十三届全国大学生信息大赛+强网杯+DASCTF八月V&N出题赛-刷题笔记

原创

水星Sur 于 2020-08-27 13:04:56 发布 1846 收藏 2

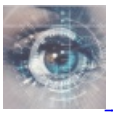
分类专栏： CTF Misc Web 文章标签： 信息安全 python 安全

本文链接：https://blog.csdn.net/pone2233/article/details/108255940


CTF 同时被 3 个专栏收录

20 篇文章 0 订阅

订阅专栏


Misc

22 篇文章 0 订阅

订阅专栏


Web

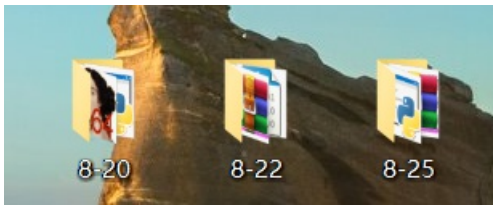
11 篇文章 0 订阅

订阅专栏

文章目录

菜鸟的自白：

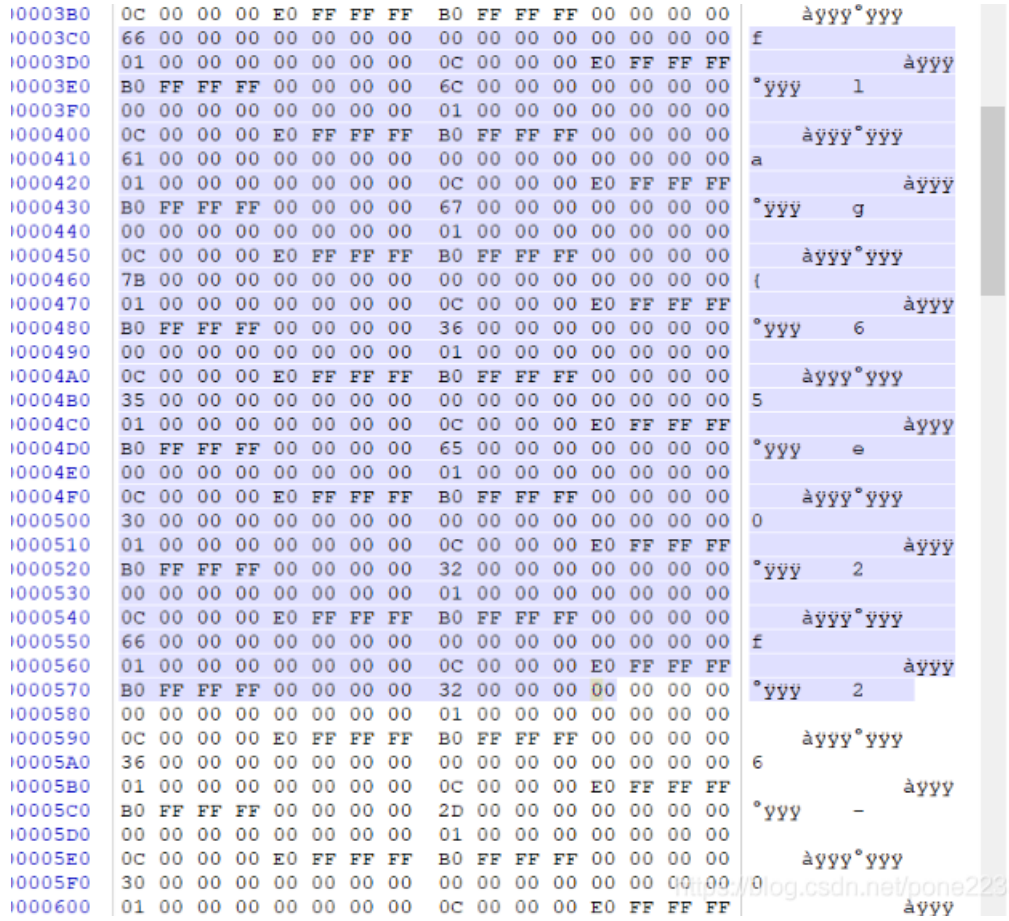
刚开始我还不知道什么是CTF到了大学，有学长带起，慢慢的步入这个信安大世界，我从基础小白，到现在入门小菜鸟，我觉得学习CTF，可以锻炼自己写脚本，看bug，学渗透，不断的充实自己，这次这3个比赛，真的让我发现，自己还是很菜鸟，需要继续锻炼，然后各位加油！下载文件猛如虎，一看战绩0-5，太难了。QWQ



第十三届全国大学生信息安全竞赛

the_best_Ctf_game

放入winhex里面就能看到flag

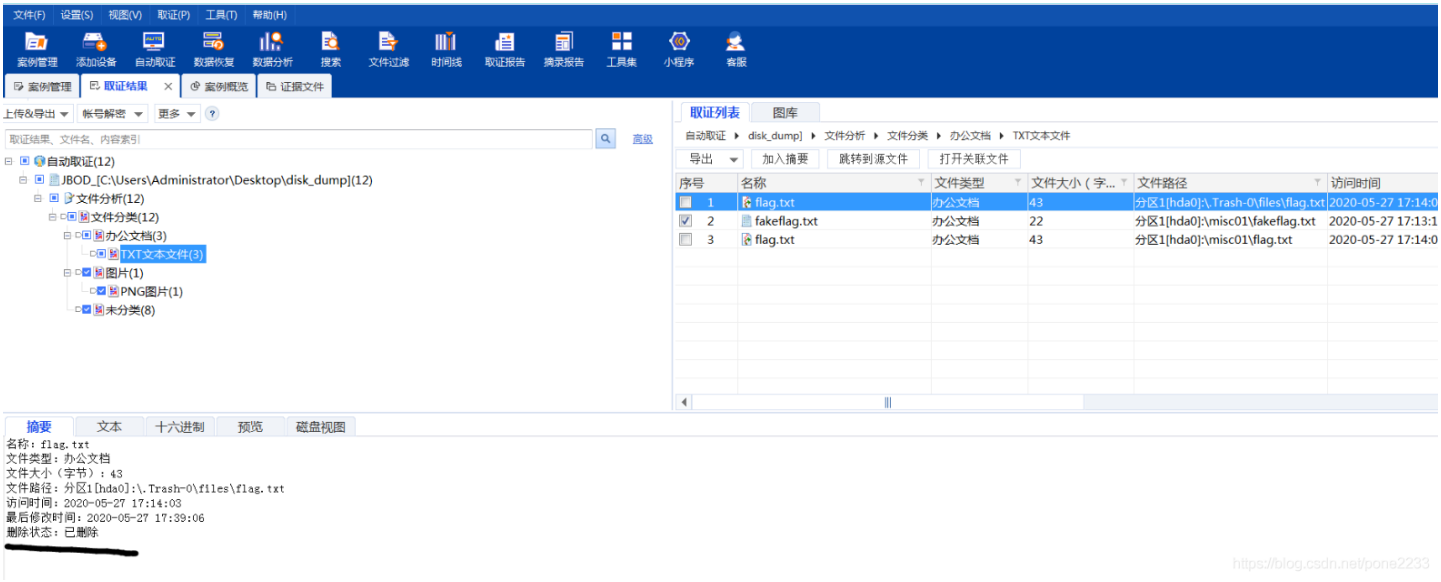


把他复制出来，删除多余的东西，就有了flag了

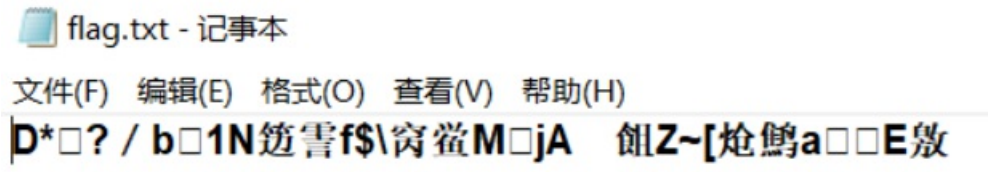
> flag{65e02f26-0d6e-463f-bc63-2df733e47fbe}

