BUUCTF MISC刷题笔记(一)

原创

<u>z.volcano</u> 于 2021-05-03 16:32:30 发布 ○ 2002 ☆ 收藏 4
 分类专栏: <u># buuoj # 刷题</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/weixin 45696568/article/details/116330991</u>





7 篇文章 1 订阅 订阅专栏



8 篇文章 0 订阅 订阅专栏

BUUOJ

Misc

喵喵喵
弱口令
(安洵杯 2019)easy misc
(文加AN2018排位赛)通行证
蜘蛛侠呀
(RCTF2019)draw
(MRCTF2020)Hello_misc
(MRCTF2020)Unrave!!!
(BSidesSF2019)zippy
(UTCTF2020)basic-forensics

粽子的来历

Misc

喵喵喵

buuoi 同时被 2 个专栏收录



下载的得到一个图片

首先右键查看属性、用winhex打开没发现隐藏的信息,然后用StegSlove打开,在最低位通道发现,很可能是LSB隐写

Blue plane 0	

选项如下时,发现隐写了一个png文件

(S)	- 🗆 ×
Extract Preview	v
fffe89504e470d0a la0a000000d4948 PNG. 4452000001180000 008c08020000008 DR. I ec7edb0000059c49 444154789ceddd51 .~I DATx. 6alc3b1440c13864 ff5b761610145038 j.;.0.8d.[v 3792ecaadf37afdd eef141908bd43f7e 77. .A. 00000000000000000 g.566ffelf3f3f37f	.IH ▲ .Q .P8 .?~ □ 8H.
1012047eedfe0fd3 739b95dd39c3f4dc~ s9	••••
Bit Planes	Order settings
Alpha 7 6 5 4 3 2 1 0	Extract By Row Column
Red 7 6 5 4 3 2 1 2 0	Bit Order 💿 MSB First 🔾 LSB First
Green 7 6 5 4 3 2 1 2 0	Bit Plane Order
Blue ☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 🗹 0	⊖ RGB ⊖ GRB
	○ RBG ○ BRG

Preview Settings Include Hex Dump In Preview 🔽	⊖ GBR
Preview Save Text Sa	ave Bin in psCancel.esch.net/weixin_45696568

导出之后发现文件头多了一些东西, 删去后发现是半个二维码

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Al	IS]
FF	FE	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	ÿþ‰PNG	
ЛЛ	52	00	00	01	1 Q	00	00	00	20	0.0	02	00	00	00	0.0	סח	0

分辨率是280*140,所以改成280*280,png图片的宽高修改还是比较方便的,把右边的数据改成和左边一致

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PN
00000016	00	00	01	18	00	00	00	8C	80	02	00	00	00	80	EC	7E	
00000032	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	Û

发现这个二维码的颜色不对劲,把黑白反色(借助StegSlove)后扫码得到一个网盘地址: https://pan.baidu.com/s/1pLT2J4f,下

🥘 flag.txt - 记事本

文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)

