


buuctf misc page 3

原创

~VAS~  已于 2022-04-02 18:28:33 修改  401  收藏

分类专栏: [笔记 ctf buuctf](#) 文章标签: [网络安全](#) [密码学](#) [python](#)

于 2022-04-01 16:43:15 首次发布

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/zip471642048/article/details/123899125>

版权



笔记 同时被 [3](#) 个专栏收录

53 篇文章 0 订阅

订阅专栏



[ctf](#)

50 篇文章 1 订阅

订阅专栏



[buuctf](#)

5 篇文章 0 订阅

订阅专栏

目录

[\[HBNIS2018\]低个头](#)

[\[HBNIS2018\]caesar](#)

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

[我吃三明治](#)

[\[ACTF 新生赛2020\]NTFS数据流](#)

[Mysterious](#)

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

[弱口令](#)

[\[HBNIS2018\]低个头](#)

键盘密码的一种

题目：低个头

描述：EWAZX RTY TGB IJN IO KL 请破解该密文 f

flag格式：XXX 明文

提交：直接提交明文 (大写) |

CSDN @~VAS~

flag{CTF}

[HBNIS2018]caesar

凯撒加密

题目：caesar

描述：gmbhjtdbftbs

flag格式：XXX 明文

提交：直接提交明文 (小写) |

CSDN @~VAS~

Caesar Cipher (凯撒密码)

Encode

Decode

Shift

1

gmbhjtdbftbs

flagiscaesar

CSDN @~VAS~

flag{flagiscaesar}

[SUCTF2018]single dog

010editor打开图片hex，尾部发现pk字符，另存位zip

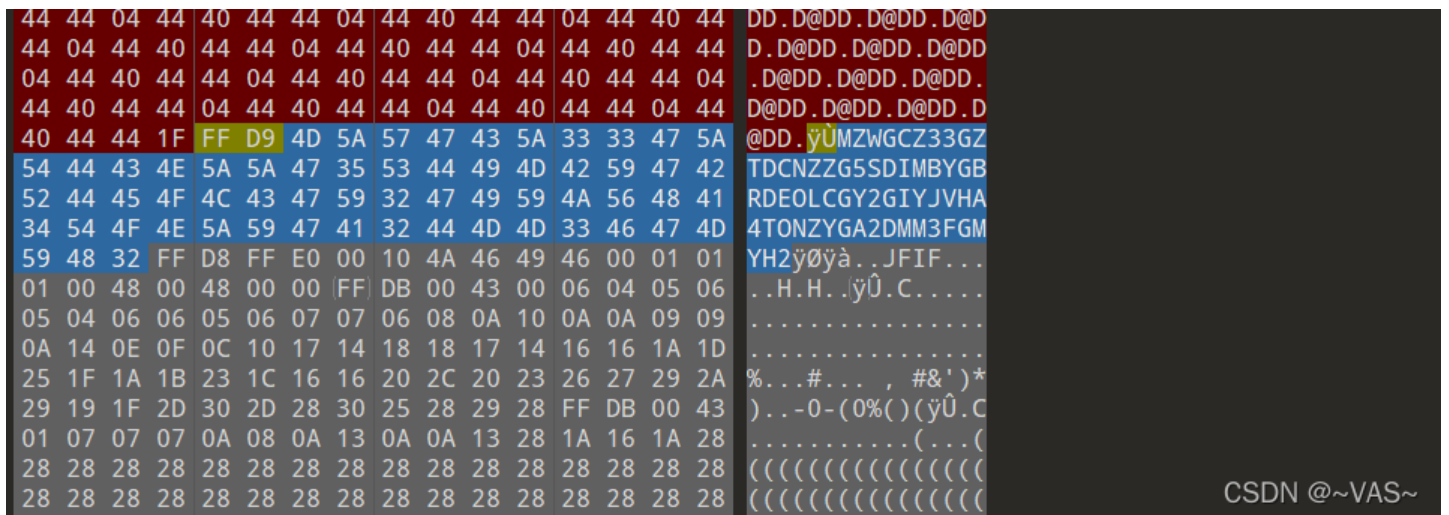
```
C360h: 7F B6 47 85 08 E8 BE F5 6D AE 58 D8 43 77 A9 5C  : |dc: e#om@60CW8\
C370h: DC 4D 89 26 F2 B1 BD 80 CD 6B F8 1D 8F FC 24 11  ÜM%&ð±½€Íkø. .ú$.
C380h: 73 D1 B8 A5 27 CC 5D 3F 74 F7 BB 7D 3F 74 7E 62  sÑ, ¥' Ì ]? t ÷ » }? t ~ b
C390h: FD DA AB 78 AB 13 33 55 AD 3E 57 F2 FE F7 5E B5  ýÛ«x« .3U->wðþ÷^µ
C3A0h: 53 54 FE FE 6E 4A CC E4 19 9C AB FE 90 AC BB 76  SThîo.Ïô.««b.~»v
```