电脑被黑

放入取证大师中找到被删除文件



打开一看是某种加密



然后使用binwalk分离一下发现了3样子东西

发现demo里面是一个文件加密程序，我们反编译一下

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax
  char v4; // [rsp+1Dh] [rbp-13h]
  char v5; // [rsp+1Eh] [rbp-12h]
  char v6; // [rsp+1Fh] [rbp-11h]
  FILE *v7; // [rsp+20h] [rbp-10h]
  FILE *stream; // [rsp+28h] [rbp-8h]

  v4 = 34;
  v5 = 0;
  v7 = fopen(argv[1], "rb");
  if ( v7 )
  {
    stream = fopen(argv[1], "rb+");
    if ( stream )
    {
      while ( 1 )
      {
        v6 = fgetc(v7);
        if ( v6 == -1 )
          break;
        fputc(v4 ^ (v5 + v6), stream);
        v4 += 34;
        v5 = (v5 + 2) & 0xF;
      }
      fclose(v7);
      fclose(stream);
      result = 0;
    }
    else
    {
      printf("cannot open file", "rb+", argv);
      result = 0;
    }
  }
}
```

1 重点算法

```
#include <iostream>
#include <stdio.h>
using namespace std;
int main(int argc, char *argv[]) {
  int result; // eax
  char v4; // [rsp+1Dh] [rbp-13h]
  char v5; // [rsp+1Eh] [rbp-12h]
  char v6; // [rsp+1Fh] [rbp-11h]
  FILE *v7; // [rsp+20h] [rbp-10h]
  FILE *stream; // [rsp+28h] [rbp-8h]
  v4 = 34;
  v5 = 0;
  v7 = fopen("flag.txt", "rb");
   stream = fopen("flag.txt", "rb+");
   if ( stream )
   {
    while ( 1 )
    {
     v6 = fgetc(v7);
     if ( v6 == -1 )
      break;
     fputc((v6 ^ v4) - v5, stream);
     v4 += 34;
     v5 = (v5 + 2) & 0xF;
    }
    fclose(v7);
    fclose(stream);
    result = 0;
   }
   else
   {
    printf("cannot open file", "rb+", argv);
    result = 0;
   }
  return result;
}
```

就得到了flag

> flag{e5d7c4ed-b8f6-4417-8317-b809fc26c047}

第四届“强网杯”全国网络安全挑战赛

主动

打开一看发现了system，那就说明可以执行linux代码指令

```php
  <?php
highlight_file("index.php");

if(preg_match("/flag/i",  $_GET["ip"]))
{
        die("no  flag");
}

system("ping  -c  3  $_GET[ip]");

?>
```


我们先使用一下ls查看一下又什么文件然后发现了flag.php

然后试一下使用cat flag.php 不行，给拦截了，那我就换成cat *.php
就成功了


```
?ip=%0a cat *.php
```

upload

下载文件发现是文件分析题目

upload.zip

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式

upload.zip - ZIP 压缩文件, 解包大小为 36,416 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
data.pcapng	36,416	33,287	Wireshark capture file	2020/8/14 22:43	10E2A7A4

老规矩追溯一下tcp然后发现了一个图片

```
-----------------------------290619977245035210337886588 82
Content-Disposition: form-data; name="file"; filename="steghide.jpg"
Content-Type: image/jpeg

......JFIF.............C.

.
.
.....
.. .....'... .)10.)-,3:J>36F7,-
@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5000000000000000000000000000000000000000000000000000000000O.....D...."..................
................
.....................}........!1A..Qa."q.2....#B...R..$3br.
.....
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....................................................................................
.......................
.....................w.......!1..AQ.aq."2...B....       #3R..br.
.$4.
%....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....................................................................................
...........?...\.Uv485Z..*.p+#....k.....=k............QA.Pi.R.ZC@.....R..h....QE..QE..QIE..4.j.......-).ZSY3....p.-8
F.@..SH.i..)(.
((AJ(..6..(<Rb..E.T. .U.b......(..
...`..  }...R..Q.........Qc9U3V...j.G.....t..0.B.O\W|-...F....;.B.60..E.=.H..<v=.S..02c.k..t...o
$;dn...X.p<......Y.}.l...fn.....R.71.\E...j.......v.8..?.Af.H..5..j.:.f
.D.D....h..a....).........bI.......u.x.,.(........Ib...Z....-.....w..SV.!|.e.lf.
B..f0..).........U.9....N....*.A.
..4...Lj...........}+...j.....J.H....c....|....s
.ZD..M.E....xV.r..W...[.y.h...r..j....-U.{8}.6..S..)V.Q....Hj:  ....z...2.ZA...EFjR*3@
.-1i.@.4.N".x.B.:..H)...qMjv.#b.....,.....%1.......a..i.....m......c..._...(.'.ug...bj:...% .4.....(4.......R.E.
%-.R...).SM-..QE..
...T.....uii...Y3...J.)..R4.9...p.k@.R.U..(.F).b.G4...E=jB..0.*.#...8.

F..Nj.u...c..I.Y..H..GZ."y....{.e....E.ePv....d1f5.
.....9.[.:.3n ..U.........S.3..W....H...5.e.I.M.H.....{z.?$8f....9..............[.y#......<.......by.I..6h.;.0...}....
9@'.k.k.....O..x..s..\.....m.j..:U..iq...Q..h..X.fA.N7....S
.B...a\....Ztsc...j..
E...iE:....VHj.&.Y..Fv6....q]..
+..&]......VR.jw3..Z..|.%......\.tE.Vt1....{..klzV..q........`J.......j7.v...jn"..1R..2"4...M.. z..5iH.."..x....7.3.#
分组 3，23 客户端 分组，1 服务器 分组，1 turn(s). 点击选择。
```


导出来还挺骚

重点来了就是他的图片名字，就是一个隐写名字

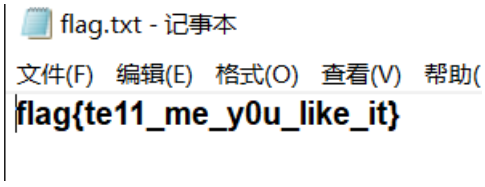
```
----------------------------290619977245035210337886588882
Content-Disposition: form-data; name="file"; filename="steghide.jpg"
Content-Type: image/jpeg
```

弱密码试试就成功了密码 123456

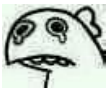
```
E:\>cd E:\桌面\CTF工具包\[隐写工具]steghide

E:\桌面\CTF工具包\[隐写工具]steghide>steghide.exe extract -sf E:\桌面\8-22\data\1.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