flag不在这里哦 你猜猜flag在哪里呢? 找找看吧

载之后得到flag.rar,里面有一个flag.txt,打开即被调戏 这个题是比赛原题,当时有一个hint是NTFS,buuoj中没有给出

扫描发现flag.txt中隐藏了一个pyc文件,导出,放到pyc在线反编译网站

C:\Users\17422\Desktop\flag.txt:flag.pyc

flag.pyc

755

1

得到一个加密脚本

#!/usr/bin/env python
visit http://tool.lu/pyc/ for more information
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]
```

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']

分析一下写个解密脚本就跑出flag了

弱口令

压缩包是加密的,注释信息处有线索



复制到记事本里,用notepad++打开,猜想是摩斯密码



把 tab 换成 - 空格 换成 .

得到-.. .-.. ---- ..-. .-- .-- ,在线解密得到压缩包密码 HELL0FORUM

压缩包里有一个图片,用Stegsolve打开发现lsb隐写痕迹,Data Extract功能没有结果,结合题目描述和题目名,可以推断是 以弱口令为密码的1sb隐写

D:\lsb隐写>python2 lsb.py extract C:\Users\17422\Desktop\女神.png flag.txt 123456

- [+] Image size: 500x500 pixels.
- [+] Written extracted data to flag.txt.

得到flag

[安洵杯 2019]easy misc

下载附件得到文件夹read、加密的压缩包和一张图片,先看压缩包

添加	1 解压到	测试	查看	删除	查找	向导	(信息	日描病毒	注释	自解	军压格式	
📴 c	lecode.zip -	ZIP 压缩文	件, 解包	大小为 235	字节							
名称	^	:	大小	压缩后大小	类型		修改的	间	CRC32		FLAG IN	((√2524921X85÷5+2)÷15-1794)+NNULLULL,
Ш.					文件夹							
dec 📄	ode.txt *		235	176	文本文档		2019/	/10/4 15:	1B68789	1		

给了解压密码的提示,那个算式算出来结果是7,所以提示:FLAG IN 7+NNULLULL,,开始以为Ⅳ后面的就是密码,结果不是,几 经测试后发现密码是七个数字+ NNULLULL,的形式,于是**掩码爆破**

٦	令已成功恢复!		\times
	Advanced Archive Pas	sword Recovery 统计信息:	
È	总计口令	2,019,451	
È	总计时间	98ms	
Ξ	平均速度(口令/秒)	20,606,642	
ì	这个文件的口令	2019456NNULLULL,	6
E	十六进制口令	32 30 31 39 34 35 36 4e 4e 55 4c 4c 55 4	6
		https://blog.cs V确 定vaixin_45696	

打开得到的 decode.txt 给出了解密的规则:

a = dIW		
b = sSD		
c = adE		
d = jVf		
e = QW8		
f = SA=		
g = jBt		
h = 5RE		
i = tRQ		
j = SPA		
k = 8DS		
I = XiE		
m = S8S		
n = MkF		
o = T9p		
p = PS5		
q = E/S		
r = -sd		
s = SQW		
t = obW		
u = /WS		
v = SD9		
W = CM=		
x = ASD		
y = FTa		
z = AE7		

再结合文件夹给出的大量文本,可以知道考察的是 字频隐写。给出的图片,使用foremost分离出两张看似一模一样的图片,很明显是**盲水印**,解出信息提示 字频隐写在11.txt (我的py2出了点问题不能演示了)。

再加上文件夹中有一个hint.txt

hint:取前16个字符

所以分析11.txt中最高频的前十六个字母,附上脚本