C3B0h:	AB 56 94 72 AA C3 F3 37 CD B7 E5 AC F8 D4 29 DA	«V"rªÄó7Í.ã~ø0)Ú
C3C0h:	38 1B BA 55 F6 40 D1 C6 48 C9 A0 9A 7E EC 6E 67	8.ºUö@NÈHÉ \$~ing
C3D0h:	5C 4A AD FB BD BF 36 EF BD 4D B7 5F 2A 45 DD 4C	\J-0½¿6i½M. *EYL
C3E0h:	85 8B DE B0 63 91 E8 6A CC FC C8 80 F4 A0 C4 BD	...<Pºc'èjIüEëÖ Å½
C3F0h:	6E BB 57 E5 A1 95 59 97 3F 77 FB B4 C8 49 DD 8E	n»Wâi•Y~?wú' ÈIÝŽ
C400h:	D5 3E C1 BD 78 A0 EA 05 F9 69 BF 7B 6E D6 F9 68	Ö>A½x è.üiz{ñ0ùh
C410h:	6E 5F 9A 55 EB 8E D5 00 32 65 6D BF 2F DE A2 35	n_šUëŽÖ.2em¿/pC5
C420h:	FF 00 67 6D 3F 71 66 20 9A 48 98 B3 73 CD 58 08	ÿ.gm?qf šH³sÍX.
C430h:	DB B3 F7 A8 A7 D1 53 71 F2 9F FF D9 50 4B 03 04	Ú³÷"šNšqöŸYÜPK..
C440h:	14 00 00 08 08 00 7A A1 61 4D 81 F7 3B 16 D9 02zjaM.+:.Ü.
C450h:	00 00 0E 20 00 00 05 00 00 00 31 2E 74 78 74 DD1.txtŸ
C460h:	59 41 6E DB 30 10 DC C2 05 8A DE FB 00 22 80 61	YAnÜ0.ÜÄ.Špú."€a
C470h:	2B AC 93 43 6F 16 04 E2 03 7D 81 AB E4 E0 07 B8	+~"Co..ä.}.«äà.
C480h:	F7 22 BD E7 07 BD F9 13 E9 23 FA A9 B2 24 97 94	+~½ç.½ù.é#ú0²\$~"
C490h:	48 8A B2 28 79 69 AB 41 60 C4 12 77 97 B3 33 BB	HŠ²(yi«A'Ä.w~³3»
C4A0h:	24 2D 89 BF 47 F1 67 71 14 2F A2 02 06 F7 F0 20	\$~½¿Gñgq./c..÷ð
C4B0h:	BE 8A 57 F8 28 AF 19 FC 84 72 F9 6E 59 2E 19 30	¾šWö(.ü..rúnY..0
C4C0h:	3D 76 OF B7 F0 A4 1F 6E 1E C4 AD FC CE 60 07 2B	=v..ð..n.Ä-üÏ'..+
C4D0h:	78 92 9F 1A 4A 79 75 80 0A D6 70 14 DF C5 51 14	x'Ÿ.Jyu€.Öp.ßÄQ.
C4E0h:	DA A3 92 A3 15 7C D1 A3 7B 33 FA 6B 81 A3 AE ED	ÚÉ'£.}NÉ{3úk.£@Í
C4F0h:	C6 F9 AE 6C D5 D5 A7 F7 AE 1D 7A 55 7A EC 00 8F	Æù@l00š÷@.zUzi.
C500h:	32 EE A3 FC 5F 68 14 FE 9D D2 F1 AE E0 87 F1 D3	2i£ü.h.Öñ@†ñŸ
C510h:	4A 3B C4 CA E0 33 D8 8C 19 6C B5 FF 1A 5A 0E 14	J;ÄÊà30œ.lmý.Z..