E:\桌面\CTF工具包\[隐写工具]steghide>steghide.exe extract -sf E:\桌面\8-22\data\1.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
```



还好手快，抢了题目，到这里为止发现了这个就是PWN杯！！！！太欺负人了



DASCTF 八月浪漫七夕战

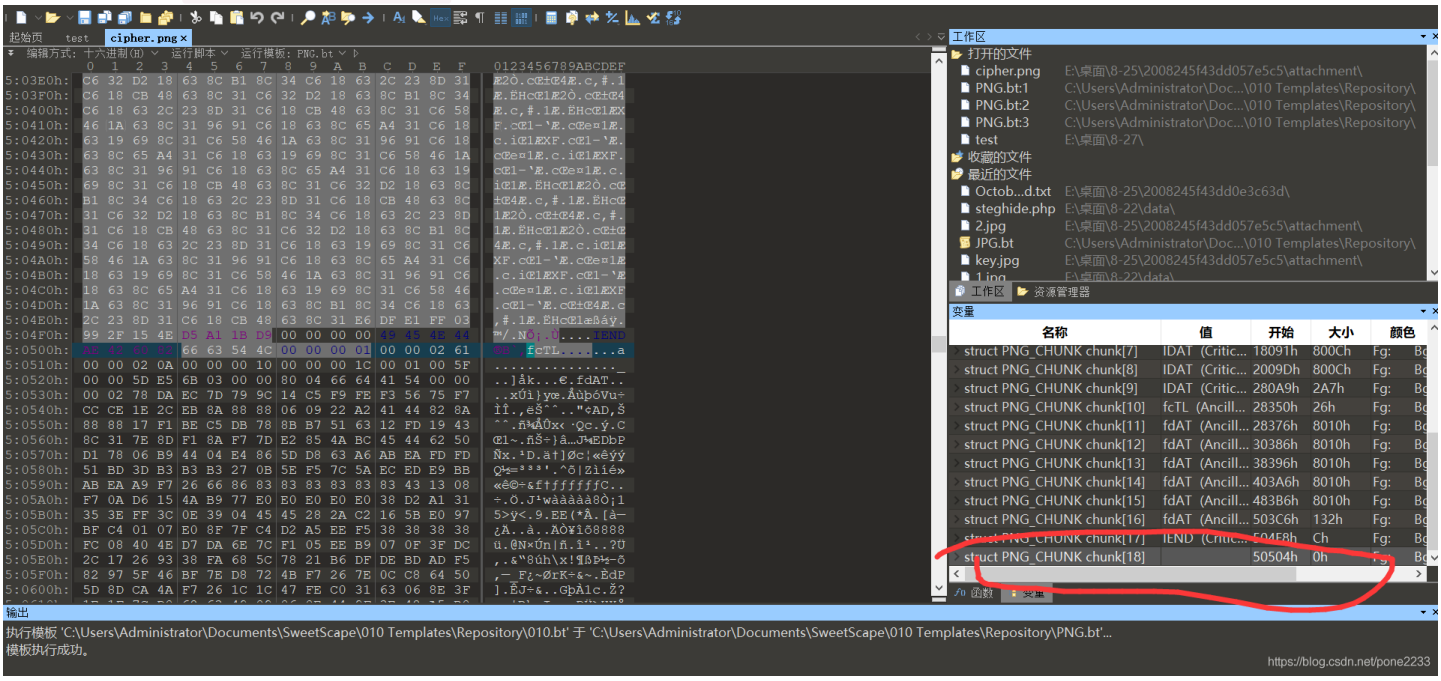
双重图格

下载文件，我们首先检查一下xls，里面是否又夹带
里里外外看了一次，就发现了一个东西

