

buu刷题7.14

原创

[GrapeSour](#)  于 2021-07-14 22:12:19 发布  42  收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/GrapeSour/article/details/118726679>

版权

BUU---7.14

[\[MRCTF2020\]ezmisc](#)

[弱口令](#)

[\[GUET-CTF2019\]KO](#)

[\[HBNIS2018\]caesar](#)

[\[HBNIS2018\]低个头](#)

[john-in-the-middle](#)

[\[ACTF新生赛2020\]NTFS数据流](#)

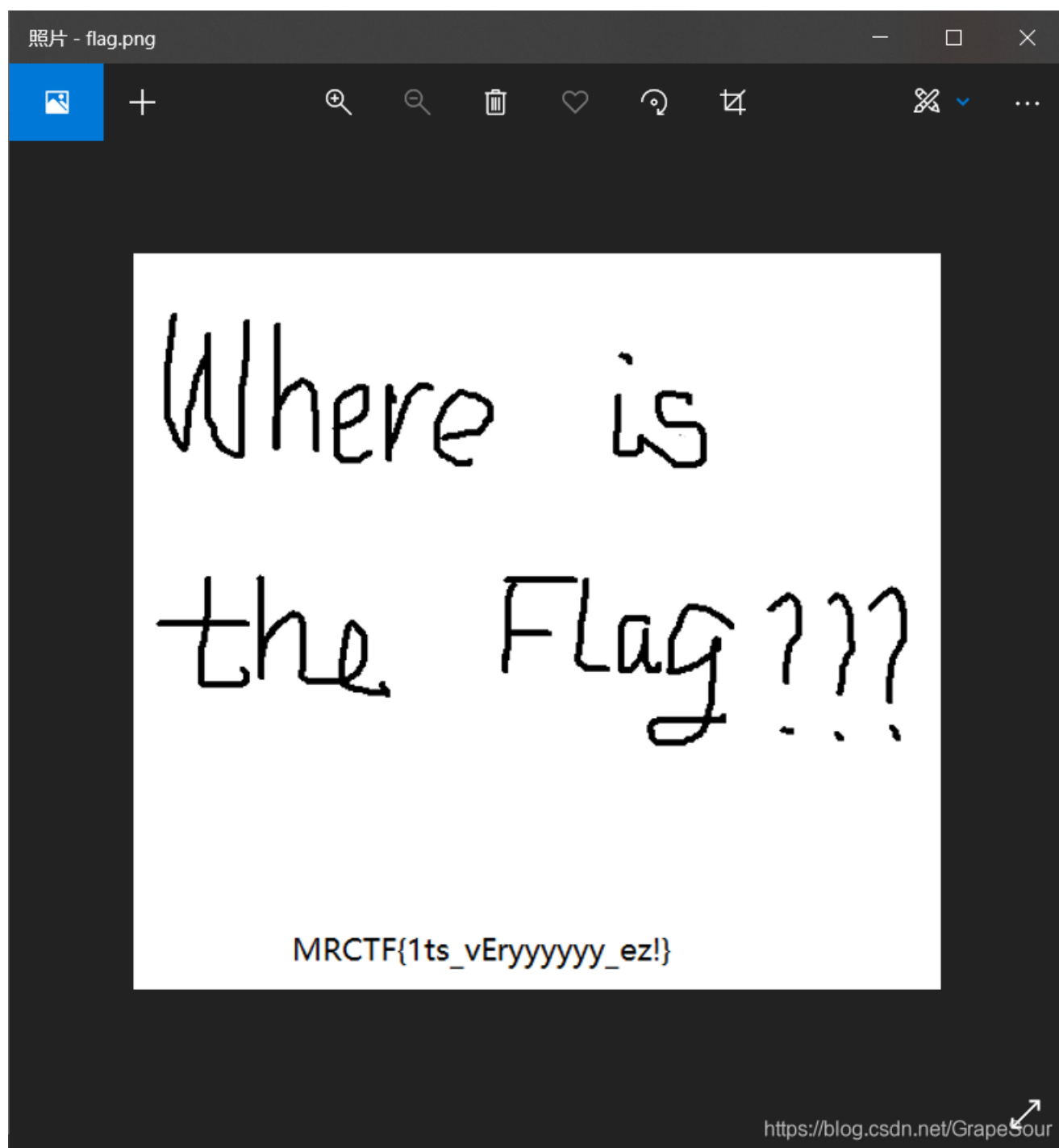
[我吃三明治](#)