```
f=open("11.txt","r")
d={}
s=""
for line in f.readlines():
    line=line.lower().replace(" ","")
    for i in line:
        if 'a'<=i<='z':
            d[i]=d.get(i,0)+1
d1=sorted(d.items(), key = lambda kv:(kv[1], kv[0]),reverse=True)
for j in range(16):
    print(d1[j][0],end="")
f.close()</pre>
```

得到这十六个字母 etaonrhsidluygw,按照规则替换得到 QW8obWdIWT9pMkFSQWtRQjVfXiE/WSFTajBtcw==, base64解密得 到 Ao(mgHY?i2ARAkQB5_^!?Y!Sj0ms, base85解密得到 flag{have_a_good_day1}

[XMAN2018排位赛]通行证

下载得到一个txt,内容是

a2FuYmJyZ2doamx7emJfX19ffXZ0bGFsbg==

这里用CyberChef,先base64解密一次,然后再栅栏加密一次(key=7)

Recipe		8	Î	Input
From Base64		\otimes	н	a2FuYmJyZ2doamx7emJfX19ffXZ0bGFsbg==
Alphabet A-Za-z0-9+/=			•	
🔽 Remove non-alphabet cha	rs			
Rail Fence Cipher Encode		\otimes	н	
Key 7	Offset Ø			
				Output kzna{blnl_abj_lbh_trg_vg}

最后就是凯撒解码,把前面的xman换成flag即可

AmanCTF - 凯撒(Caesar)加密/解密

在线凯撒(Caesar)加密/解密

kzna{blnl_abj_lbh_trg_vg}	
偏移量加密解密	枚举
<pre>bger{scec_rsa_csy_kix_mx} frbdb_qrz_brx_jhw_lw} qaca_pqy_aqw_igv_kv} ynbo{pzbz_opx_zpv_hfu_ju} xman{oyay_now_you_get_it} wlzm{nxzx_mnv_xnt_fds_hs} vkyl{mwyw_lmu_wms_ecr_gr} ujxk{lvxv_klt_vlr_dbq_fq} tiwj{kuwu_jks_ukq_cap_ep}</pre>	

蜘蛛侠呀

得到一个流量包,用 wireshark 打开,没发现什么

用 tshark 命令看一下

tshark -r out.pcap -T fields -e data > 1.txt

/home/volcano/桌面/1.txt - Mousepad	_ 0 ×
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)	
242453544152542424654e6c6a5867456t523432456t623173305431502t37635866	3654462†7461
242453544152542424494e666148346139614a6f776771334848774159354874724e4	4466594c555a
24245354415254242459567959734975447170382b58546270506664695444786b61	51386864345(
242453544152542424564e5a4c35426a2f30327341514a6868474672466d42574d42	486361584e52
24245354415254242464664673722f485a6669547a5864566a65317451465937794a	6f687a523221
24245354415254242464664673722f485a6669547a5864566a65317451465937794a	6f687a523221
24245354415254242464664673722f485a6669547a5864566a65317451465937794a	5f687a523221
24245354415254242464664673722f485a6669547a5864566a65317451465937794a	5f687a523221
242453544152542424446c51686a7a4b376a534735647749327557586f632f71506c	553053417448
24245354415254242458315464472f736477492f6631554e7a6476554b63737a5578	795333627961
24245354415254242458315464472f736477492f6631554e7a6476554b63737a5578	795333627961
