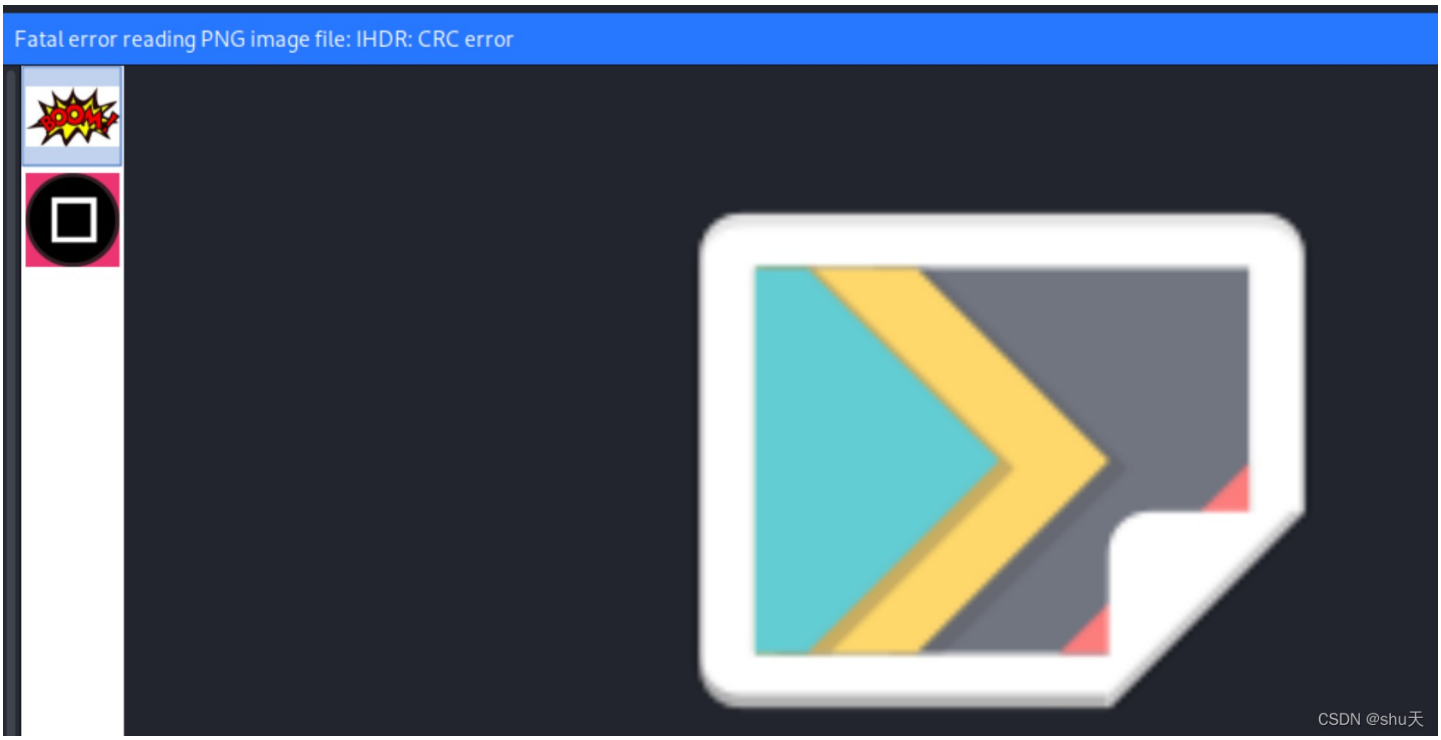

导出数据

```
zsteg -E "extradata:0"  /home/kali/Desktop/flag.png > data
```

有点像是rar压缩包，补上文件头52 61 72 21

```
λ rar2john.exe D:\download\1211\Boom_494be30c25f203f5708be917ac005f08\data12.rar
D:\download\1211\Boom_494be30c25f203f5708be917ac005f08\data12.rar:$rar5$16$04bb0050160947c411050ce029aae3be$15$e5f14a7c0daf25d48633d4fb82f79747$8$3c3973a5ee8b3cc2
```

看了大佬的wp，哈哈，密码是783d793c313030，我是真的想不到，x=y<100，为什么
https://mp.weixin.qq.com/s?__biz=Mzg5NDY4NTc4NQ==&mid=2247484083&idx=1&sn=e28f921dee8b9a95524159556a74989f&chksm=c01a8585f76d0c93fa44f8368465b5953c2b91457dbb7b75683daf810e64e5d8e0b1d3fa6644&mpshare=1&scene=23&srcid=1212Tg9rishWwQX0pSg6dSav&sharer_sharetime=1639297811835&sharer_shareid=2cd15dd5abca7cee0fa30d6c72437d05#rd
解压得到的图片crc错误



crc爆破没出来

Crypto

Symbol

http://detexify.kirelabs.org/classify.html
https://blog.csdn.net/anscor/article/details/80878285

flag{fun_LaTeX_Math}

MD5 32位

fun_LaTeX_Math

e1b217dc3b5e90b237b45e0a636e5a86

flag{e1b217dc3b5e90b237b45e0a636e5a86}