[\[GXYCTF2019\]SXMgdGhpcyBiYXNIPw==](#)

[\[SUCTF2018\]single dog](#)

[\[MRCTF2020\]ezmisc](#)

打开图片发现有crc报错，跑一下脚本，爆出正确高度为0x1c8，得到flag



弱口令

先尝试爆破没有成功，复制注释得到

```
┌
|
| . . . . . ←
| . ←
| . → | . ←
| . → . . ←
| → → → → → ←
| . . → . ←
| → → → ←
| . → . ←
| . . → ←
| → → ←
```

<https://blog.csdn.net/GrapeSour>

是摩斯密码，将.看成.，将->看成-，得到

```
.....-...-...-.....-...-...-.....-...-
```

所以密码为

```
HELL0FORUM
```

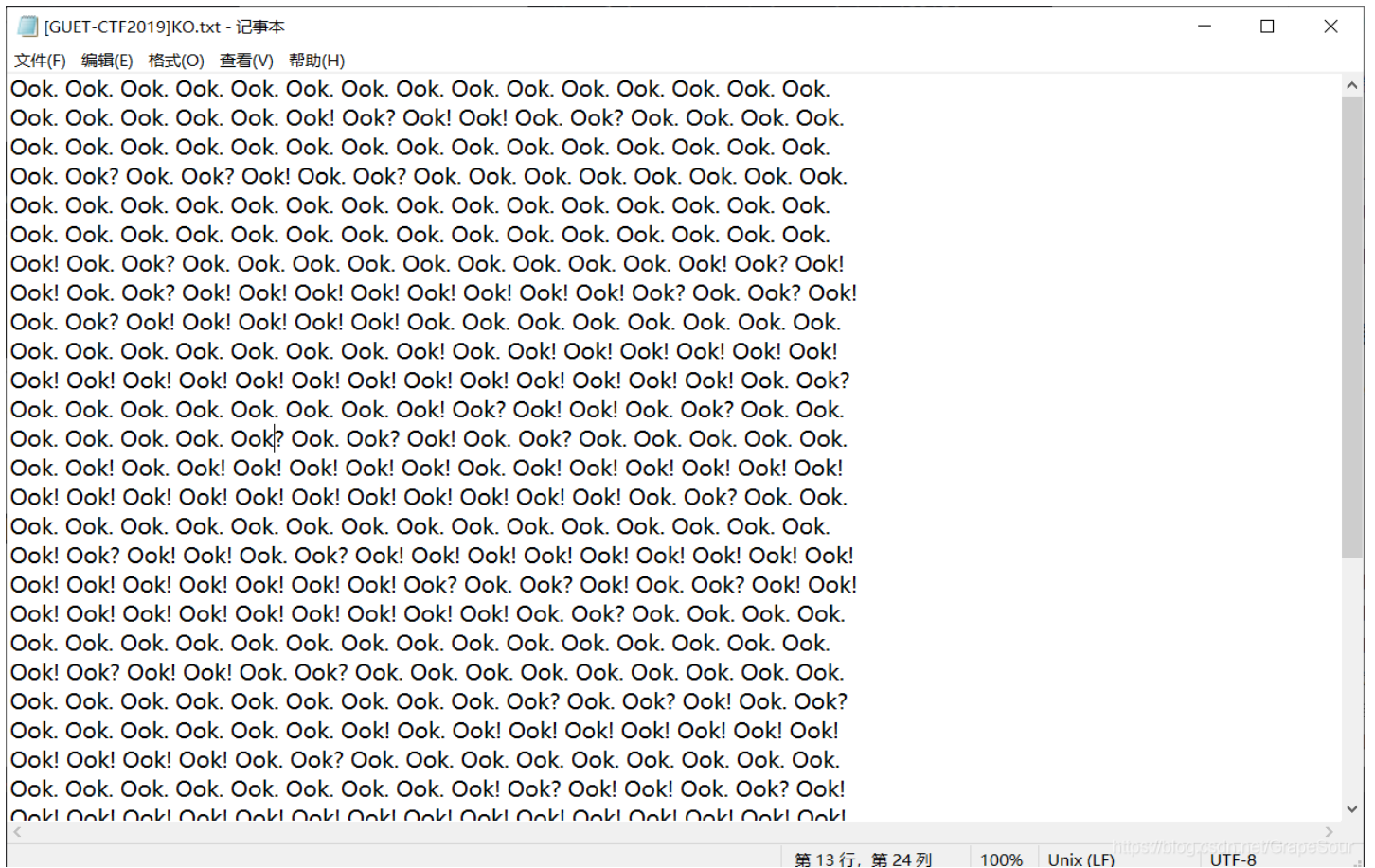
因为说的是弱口令，所以推测是lsb隐写，

```
root@kali)~[~/home/a/桌面/cloacked-pixel-master]
python lsb.py extract 1.png 1.txt 123456
```

```
≡ 1.txt ×
home > a > 桌面 > cloacked-pixel-master > ≡ 1.txt
1 flag{jsy09-wytg5-wius8}
```