24245354415254242458315464472f736477492f6631554e7a6476554b63737a5578	795333627961
24245354415254242458315464472f736477492f66315546g2a6476554b63737a7a5578	795333627961
242453544152542424727356492b78773776474277517674774b764a6b666e324130	517751435647

写脚本去重,再把每一行的十六进制转字符。

🥘 3.txt - 记事本				—		×
文件(E) 编辑(E) 格式(Q) 查看(⊻) 帮助(H)						
\$\$START\$\$++5srB91Ram3cONSZmjif9aXY9K1UCR	/re0qvhPy9cDDkRZ	Ot6Bvvts	naYwbb0L	.l		^
\$\$START\$\$++AWwJ/ekSjMgOz+vh80Uqs3Fn3WM	9PQqW5vap2ZvFNJ	ZKesQv0)xXD21xT+	rPKs2		
\$\$START\$\$++CJWqZqpQMGbzM+RFG4zUM382IL	DR6tild2Qrb+CxEFlk	(+KhQ7ι	IXMA55qB	7aT4n		
\$\$START\$\$++EWNtcWkEG6Z33hiPs5NcubPyVL9N6	PwnhT/cU818pfCU	SO/Lbrg	LUZkF8yqI	И7В		
\$\$START\$\$++Y1juVt+waLPTv3rrmT+MK/BPhVyXic	M398lm1c4cz7ljJpV	VF2JFEn8	BL4QQ1FK	2		
\$\$START\$\$++ZCkzP8mmw27xs2N+BmskRrHELlxyl	17qqyTdNIRXMuWo	oZC3zym	N+fxU3+y	/0ZhEd		
\$\$START\$\$++hklkPJt0jSmuglhFpY8CH5LACblgS2D	jMPjGwuqpno1iA9A	A3V/cpSl	kg1DnJ1W	н		
\$\$START\$\$++qndQh1j+2zjPzBKkXYv9ArN8aFlgHC	EE65Io7QTnE7lx9G	xKC5wq	LUj0MDpC	29		
\$\$START\$\$++yP30lJPwpBgv0Mb+6GxG8oamr//Kl	IW/O818uDuHfZeW	/6v3v+U	CeyuSpUY	ujbZG		
\$\$START\$\$+/6Vlf57JROpQbl3rSsvbjEPfyHB5NXtbE	VsQrqmHUO/f3V0T	Mfb5wZ	9j3ZYEH26	5		
\$\$START\$\$+/S949Puf59eMXgcL1PsnVsdKC6d2LnD	Oj7f/vxZm/tLkcaXK	ynOah70	QEgNle/kL			
\$\$START\$\$+/laalKCvdmoTaH3UZe1gh5veP4mHON	1YMBwX8zyWvV8ix	3dieOXN	IEDX1y+F>	aNul		
\$\$START\$\$+/pJOs81PbpnbLni/h85W7uYYZFRhdhF	eHhV7My3AVspz6l	YMenXc	TdTjFgJqrY	J		
\$\$START\$\$+/tj8JdxNsXK1buWJ5tdayeej9tq706Km	r/t1vQ7KzBD685xw	/dxrSnDJ	nH0Kbbl			
\$\$START\$\$+02VFWwLtiy5mNcAVdmLsjGgIBiQfgJ0	el/ObU+82Cafiwq+	JUii3GN	Rru3lKk8E			
\$\$START\$\$+0DNzMGfQ7C+3aXfgvi/8S//QZ7/89YE	GU7Qg7uvac2m2A	0hsjTvR5	OY/J7Htb	OK		
\$\$START\$\$+0MnrntRB6sg2kKaME4Kr4jhMJFniCAF	GPC9Do0EuRcmfgC	m64KiCa	aaqnPYLbC)7U		
\$\$START\$\$+0MyIsG7qdDjfsPIDwxP+buqMonIrbkY	/y2BCLXA3olMtrsL/	GDRh2D	1luVbf5pu			
\$\$START\$\$+0RPbKdEI25xODNJpEA3WBIq4DUQ31	1bMsgs162S9BtXd0	QplJo+qi	n6MFlsbeJ	7rf		
\$\$START\$\$+0TbskVicyyP5fef9n368v2pQwPPWO3S	L+egf5bTlAS7kMqY	zQLwf4	/g089LtpH	lb		
\$\$START\$\$+0X9o7RNiP3F2biewPuP6lzg/Hkhf4BBF	b/27kQDd8/GqqW	xTXw/b3	AfnHrQ/ku	ıf		
\$\$START\$\$+0sMjhM6g3u26n49QuhCQDPSAv+OS	V5oulMZ5oECtaPC	Upt4dzZ	PHcTxrlVzj	kw		~
	第5行, 第57列	100% U	nix (LF)	dnineÚtri	8 n_4569	96568