C520h:	5E 35 2F 37 F6 85 CE 13 A3 D4 C6 5B 21 45 EF D6	^5/7ö...î.£0Ê[!EiÖ
C530h:	93 37 33 14 D2 BE 45 C4 4C 76 98 81 8D A0 F0 BD	"73.0¾EÄLv~ . . ð½
C540h:	88 AD 99 5B C5 8B CD BC 33 63 CA EB B9 C3 8C 8B	^~™[Ä<Í¼3cÊé'Äœ<
C550h:	AA 4A CA 62 DF A0 AA 3D 9E 50 C9 BD 56 92 19 96	ªJÊbBª =žPÉ½V' .-
C560h:	DB 51 3F 06 73 B4 E2 1D 0D AD BA B1 F8 87 A4 F8	ÜQ?.s'â..-º±ø†±ø
C570h:	36 27 F4 3F 00 EA 18 C7 CA 7B E6 E0 0E 17 21 9F	6'ô?.é.ÇÉ{æà..!Ÿ
C580h:	18 9D 27 EB 6E FA E7 01 EA D0 32 CE 8A 3B 53 9F	.. 'ènùç.èÐ2Íš;Ÿ
C590h:	CA CC C3 35 6C EB F6 D8 C6 E8 61 AB AB CB 48 CB	ÊiÄ5lëð0Æèa««ÈHÈ
C5A0h:	54 1F E3 A7 91 F7 F1 9B 9A 51 B7 0E 9E 9A 3A F0	T.âš'÷ñ;šQ. žš:ð
C5B0h:	3B 17 BD 94 E2 B5 F7 1D 23 FC 5E D8 4A 48 E7 D2	; .½"âµ÷.#ü^0JHçÖ
C5C0h:	C7 7F D7 F4 5D 1A 1B AC 89 D0 32 32 3C BB DF F9	Ç.×ó). .-šð22<>ßù
C5D0h:	63 74 0D 71 77 EB D7 E7 D5 EF 44 77 9D F4 57 8A	ct.qwë×çÖiDw.ôwš
C5E0h:	9D 61 AF 96 36 2B F8 26 FF 56 81 C5 9D F1 54 7D	.a~6+ø&ÿV.Ä.ñT}
C5F0h:	60 EF 2A 14 36 FA A9 F5 AC D4 2A A2 A5 52 B1 EA	`i*.6úøð-0*ç¥R±è
C600h:	ED BD 53 AB 8F D5 1A 11 DE 68 84 7D 75 B3 8E D4	í½S«.Ö..ph„}u³ŽÖ
C610h:	65 3B 86 B9 F2 20 7F 8C CE 7B 78 E1 4E 46 3C E0	e;†'ò .Æi{xâNF<à
C620h:	15 BB D7 AF 53 1E DC 29 46 44 4E 8D 15 AB 43 8C	.»×Š.Ü)FDN..«CÈ
C630h:	33 6E B6 A1 28 94 B9 F9 AC B9 51 E8 F9 F1 E7 A2	3n¶i(" 'ù~1Qèñçç
C640h:	E1 22 CC 86 86 DF D0 62 7A E5 E4 D6 D2 65 74 3F	á"i††ßBbzâš00et?
C650h:	49 BD 50 95 61 3E 87 B3 4A 45 92 47 5F 9F D1 4D	I½P•a>†³JE'G_ŸNM
C660h:	4F DC 29 EA C5 94 A1 E9 99 73 50 A6 AE 4E B9 56	OÜ)êÄ"jé™sP!@N!V
C670h:	8D E3 35 4A C5 3C 8E A5 79 F4 06 ED 4E 71 6A 8F	ó5JÄ<žÿvö.íNqj