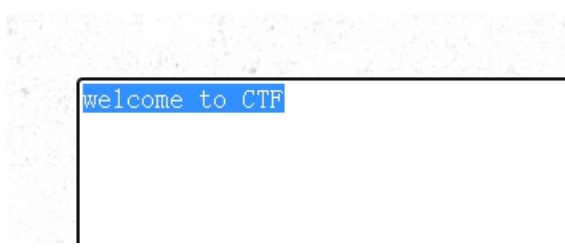
[GUET-CTF2019]KO

得到一个txt文档



Ook!编码

Ook编码



[HBNIS2018]caesar

gmbhjtdbftbs

1

flagiscaesar

<https://blog.csdn.net/GrapeSour>

[HBNIS2018]低个头



看键盘，所以是
但是不是我想象的



所以flag是
flag{CTF}

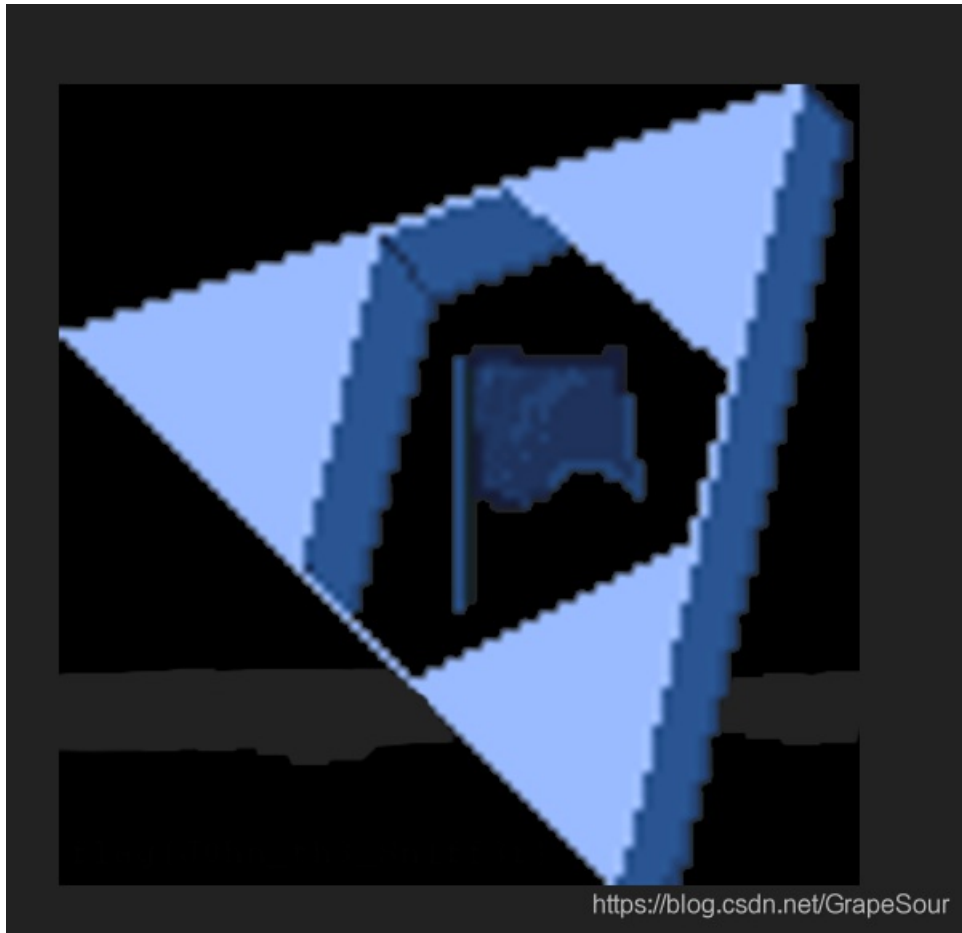
john-in-the-middle

过滤http流，发现一堆图片，导出来

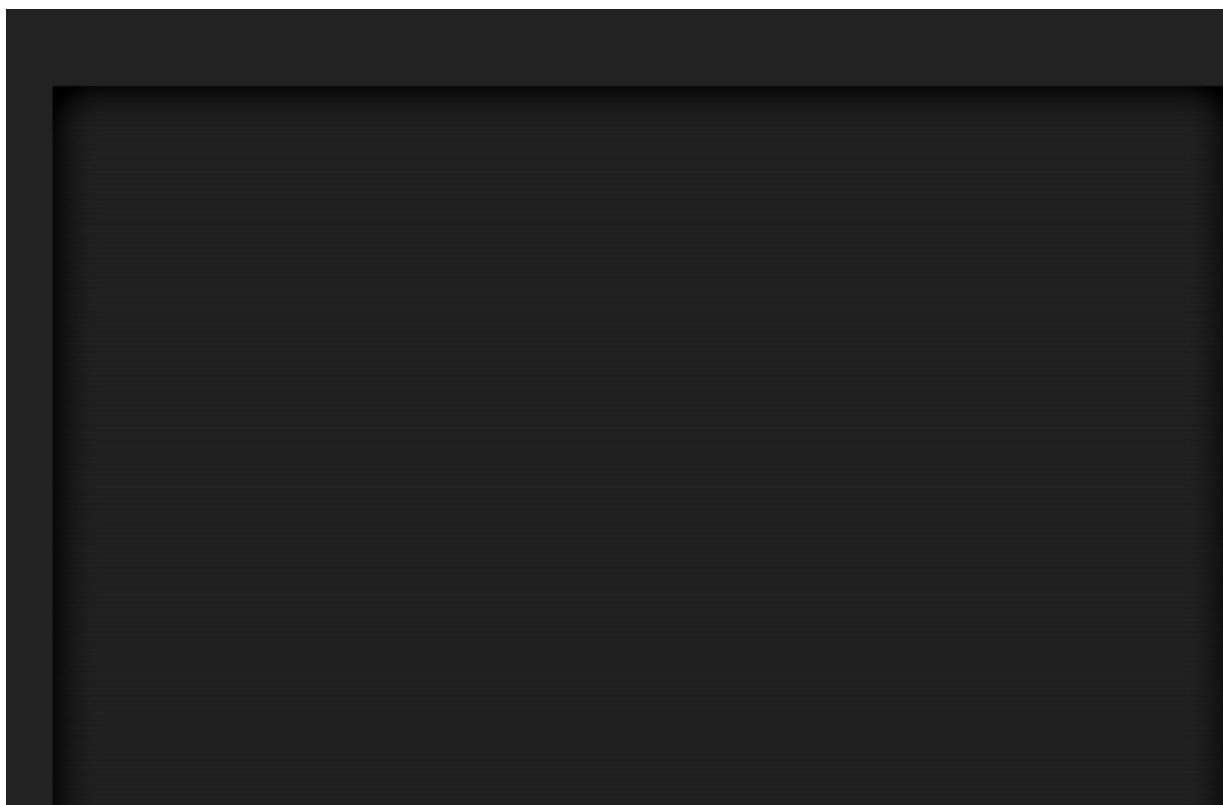
```
GET /js/countdown.js HTTP/1.1
GET /js/jquery.js HTTP/1.1
GET /js/bootstrap.min.js HTTP/1.1
GET /images/logo.png HTTP/1.1
GET /images/sponsor/reply_cv.png HTTP/1.1
GET /images/sponsor/cini.png HTTP/1.1
GET /images/texture.png HTTP/1.1
GET /images/font c3.png HTTP/1.1
```

```
GET /images/scanlines.png HTTP/1.1  
GET /fonts/glyphicons-halflings-regular.woff HTTP/1.1  
GET /fonts/TopazPlus.woff HTTP/1.1  
GET /tunes/between2.mod HTTP/1.1
```