```
import base64
```

```
f = open("3.txt","rb").read()
f1 = open("x","wb")
f1.write(base64.b64decode(f))
```

得到的是一个zip文件,打开得到一个gif,这里是 gif帧数间隔隐写



转为十六进制后再转字符,然后md5加密,最后得到 flag{f0f1003afe4ae8ce4aa8e8487a8ab3b6}

[RCTF2019]draw

给了一些看不太懂的东西,结合题目名,应该是要画出来

cs pu lt 90 fd 500 rt 90 pd fd 100 rt 90 repeat 18[fd 5 rt 10] lt 135 fd 50 lt 135 pu bk 100 pd setcolor pick [red orange yellow green blue violet] repeat 18[fd 5 rt 10] rt 90 fd 60 rt 90 bk 30 rt 90 fd 60 pu lt 90 fd 100 pd rt 90 fd 50 bk 50 setcolor pick [red orange yellow green blue violet] lt 90 fd 50 rt 90 fd 50 pu fd 50 pd fd 25 bk 50 fd 25 rt 90 fd 50 pu setcolor pick [red orange yellow green blue violet] dt 90 fd 50 pu fd 50 bk 50 rt 90 fd 50 bk 100 fd 50 rt 45 pu fd 50 lt 90 pd fd 50 bk 50 rt 90 setcolor pick [red orange yellow green blue violet] fd 100 pd rt 90 fd 50 pu lt 90 fd 100 pd fd 50 rt 90 fd 50 bk 25 rt 90 fd 25 setcolor pick [red orange yellow green blue violet] pu fd 25 lt 90 bk 30 pd rt 90 fd 25 pu fd 25 lt 90 pd fd 50 bk 25 rt 90 fd 25 lt 90 fd 25 bk 50 pu bk 100 lt 90 setcolor pick [red orange yellow green blue violet] pu fd 25 lt 90 pd rd 90 rd 25 pu fd 25 lt 90 pd fd 50 pd rc 360 15 pu fd 15 setcolor pick [red orange yellow green blue violet] fd 100 pd rt 90 arc 360 20 pu rt 90 fd 50 pd arc 360 15 pu fd 15 setcolor pick [red orange yellow green blue violet] lt 90 pd bk 50 lt 90 fd 25 pu home bk 100 lt 90 fd 100 pd arc 360 20 pu home

后面百度了一波,得知这个是 logo语言,可以参考这个贴子

直接到这个在线网站运行即可

Logo解释器 测试 源码 协作 中文 V	参考 - Logo语音 仓库 - 你的过程 历史 - 你的代码执行记录 元时 - 你可以尝试一下的有趣代码 更多 - 有用的小工具 链接 - 其他Logo资源
	TO <u>star</u> repeat 5 [fd 100 rt 144] END clearscreen star TO <u>square :length</u> repeat 4 [fd :length rt 90] END TO <u>randomcolor</u> setcolor pick [red orange yellow green blue viol END clearscreen repeat 36 [randomcolor square random 200 rt 10]
$ \begin{array}{c} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	<pre>clearscreen window hideturtle repeat 144 [setlabelheight repcount penup fd repcount * repcount / 30 label 'Logo bk repcount * repcount / 30 pendown rt 10 wait 5] showturtle</pre>
	To <u>tree :size</u> if :size < 5 [forward :size back :size stop] forward :size/3 left 30 tree :size#2/3 right 30 forward :size/6 right 25 tree :size/2 left 25 forward :size/6 back :size END clearscreen tree 150
<i>请在此输入代码</i> / ↓// →// →// →// →// →// →// →// →// →	T0 fern :size :sign if :size < 1 [stop] fd :size fd :size

所以 flag{RCTF_HeyLogo}

[MRCTF2020]Hello_misc

用Stegsolve打开图片,在 <u>红色通道</u> 隐写了东西

	– 🗆 X											
Extract Preview												
89504e470d0ala0a 000000d49484452 .PNGIHDF	٤ 🗖											
0000020e0000012a 080200000f20c4f*) –											
d30000001735247 4200aecelce90000sRG B												
000467414d410000 b18f0bfc61050000gAMAa												
0009704859730000 0ec300000ec301c7pHYs												
6fa86400001cfa49 444154785eedddcd o.dI DATx^												
adec36b2c0f11bc8 2c278a13825713c56,'W												
096016cec0fbbblc c0093882bb312692 .`81&.												
8b990cdec2f0c218 c0809f2456f1b3a8\$V												
a2d4ad8f3ee7ff43 2fe65054b148b159>C /.PT.H.Y	· · · · · · · · · · · · · · · · · · ·											
Bit Planes	Order settings											
Alpha 7 6 5 4 3 2 1 0	Extract By 💿 Row 🔾 Column											
Red 7 6 5 4 3 2 1 1 0	Bit Order 💿 MSB First 🔾 LSB First											
Green 7 6 5 4 3 2 1 0	Bit Plane Order											
Blue 7 6 5 4 3 2 1 0	● RGB ○ GRB											
	○ RBG ○ BRG											
Preview Settings												
Include Hex Dump In Preview 🔽												
Preview Save Text Save Bin h osCancel oscin.nei/weixin_45696568												

save bin保存为png图片,给了zip压缩包的密码 !@#\$%67*()-+,题目给的是rar,所以还需要找出这个zip

Maybe you should try to separate the files!

And I will give u zip-passwd: !@#\$%67*()-+

直接foremost,提取出zip,用密码解密,得到的out.txt中由几种数字组成

🥘 out.	txt - 记事	本			—		×
文件(<u>F</u>)	编辑(<u>E</u>)	格式(<u>O</u>)	查看(<u>∨</u>)	帮助(<u>H</u>)			
127							^
255							
63							
191							
127							
191							
63							
127							
127							
255							
63							
191							
63							
191							
255							
127							
127							
255							
63							
63							
127							
191			. hite and		a a state and a	1. 1500/	×
第1行,	第1列	100%	Unix (Lf	y iogiesan.	UTF-	B N_40098	000

把这些数字分别转为八位的二进制,发现后面六位都是1,只有前两位有区别,写脚本把所有组的前两位连起来,再转字符。