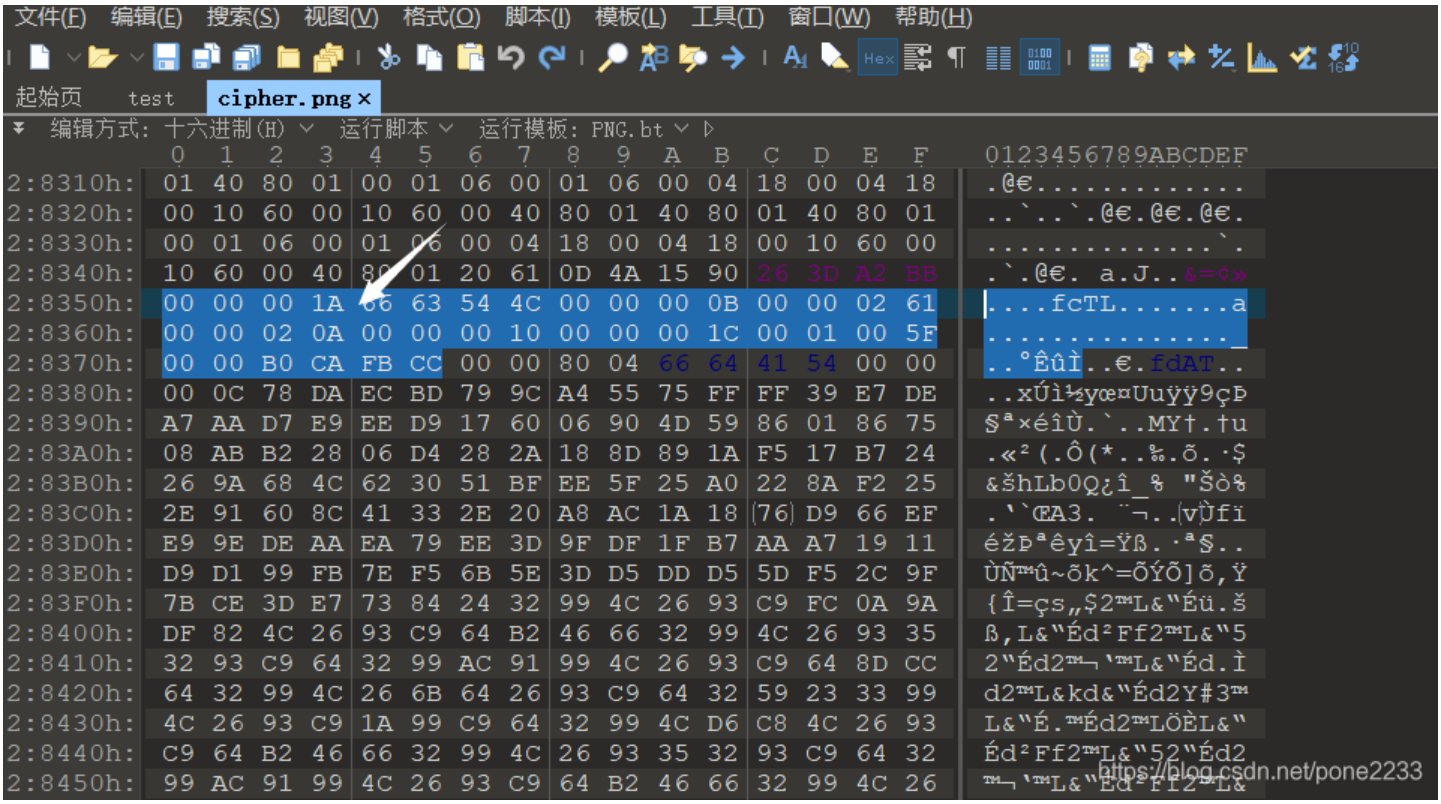
给他加上外衣

Insert:OFFSET 28354h

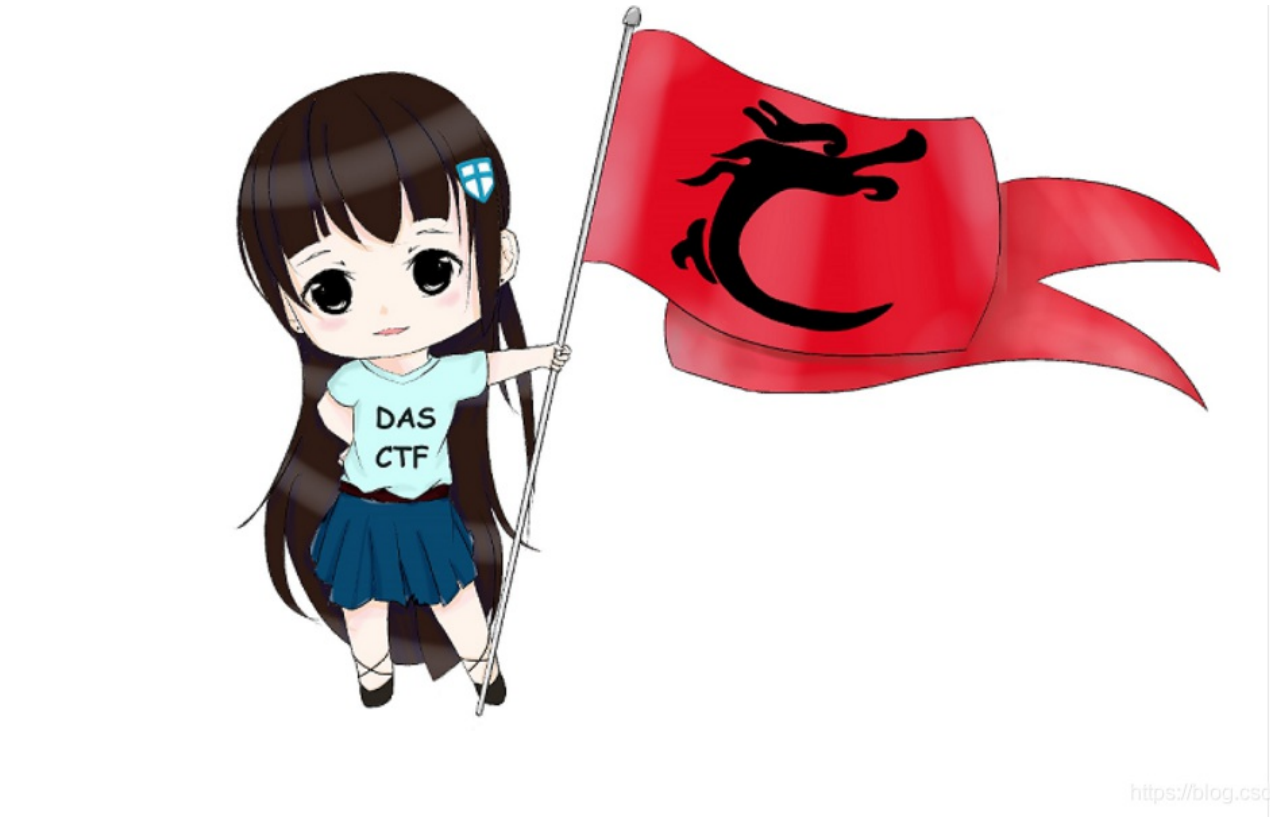
就看的很清楚了`Insert:OFF5ET 28354h`这个词汇翻译一下，就知道位移，在28345H这个为止上面需要位移。



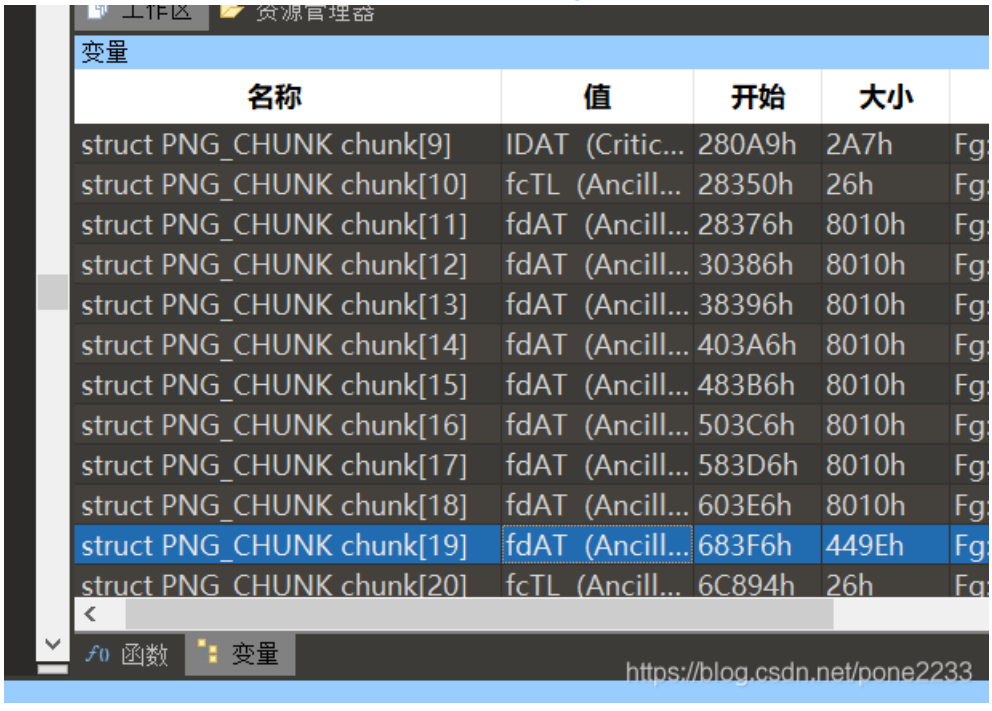
我们首先，让如010里面看，发现一个没有识别的东西，我猜测应该是这个东西需要位移，应该是插入这个位置

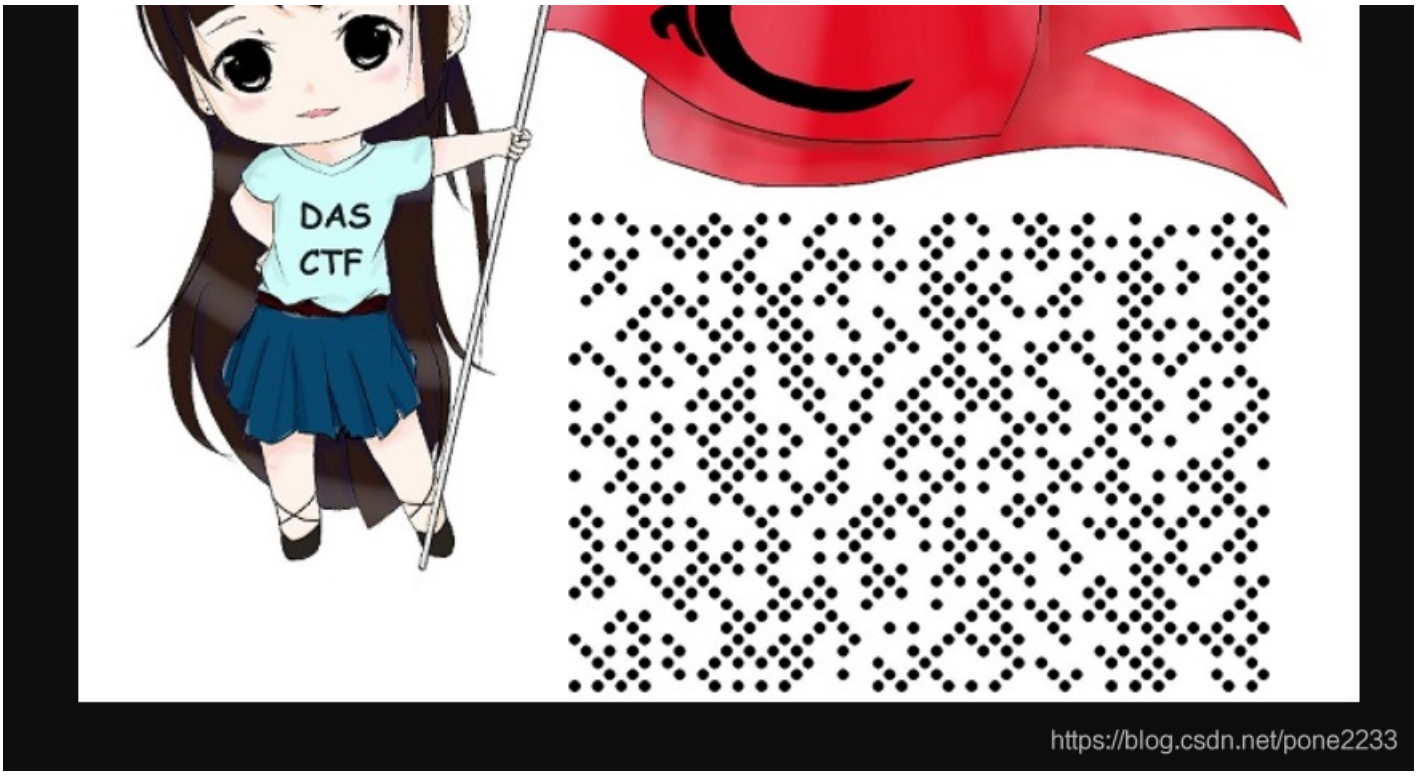