解压后打开发现是aaencode

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

foremost分解出两张图片以为是盲水印，结果在两图的交界处找到base32的字符



CSDN @~VAS~

Base64 Encoding

Pattern: Base32

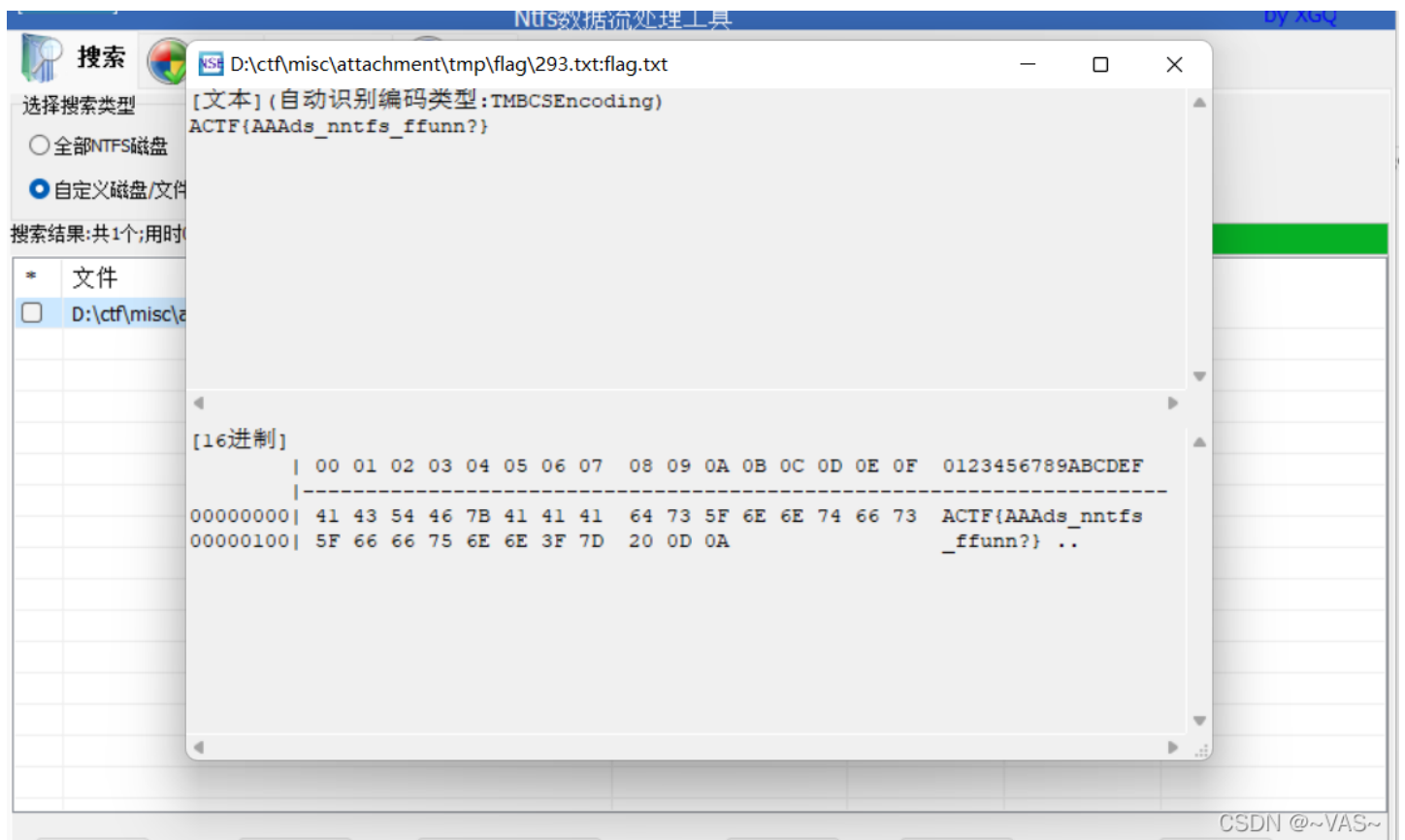
MZWGCZ33GZTDCNZG5SDIMBYGBRDEOLCGY2GIYJVHA
4TONZYGA2DMM3FGMYH2