```
f = open("out.txt","r")
flag=y=x=""
for line in f.readlines():
    x = bin(int(line))[2:].zfill(8)
    y += x[:2]
f.close()
for i in range(len(y)//8):
    flag += chr(int(y[i*8:(i+1)*8],2))
print(flag)
```

最下面有一些透明字,把颜色改深就可以看到

(
4
4
4
4
د ا
MTEwMTEwMTExMTExMTEwMDExMTExMTExMTExMTExMTExMTExMTExMTExMTExMT
xMTEwMDAwMDAxMTExMTExMDAxMTAx↔
MTEwMTEwMDAxMTAxMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTExMTEx
xMTAxMTExMTExMTExMTEwMTEwMDEx↔
MTEwMDAwMTAxMTEwMTExMDExMTEwMTExMTExMTAwMDExMTExMTExMDAxMDAxMDAxM
TAxMTEwMDAwMDExMTExMDAwMDExMTExMTEx↔
MTEwMTEwMTAwMDAxMTExMDExMTEwMTExMTExMDExMTAxMTExMTEwMTEwMTEwM
TAxMTExMTExMTExMTExMTExMTExMTEx←
MTEwMTEwMTAxMTExMTExMDExMTEwMTExMTAxMDExMTAxMTExMTExMTEwMTEwMTEwMT
AxMTAxMTExMTEwMTExMTExMTExMTEx<
MTEwMTEwMTAwMDAxMTAwMDAwMTEwMDAwMDAxMTAwMDExMTAwMDAwMTEwMTEwM
TEwMTAxMTEwMDAwMDAxMTExMDAwMDExMTExMTEx←

https://blog.csdn.net/weixin_45696568

得到的这些像是base64编码,分别解码得到一串二进制

Recipe		Î	Input	length: 60 lines:)6 7	+ (∋	Î	
From Base64	\otimes	П	MTEWMTEXMTEXMTEXMTEXMTEXMTEXMTEXMTEXMTEXMTEX	ExMTEXMTEXMTAX	MTEWMD	\wMDAx!	MTEX	MTEXM	ITEXM	DAxMT
Alphabet A-Za-z0-9+/=		•	MTEWMTEWMTEWMDAxMTAXMDEXMTEWMTEXMTEXMTEXMTEXMTEXMTEXMTEXMTEX EX	ExMTEXMTEXMTEX	MTAXMTI	EXMTEX	4TEX	MTEXN	1TEwM	TEWMD
			MTEWMDAWMTAXMTEWMTEXMDEXMTEWMTEXMTEXMTAWMDEXMTEXMTEX Ex	EXMDAXMDAXMTAX	MTEWMD	AWMDEX	ITEX	MDAwn	1DExM	TEXMT
Remove non-alphabet chars			MTEWMTEWMTAWMDAXMTEXMDEXMTEXMTEXMTEXMTEXMTEXMTEXMTEXMTEXMTEXMT	EWMTEWMTEWMTAX	MTEXMT	EXMTAW	4TEwi	MTEXN	ITEXM	TEXMT
			MTEWMTEWMTAXMTEXMTEXMDEXMTEXMTEXMTAXMDEXMTAXMTEXMTEXMT EX	EWMTEWMTEWMTAX	MTAxMTI	EXMTAW	4TEW	MTEXN	ITEXM	TEXMT
			MTEWMTEWMTAWMDAXMTAWMDAWMTEWMDAWMDAXMTAWMDEXMTAWMDAWMT Ex	EWMTEWMTEWMTAX	MTEwMD/	\wMDAx!	ЧΤЕХ	MDAwn	1DExM	TEXMT
			Output 🥻	time: length: lines:	1ms 450 1			(†)		::