插入之后发现，似乎还是没什么变化，然后在010中发现了



这个fdAT是什么东西然后查一下，找到了APNG，他们说这个是很相似gif然后放入谷歌和火狐里面就可以查看了

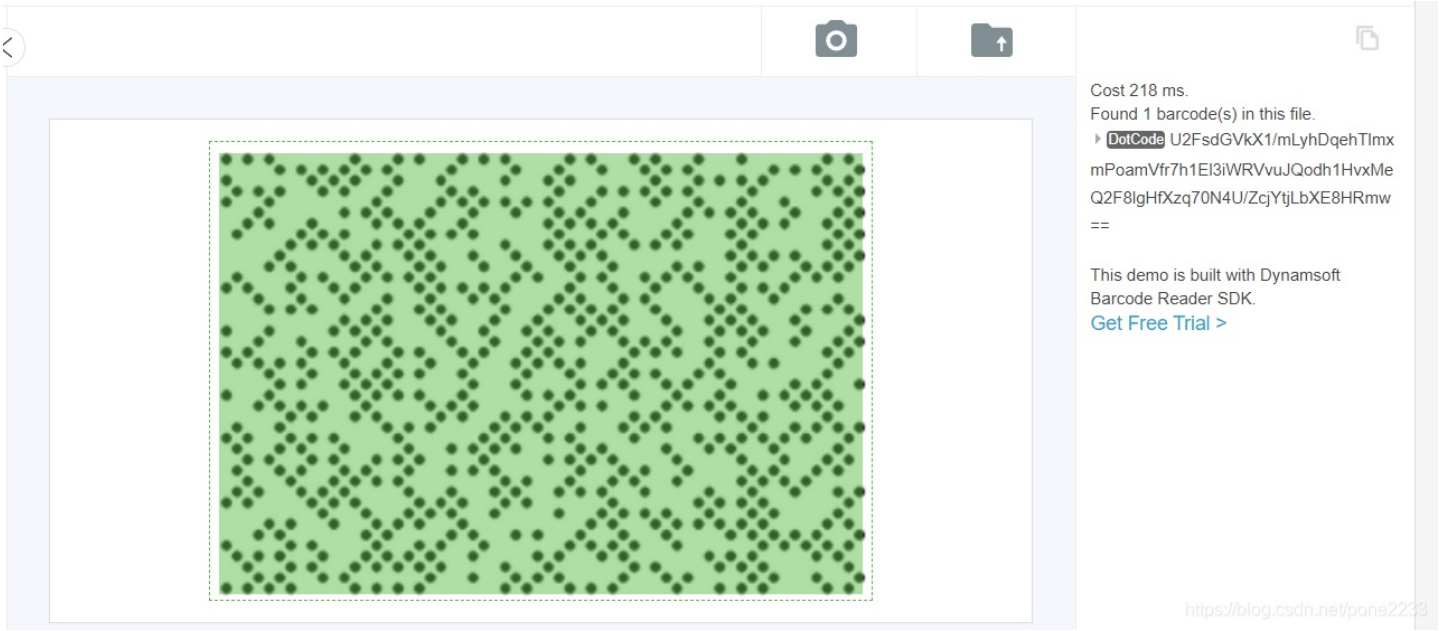




手快就行，然后发现这个点点，起初以为是哪个猪圈密码，后门查一下，发现了是DotCode，也是一种二维码，真的是长见识了

大家可以了解一下DotCode|斐泰二维码

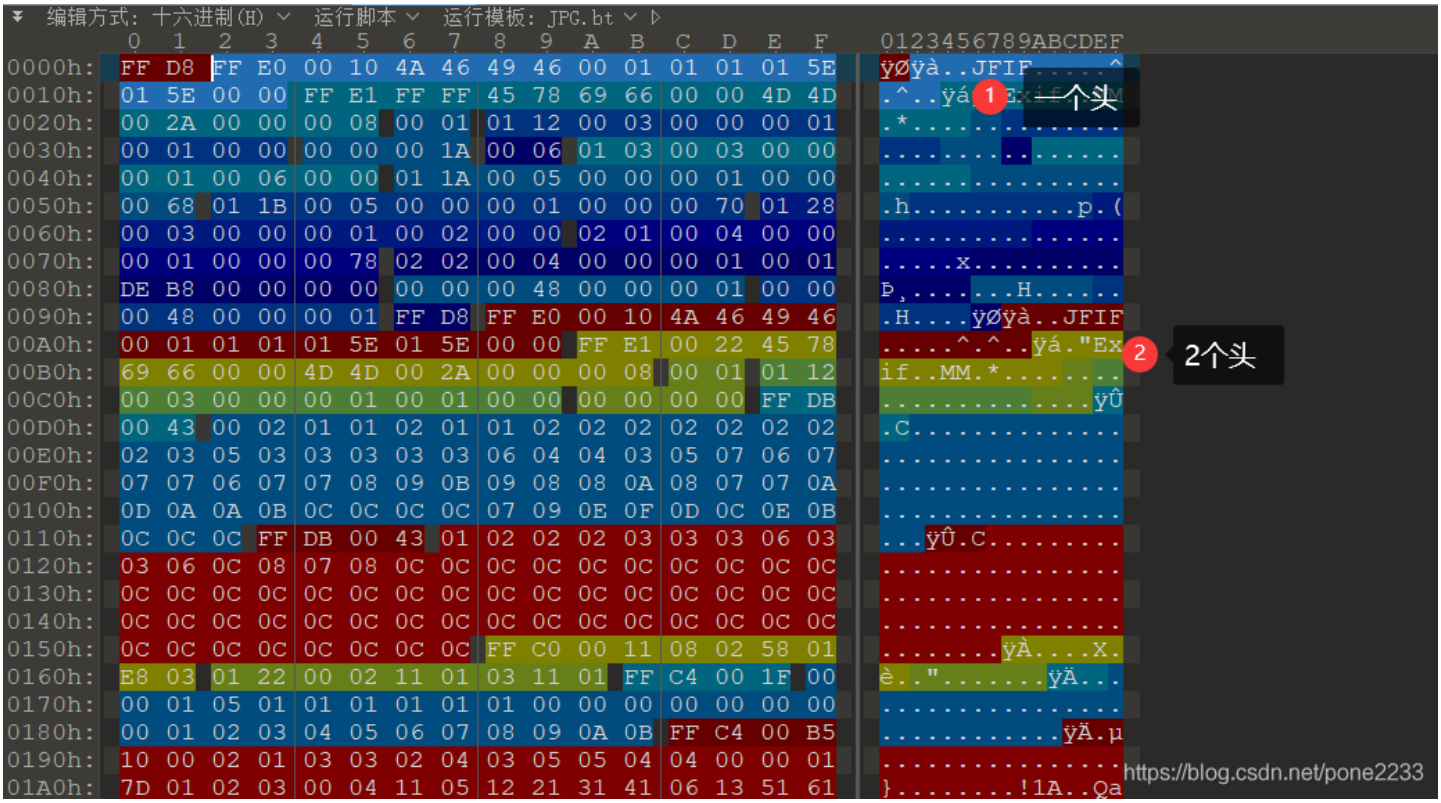
然后，这里就卡住了，然后多谢一个大佬，送的破解网址