flag{6f1797d4080b29b64da5897780463e30}

CSDN @~VAS~

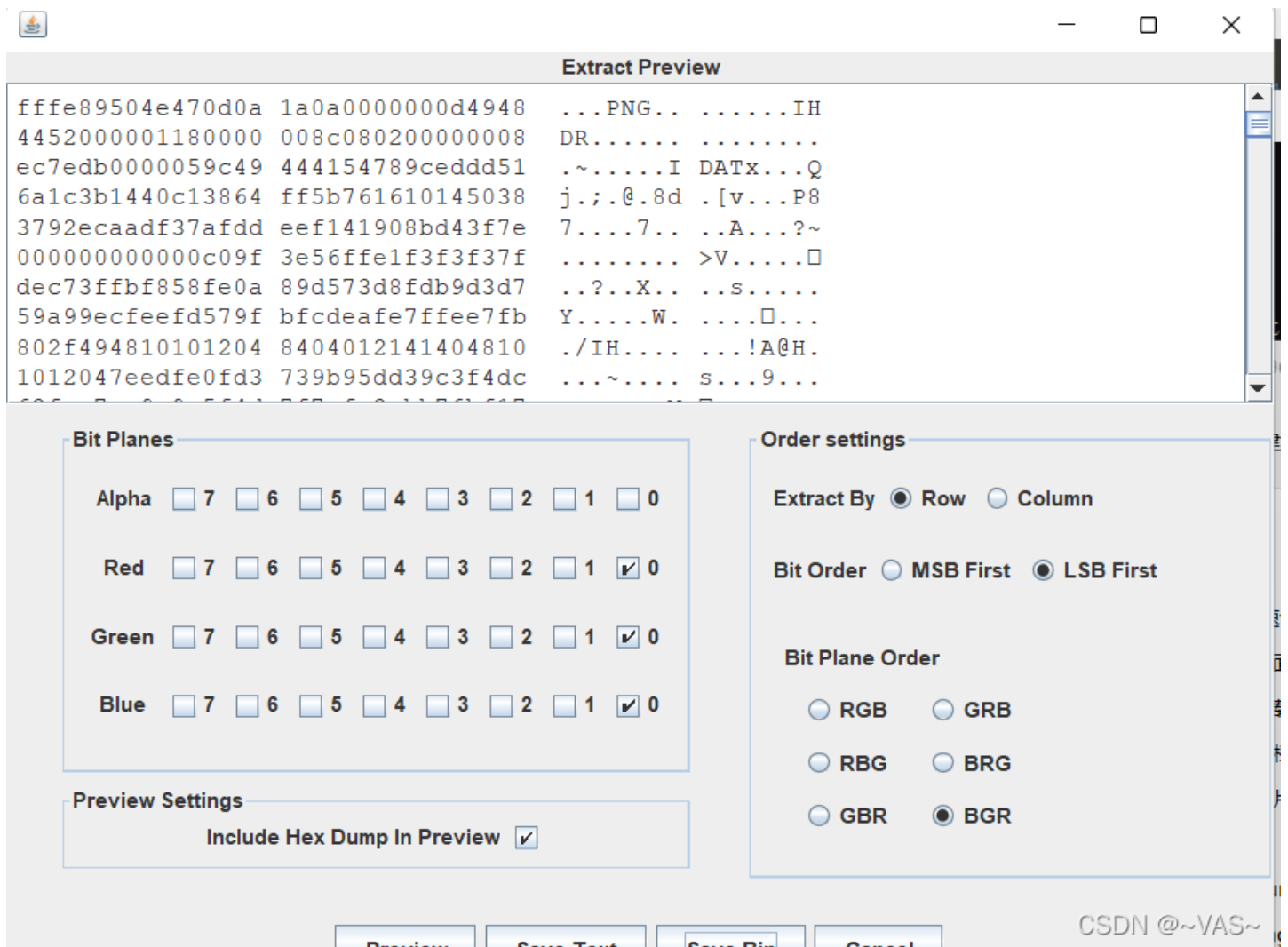
[ACTF新生赛2020]NTFS数据流

跟题目名字一样考ntfs文件流



Mysterious

stegsolve打开图片发现bgr有图片，另存



发现图片只有一半，怀疑是修改了高度



```

import binascii
import struct
import sys

file = input("图片地址: ")
fr = open(file, 'rb').read()
data = bytearray(fr[0x0c:0x1d])
crc32key = eval('0x'+str(binascii.b2a_hex(fr[0x1d:0x21]))[2:-1])
#原来的代码: crc32key = eval(str(fr[29:33]).replace('\x', '').replace("b'", '0x').replace("'", ''))
n = 4095
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
        crc32result = binascii.crc32(data) & 0xffffffff
        if crc32result == crc32key:
            print(width,height)
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png', 'wb')
            fw.write(newpic)
            fw.close