			11011011111110011110111111111111111111	000000111111111 000001011101110	100110: 111101:	111011(111111)	9110 0001	00110 11111) 1011 11111	11011 10010
			01101110000011111000001111111111011010000	.11011101111111	110110: 011111:	10101: 111111	1111 1110	11100 11010) 1101)0001	11111 10000
			0110000001100011100000110110101010100000	1111						

这里不能这样看,把结果平均分为六行,再把1替换成空格就能看到flag

[MRCTF2020]Unravel!!

拿到三个文件

📕 u			又件类		
🔯 win-win.zip	4,957,332	4,957,332	WinRAR ZIP 压缩	2020/3/12 21:	7424C34C
JM.png	407,605	398,554	PNG 文件	2020/3/12 21:	361DEAAE
Look_at_the_file_ending.wav	6,078,590	3,713,450	WAV 文件	2020/3/15 16:	99277858

先看一下wav, 文件名提示让看一下文件的尾部, 所以用010打开看一下

5C:C020h:	В7	FC	Е9	FC	9B	FC	F.2	FC	8D	FC	FD	FC	/4	FC	ΕT	FC	•ueu>uou.uyutunu
5C:C030h:	4E	\mathbf{FC}	E2	FC	2B	\mathbf{FC}	E2	FC	10	FC	D6	FC	03	\mathbf{FC}	в0	FC	Nüâü+üâü.üÖü.ü°ü
5C:C040h:	0C	\mathbf{FC}	84	\mathbf{FC}	25	\mathbf{FC}	54	\mathbf{FC}	3C	\mathbf{FC}	24	FC	44	\mathbf{FC}	6B	65	.ü"ü%üTü<ü\$üDü <mark>ke</mark>
5C:C050h:	79	3D	55	32	46	73	64	47	56	6B	58	31	2F	6E	53	51	y=U2FsdGVkX1/nSQ
5C:C060h:	4E	2В	68	6F	48	4C	38	$4 \mathrm{F}$	77	56	39	69	4A	42	2F	6D	N+hoHL8OwV9iJB/m
5C:C070h:	53	64	4B	6В	35	64	6D	75	73	75	6C	7A	34	3D			SdKk5dmusulz4=

U2F开头,很明显是AES了,需要秘钥,在这个文件里找了一下没找见

再去看一下那个图片,直接binwalk一把梭,拿到一个图片,内容就是前面需要的秘钥: Tokyo 解得key= CCGandGulu

Home	AES 🗵				
AES				Encode	Decode
^{Key} Tokyo		Output Base64 💌			
U2FsdGVkX1	/nSQN+hoHL8	80wV9iJB/mSdKk5dmusulz4=	CCGandGulu		

拿得到的key去解压压缩包,得到一个wav文件,这里是比较坑的,没找到提示,尝试了一遍发现要用 SilentEye

🧟 Decode messa	age: C:/Users/	//Desktop/Ending	g.wav	?	\times
	Options	Media's	encoding format	t: WAVE	• 0
	Sound quality: 9	93.75% normal	T	Adva	nced
Deco	ded message				
	MRCTF{Th1s_is_t	the_3nd1n9}			
CharSet: UTF8 💌	🛛 🖉 🔲 Encrypte	ed data 🔽 Compre	ssed dat 🧕 🥹 Canc	el 🖉 De	ecode

[BSidesSF2019]zippy

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · attachment.pcapng – 🛛 🛛 🗙