<https://blog.csdn.net/GrapeSour>



<https://blog.csdn.net/GrapeSour>



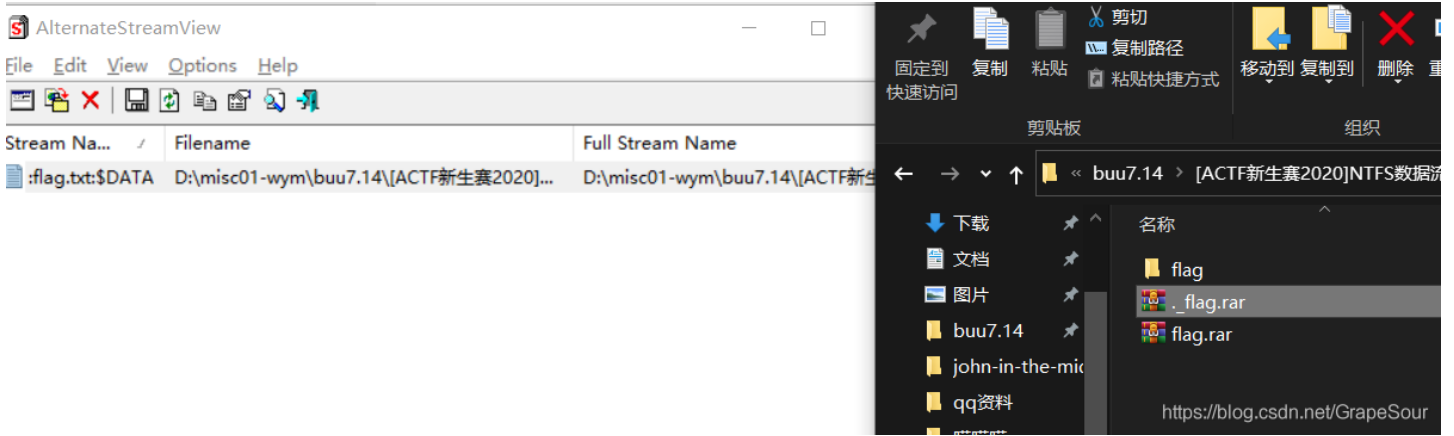
发现两张奇怪的图片
用stegsolve打开

<https://blog.csdn.net/GrapeSour>

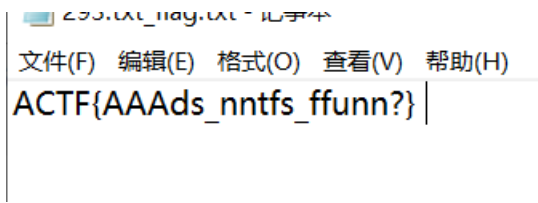
发现奇怪的线条
看logo.png 发现了flag



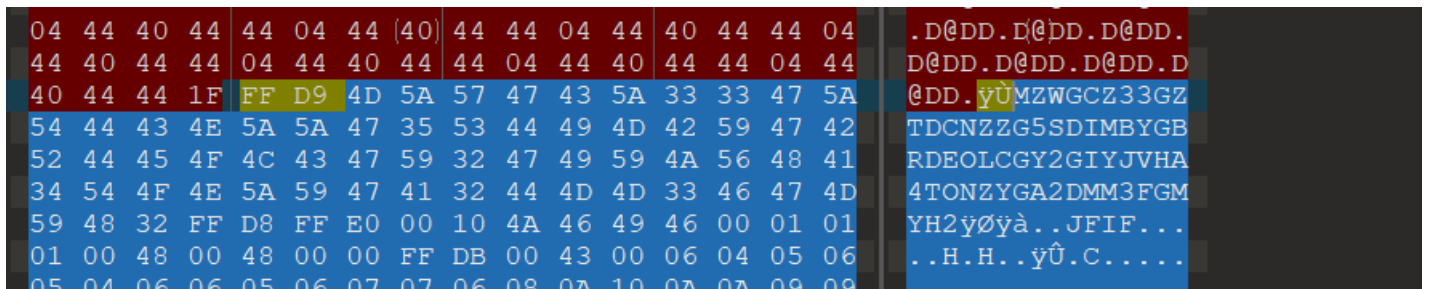
[\[ACTF新生赛2020\]NTFS数据流](#)



解压，用工具，得到



我吃三明治



在两张图片拼接处，发现base32的加密，解密得到flag



[GXCTF2019]SXMgdGhpcyBiYXNIPw==

猜测base64隐写

```

C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python37_64\python.exe
6
GXY{fazhazhenhaot□
9
GXY{fazhazhenhaoti
6
GXY{fazhazhenhaoti□
14
GXY{fazhazhenhaotin
6
GXY{fazhazhenhaotin□
0
GXY{fazhazhenhaotin□
7
GXY{fazhazhenhaoting
7
GXY{fazhazhenhaoting
13
GXY{fazhazhenhaoting}
0
GXY{fazhazhenhaoting}
Press any key to continue . . . █