```
密文1：U2FsdGVkX1/mLyhDqehTlmxmPoamVfr7h1El3iWRVvuJQodh1HvxMeQ2F8lgHfXzq70N4U/ZcjYtjLbXE8HRmw==
```

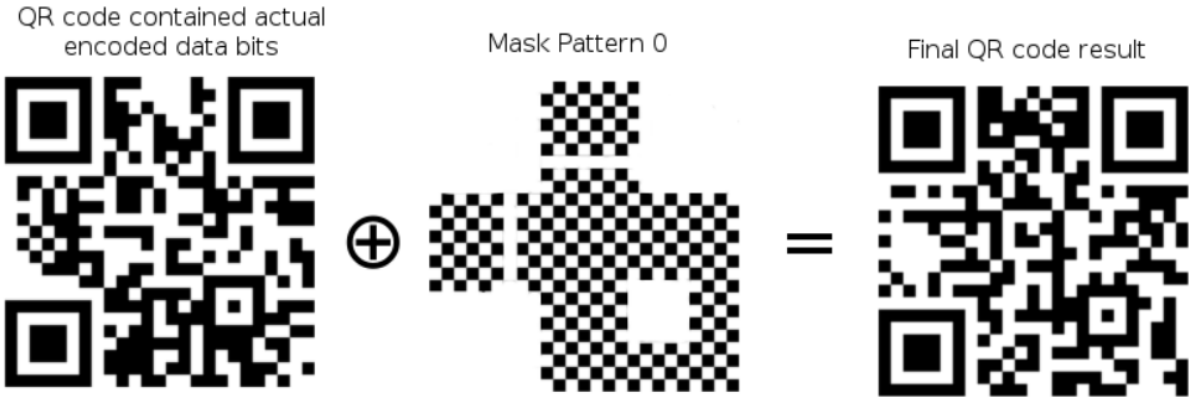
然后接下来就是破解key.jpg 当时尝试了很多jpg的加密都不对，然后这个二维码扫描不出来

然后拖入010觉得很奇怪

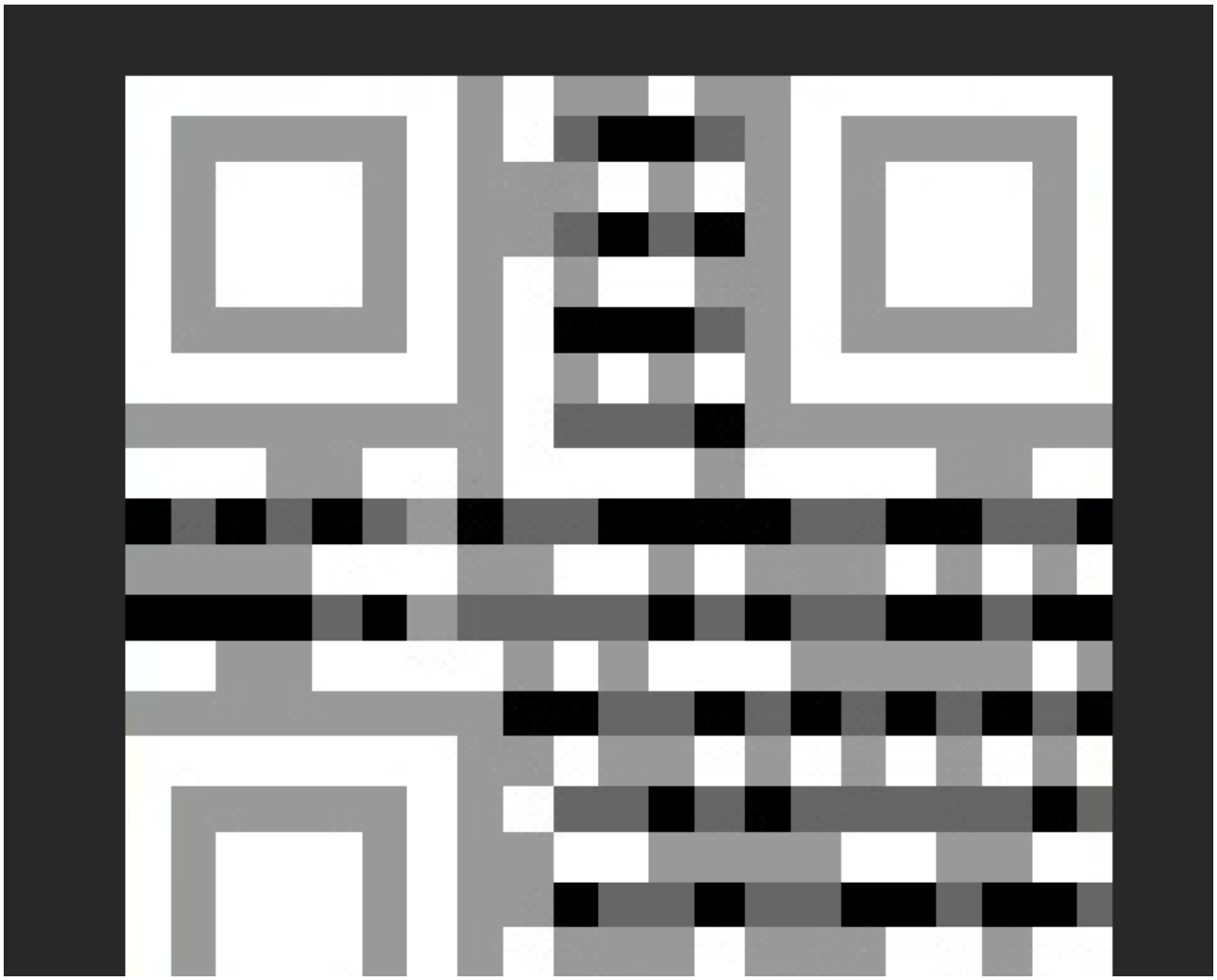


首先删除一个头看看

删除头1，就获得了这个然后这个很明显就是二维码还没有结合
使用PS，进行修复把类似参考这个

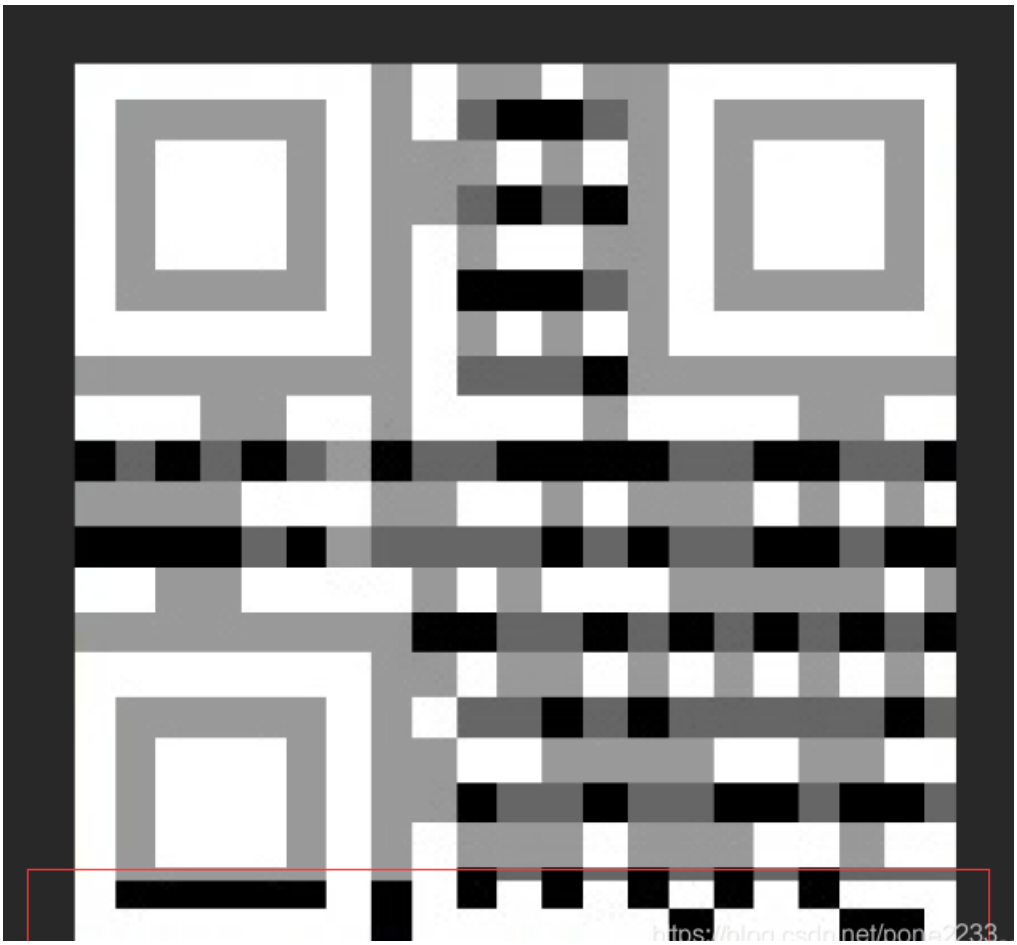


我们首先把2个图片何在一起



我可真实二维码修复第一人哈哈哈，这里因为他给的一个图片有残缺我送大家完好的

和大家说一下流程，首先2张图片对在一起，比对首先先把下面没有的，给取出来



然后就可以操作了，把除了红框里面的进行比对如果颜色深那就把他变成白色，如果浅色变成黑色，然后弄完之后，在加上这个底部进行合并，用魔棒工具取白色变成红色，然后把黑色变成白色，在把红色变成黑色，就成功了

密钥1：apngisamazing

加密/解密 | AES加密/解密 | DES加密/解密 | RC4加密/解密 | Rabbit加密/解密 | TripleDes加密/解密 | MD5加/解密 | Base64加/解密 | Hash加/解密 | JS 加密 | JS 解密

DASCTF{b12e6674e844486d20d24793809ae38a}

apngisamazing

密码是可选项，也就是可以不填。

< 解密 | 加密 >

U2FsdGVkX1/mLyhDqehTlmxmPoamVfr7h1El3iWRVvuJQodh1HvxMeQ2F8lgHfXzq70N4U/ZcjYtjLbXE8HRmw==

> DASCTF{b12e6674e844486d20d24793809ae38a}

在xls发现了一个秘密

core.xml - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties"
xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/" xmlns:dcmitype="http://purl.org/dc/dcmitype/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:creator>G a1@xy</dc:creator><cp:lastModifiedBy>G
a1@xy</cp:lastModifiedBy><dcterms:created xsi:type="dcterms:W3CDTF">2020-07-29T08:58:43Z</dcterms:created><dcterms:modified
xsi:type="dcterms:W3CDTF">2020-07-29T09:27:15Z</dcterms:modified></cp:coreProperties>
```