```
nc -l -p 4445 > flag.zip
unzip -P supercomplexpassword flag.zip
Archive: flag.zip
inflating: flag.txt
```

直接binwalk分离出压缩包,密码是: supercomplexpassword,解压拿到flag

[UTCTF2020]basic-forensics

下载的jpg打不开,拖进winhex里看一下,发现里面都是明文

所以用notepad打开,ctrl+f搜索一下flag、key等关键字

然后找到了 utflag{fil3_ext3nsi0ns_4r3nt_r34l}

粽子的来历

曹操的私生子曹小明因为爸爸活着的时候得罪太多人,怕死后被抄家,所以把财富保存在一个谁也不知道的地方。曹小明比较喜欢屈原,于 是把地点藏在他的诗中。三千年后,小明破译了这个密码,然而却因为担心世界因此掀起战争又亲手封印了这个财富并仿造当年曹小明设下 四个可疑文件,找到小明喜欢的DBAPP标记,重现战国辉煌。(答案为正确值(不包括数字之间的空格)的小写32位md5值)注意:得到的 flag 请包上 flag{} 提交

鬼脑洞题...

		± ±		± ±	± ±	± ±				± ±			- -		- -		
)0128	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
)0144	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
)0160	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	<u> </u>
)0176	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
)0192	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
)0208	FF	49	43	6F	6D	65	46	72	6F	6D	41	6C	69	62	61	62	y <mark>IComeFromAlibab</mark>
)0224	61	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	a <mark>ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ</mark>
)0240	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
)0256	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
)0272	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ
20000																	

新建一个doc文档,对比一下

00000112	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
00000128	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
00000144	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	<u> </u>
00000160	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	<u> </u>
00000176	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000192	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000208	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000224	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000240	FF	FF	\mathbf{FF}	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	\mathbf{FF}	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000256	FF	FF	\mathbf{FF}	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	FF	\mathbf{FF}	FF	<u> </u>
00000272	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
00000288	FF	FF	\mathbf{FF}	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	FF	\mathbf{FF}	FF	<u> </u>
00000304	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000320	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u> Ÿ
00000336	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
00000352	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000368	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
00000384	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000400	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ</u>
00000416	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	<u> </u>
00000432	FF	FF	\mathbf{FF}	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	000000000000000000000000000000000000000

所以把红框位置对应的十六进制全部改成F,就能正常打开了

帝高阳之苗裔兮,朕皇考曰伯庸。↩ 摄提贞于孟陬兮,惟庚寅吾以降。↩ 皇览揆余初度兮,肇锡余以嘉名: ↩ 名余曰正则兮,字余曰灵均。↩ 纷吾既有此内美兮,又重之以修能。↩ 扈江离与辟芷兮,纫秋兰以为佩。↔ 汨余若将不及兮,恐年岁之不吾与。↩ 朝搴阰之木兰兮,夕揽洲之宿莽。↩ 日月忽其不淹兮,春与秋其代序。↩ 唯草木之零落兮,恐美人之迟暮。↩ 不抚壮而弃秽兮,何不改乎此度?↩ 乘骐骥以驰骋兮,来吾道夫先路! ↔

Ł

但是仔细对比会发现 行距不一样

帝高阳之苗裔兮, 朕皇才 摄提贞于孟陬兮, 惟庚 皇览揆余初度兮, 肇锡; 名余曰正则兮,字余曰, 纷吾既有此内美兮,又 扈江离与辟芷兮, 纫秋; 汨余若将不及兮,恐年; 朝搴阰之木兰兮,夕揽; 日月忽其不淹兮,春与利 唯草木之零落兮,恐美, 不抚壮而弃秽兮,何不, 乘骐骥以驰骋兮, 来吾礼 \leftarrow

帝高阳之苗裔兮,朕皇考曰伯庸。↩ 摄提贞于孟陬兮,惟庚寅吾以降。↔ 皇览揆余初度兮,肇锡余以嘉名: ↔ 名余曰正则兮,字余曰灵均。↩ 纷吾既有此内美兮,又重之以修能。↩ 扈江离与辟芷兮,纫秋兰以为佩。↔ 汨余若将不及兮,恐年岁之不吾与。↩ 朝搴阰之木兰兮,夕揽洲之宿莽。↩ 日月忽其不淹兮,春与秋其代序。↩ 唯草木之零落兮,恐美人之迟暮。↩ 不抚壮而弃秽兮,何不改乎此度?↩ 乘骐骥以驰骋兮,来吾道夫先路! ↔

把每一行右键→段落,查看行距,把1.5倍行距换成1、单倍行距换成0

ABCD对应的分别是

A 100111100010 B 100100100001 C 100100100001 D 010100100001

按个测试,最后正确的是C对应的二进制值转md5 flag{d473ee3def34bd022f8e5233036b3345}