            sys.exit()

```

得到一个百度网盘的链接，里面有一个压缩包，解压后用查看ntfs文件流，并导出pyc文件


```

import base64

def encode():
    flag = '*****'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i ^ ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))

    return ciphertext[::-1]
def decode(ciphertext):
    flag = ''

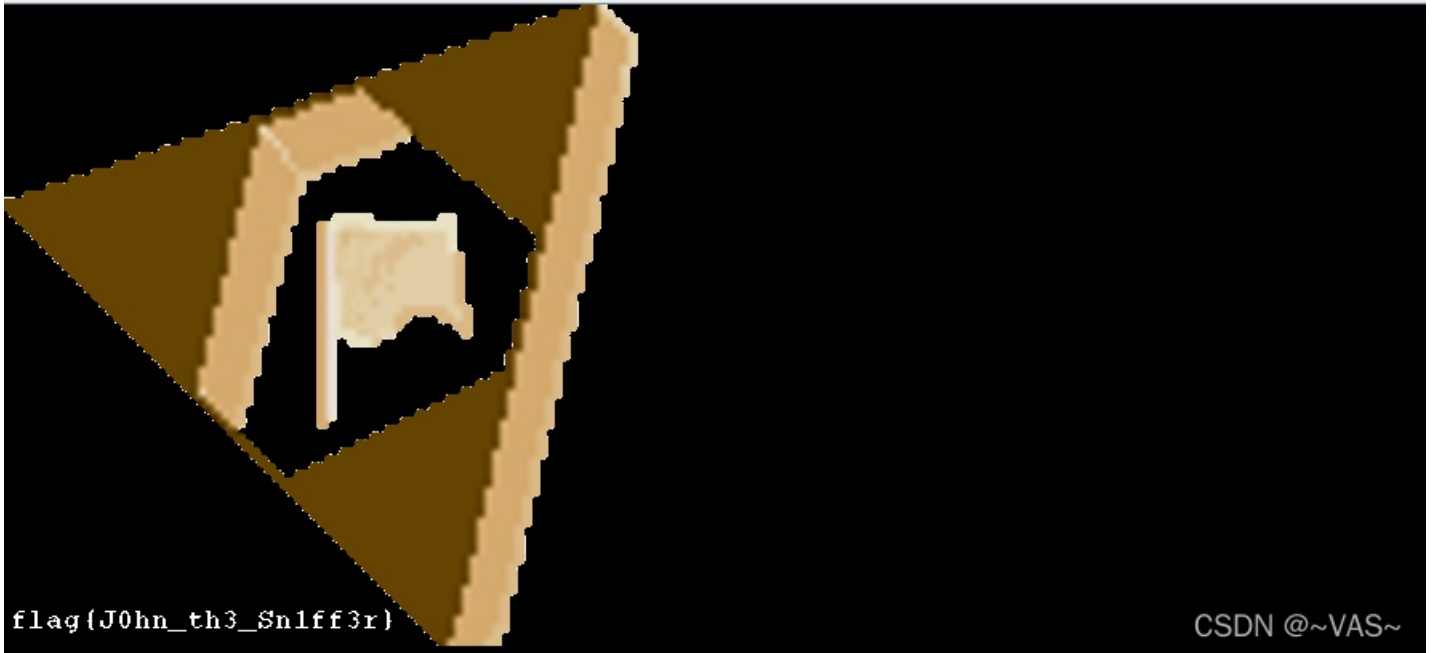
    for i in range(len(ciphertext)):
        #
        if i % 2 == 0:
            s = int(ciphertext[i]) - 10
        else:
            s = int(ciphertext[i]) + 10
        # s = s^i
        # flag+=(chr(s))
        print(chr(s^i),end='')
    print(flag)

ciphertext = [
'96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '132', '46', '112', '64', '97', '88', '80',
'82', '137', '90', '109', '99', '112']
decode(ciphertext[::-1])