Ga1@xy师傅出的tql

eeeeeeeasyusb

这道题目和之前做的知识点就在一起了零宽度加密，本来是有网址的，现在似乎给拦截了

那拿出比赛的时候的图把

nut翻译一下就是坚果

https://www.jianguoyun.com/p/DYcbU-gQz_TZCBjh8rID 这个则是密码JmTjTw

然后下载下来，发现2个都是usb数据流量包，我推荐参考这个文章做

https://www.cnblogs.com/ECJTUACM-873284962/p/9473808.html

不过不太准确需要后期修改，

我们先把usb的信息提取出来

```
tshark -r part1.pcapng -T fields -e usb.capdata >data1.txt
tshark -r part2.pcapng -T fields -e usb.capdata >data2.txt
```

这边，我卡了很久，应为他的脚本都很有问题，然后技能尚浅，所以脚本有点不太会改
我这边推荐一个师傅的博客大家可以看一下
http://www.fzwjscj.xyz/index.php/archives/38/#eeeeeeeeasyusb
在这个师傅这个里边学边敲，还是很方便的，我建议可以保存一波，然后我这边送大家一个画图的脚本把

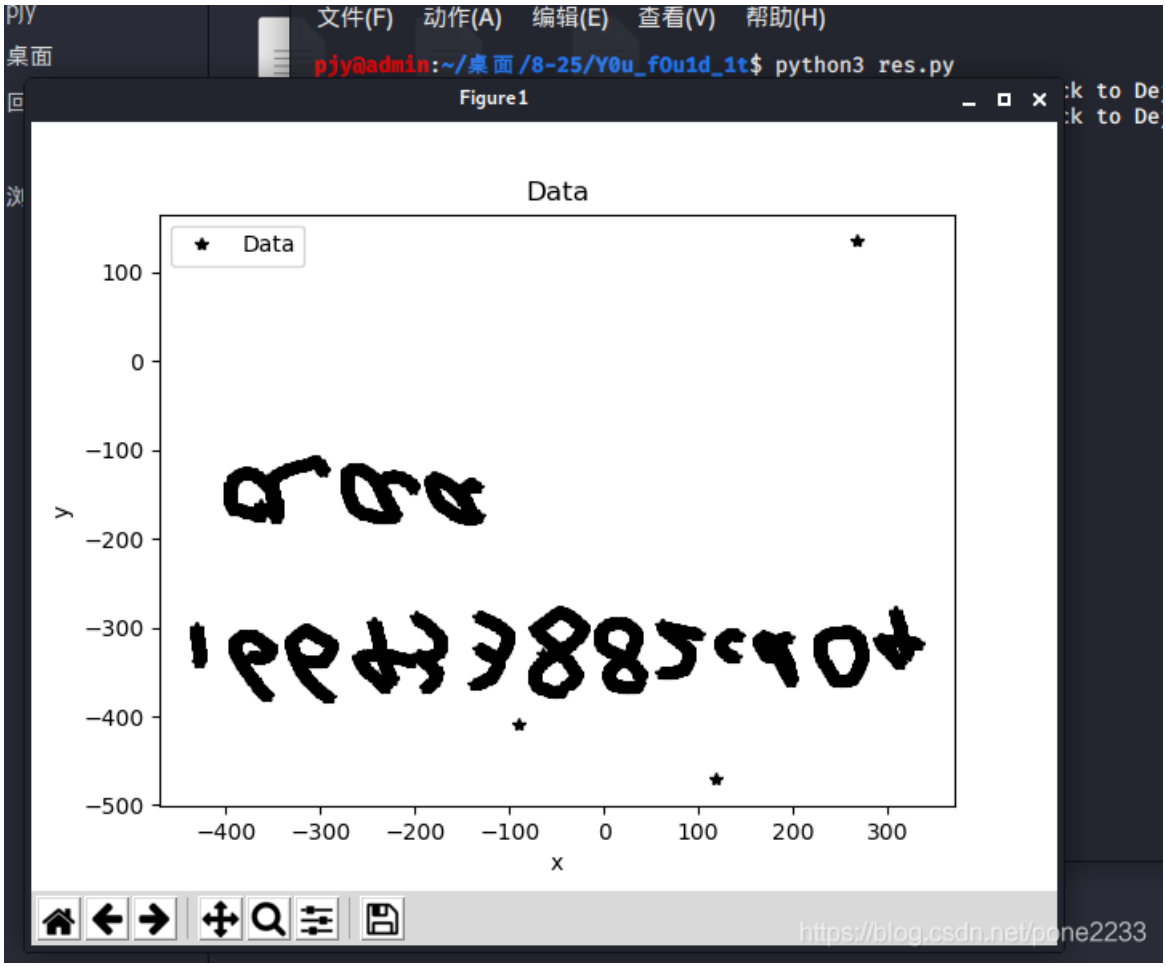
```
#!/usr/bin/python
# coding: utf-8
import matplotlib.pyplot as plt
import numpy as np
import matplotlib as mpl

mpl.rcParams['font.family'] = 'sans-serif'
mpl.rcParams['font.sans-serif'] = 'NSimSun,Times New Roman'

x, y = np.loadtxt('res.txt', delimiter=' ', unpack=True)
plt.plot(x, y, '*', label='Data', color='black')

plt.xlabel('x')
plt.ylabel('y')
plt.title('Data')
plt.legend()
plt.show()
```