```

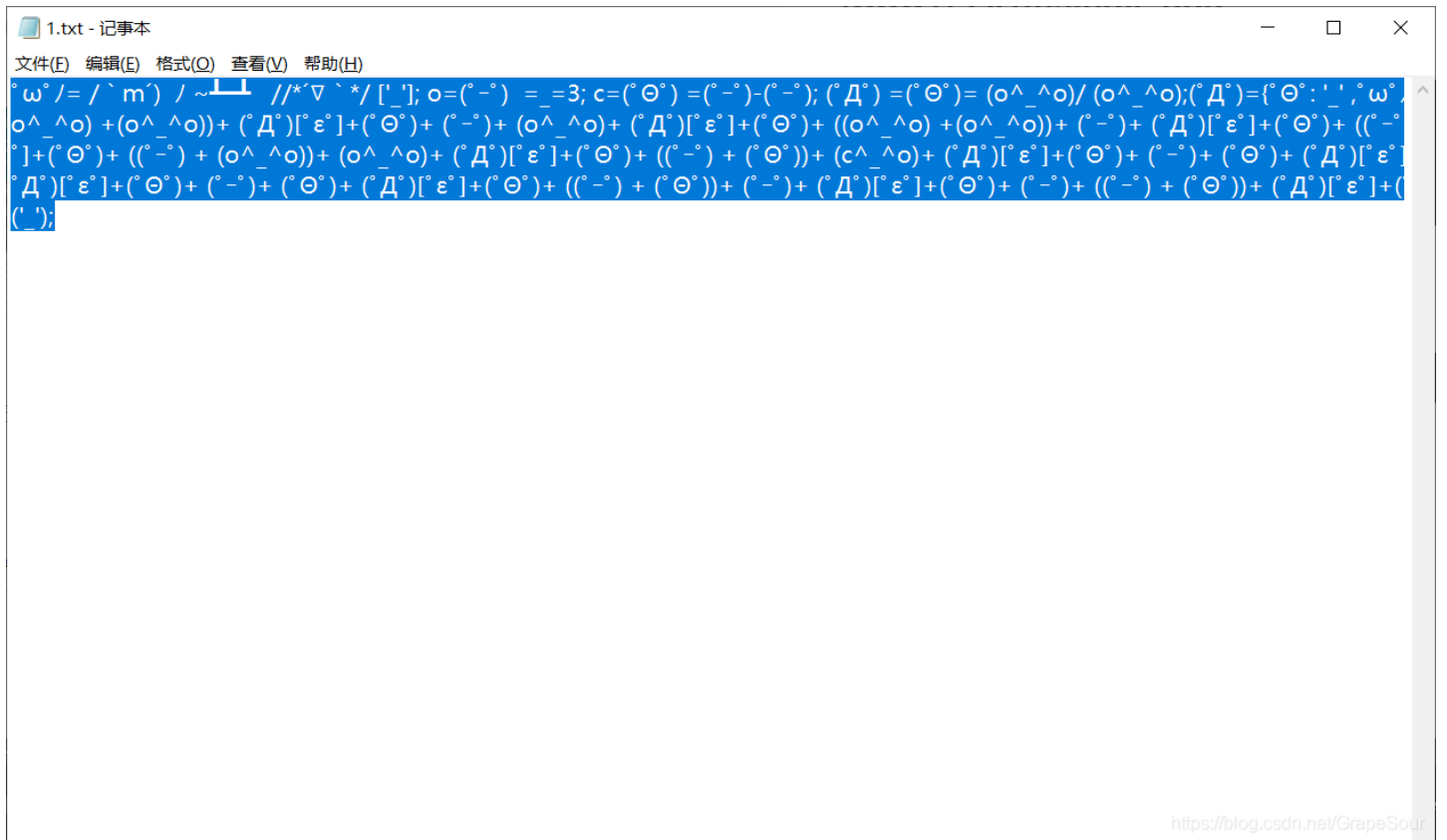
<https://blog.csdn.net/GrapeSouj>

跑解密脚本得到flag

[SUCTF2018]single dog

5	00	32	65	6D	BF	2F	DE	A2	35	n_šUežŔ.2em¿/pç5
5	20	9A	48	(98)	B3	73	CD	58	08	y.gm?qf šH~p sÍX.
8	71	F2	9F	FF	D9	50	4B	03	04	Ūª÷"šŇSqdŔyŪPK..
A	A1	61	4D	81	F7	3B	16	D9	02zjaM.÷;.Ū.
5	00	00	00	31	2E	74	78	74	DD1.txtÝ
C	C2	05	8A	DE	FB	00	22	80	61	YAnŪ0.ŪÂ.špŪ."ea

发现压缩包



1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
ω / = / ` m´ / ~ 1 // * ∇ ` * / [! _]; o = (° - °) = _ = 3; c = (° Θ°) = (° - °) - (° - °); (° D°) = (° Θ°) = (o^_ ^o) / (o^_ ^o); (° D°) = {° Θ° : ! _ , ω }  
o^_ ^o) + (o^_ ^o) + (° D°)[° ε°] + (° Θ°) + (° - °) + (o^_ ^o) + (° D°)[° ε°] + (° Θ°) + ((o^_ ^o) + (o^_ ^o)) + (° - °) + (° D°)[° ε°] + (° Θ°) + ((° -  
°] + (° Θ°) + ((° - °) + (o^_ ^o)) + (o^_ ^o) + (° D°)[° ε°] + (° Θ°) + ((° - °) + (° Θ°)) + (c^_ ^o) + (° D°)[° ε°] + (° Θ°) + (° - °) + (° Θ°) + (° D°)[° ε°]  
° D°)[° ε°] + (° Θ°) + (° - °) + (° Θ°) + (° D°)[° ε°] + (° Θ°) + ((° - °) + (° Θ°)) + (° - °) + (° D°)[° ε°] + (° Θ°) + (° - °) + ((° - °) + (° Θ°)) + (° D°)[° ε°] + (°  
(° - °);
```

<https://blog.csdn.net/GrapeSour>

<http://www.atoolbox.net/Tool.php?id=703>

aaencode 编码