```

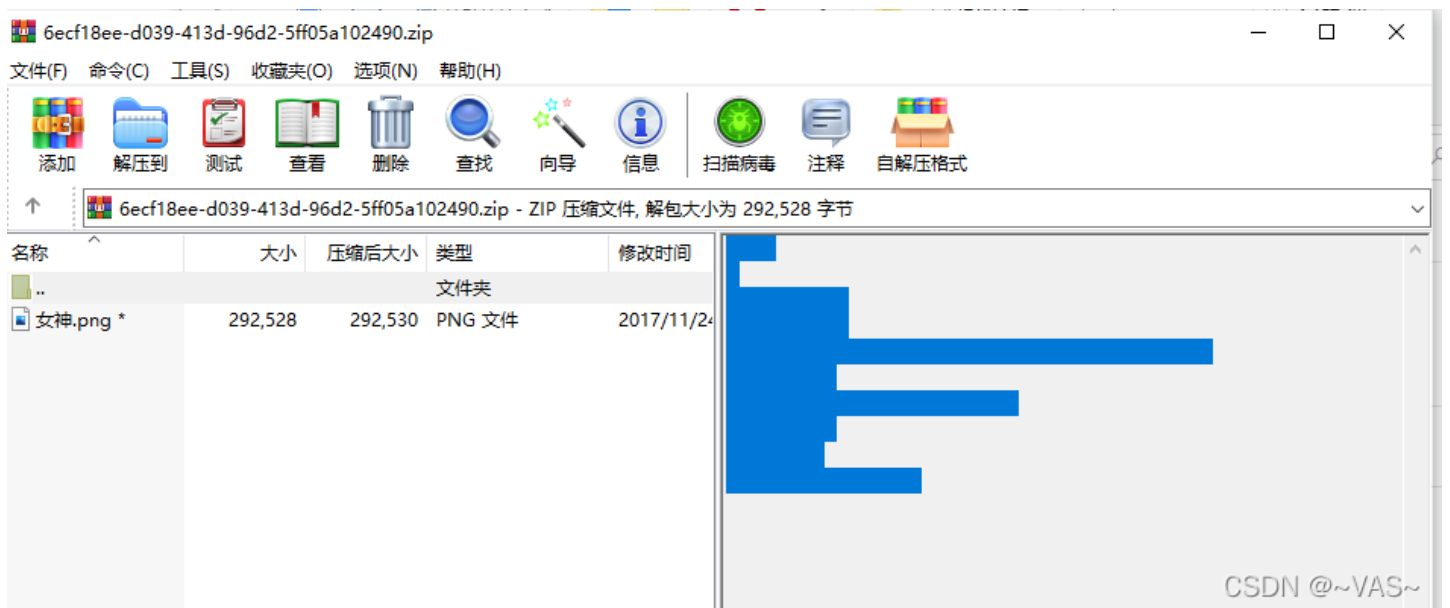
john-in-the-middle

从scanlines.png其他通道可以找到，然后和logo.png 合并就出来了



弱口令

空格和table转成相应的.和-



```
a = ""
```

```
"".split('\n')  
for b in a:  
    for i in b:  
        if ord(i) == 32:  
            print(".",end='')  
        else:  
            print("-",end='')  
    print(end=' ')
```

[随波逐流]CTF编码工具 V1.0 20201022

Base加解密 字符加解密 字符编码转换 已知key解密 进制转换 其他工具 赞赏作者

需要解密的文本 ↓

密钥(key):

字数统计

一键解码

粘贴剪切板

清空内容

解密结果 ↓

复制内容

↑解密结果转至文本框 ↑

HELLOFORUM

CSDN @~VAS~