然后就有图了



推荐反一下看：`166433882cd04aaa`

在然后分析第二个文件，第二个文件很明显就少很多信息，就应该是键盘了，然后键盘脚本，我自己码，把虚拟机码炸了，太恐怖了，我太菜了

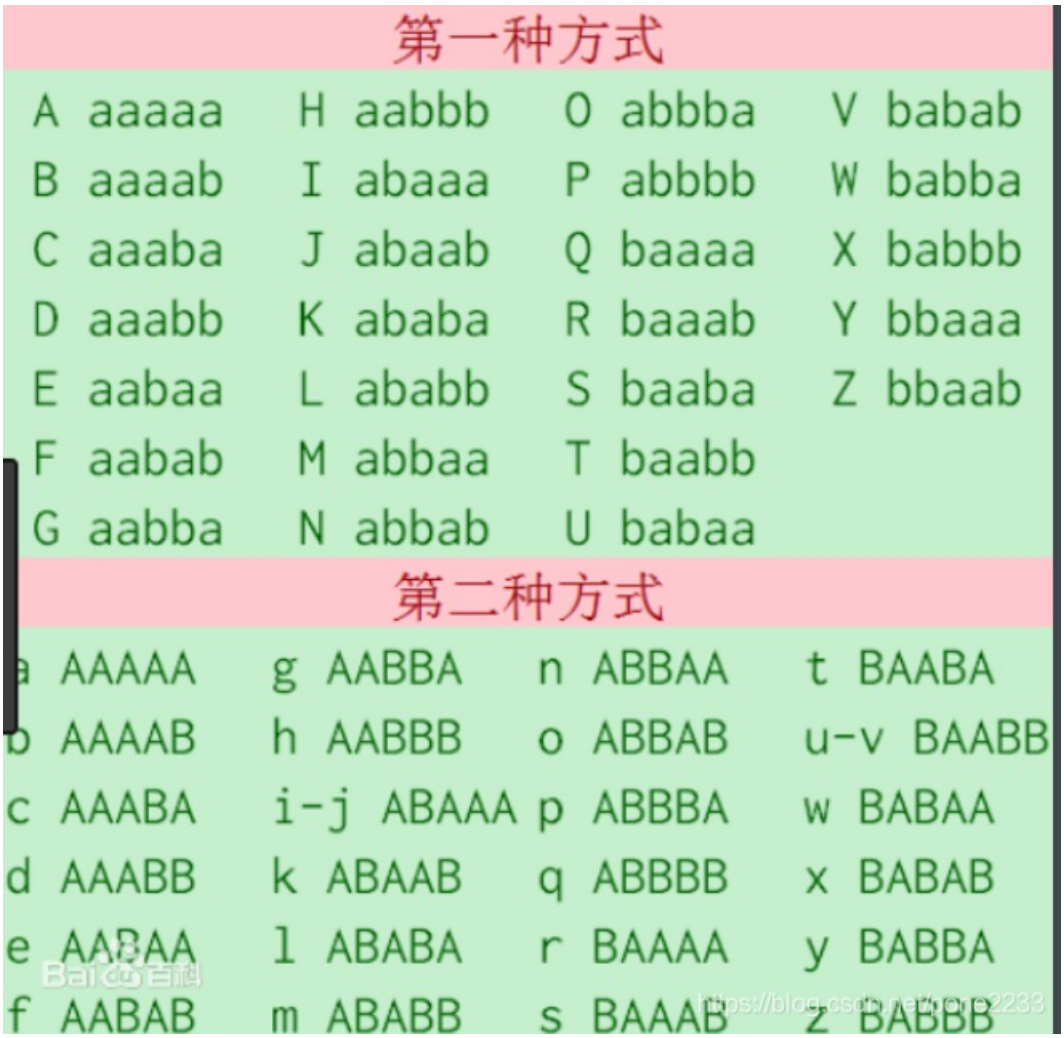
然后还是哪里哪个师傅的脚本，存了，感谢师傅

```
all.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/libwsutil11_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/libwiretap10_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/libwireshark13_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/wireshark-qt_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/tshark_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/wireshark-common_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 无法下载 http://http.kali.org/kali/pool/main/w/wireshark/wireshark_3.2.3-1_i386.deb  404  Not Found [IP: 192.99.200.113 80]
E: 有几个软件包无法下载，要不运行 apt-get update 或者加上 --fix-missing 的选项再试试？
pjy@admin:~/桌面/8-25/Y0u_fOu1d_1t$ python2 data2.py
  File "data2.py", line 8
SyntaxError: Non-ASCII character '\xe9' in file data2.py on line 8, but no encoding declared; see http://python.org/dev/peps/pep-0263/ for details
pjy@admin:~/桌面/8-25/Y0u_fOu1d_1t$ python2 data2.py
output :n056<F2><F2><F2><F2><F3><F2><F2><F2><F3><F3>4<F2><F2><F2><F2><F2><F2><F2><F2><F3><F3>29<F2><F2><F2><F2><F3><F2><F2><F2><F2><F3>522<F2><F2><F2><F2><F3>
pjy@admin:~/桌面/8-25/Y0u_fOu1d_1t$
```



```
output :n056<F2><F2><F2><F2><F3><F2><F2><F2><F3><F3>4<F2><F2><F2><F2><F2><F2><F2><F2><F3><F3>29<F2><F2><F2><F2><F3><F2><F2><F2><F2><F3>522<F2><F2><F2><F2><F3>
```

然后这个这种东西当时看，还以为是莫斯，然后发现数量对不上，最后后知后觉的发现了是培根加密




```
056bd4ad29bb522b
```

> 最终flag是：166433882cd04aaa056bd4ad29bb522b

参考文献

这里由衷的感谢这位师傅，让我没卡住！

师傅1：http://www.fzwjscj.xyz/index.php/archives/38/

师傅2：https://www.cnblogs.com/ECJTUACM-873284962/p/9473808.html