CTF红明谷杯2021 MISC WP

原创

Sapphire037 于 2021-04-04 22:12:12 发布 426 收藏 2

红明谷杯赛后复现

没报名呜呜呜

1.InputMonitor

下载文件，发现东西很多，怎么办呢，一个一个找吧，在Desktop中发现有flag.7z和log_data.txt还有个exe文件，先看flag.7z，有密码，再看txt文件，

很明显的提示说在监控输入，那么就要找到他输入的内容，尝试爆破7z无果，到这里就卡住了，

听师傅们说取证大师可以一把梭，赛后看了师傅们的wp，取证大师直接把压缩包密码梭出来了，密码是 有志者事竟成.打开压缩包得到hidden.pdf，可以把图片删掉得到flag，也可以直接选中复制得到flag，最终flag为□□□□{□0□_□1□□_ 1□□3□_□3□}.

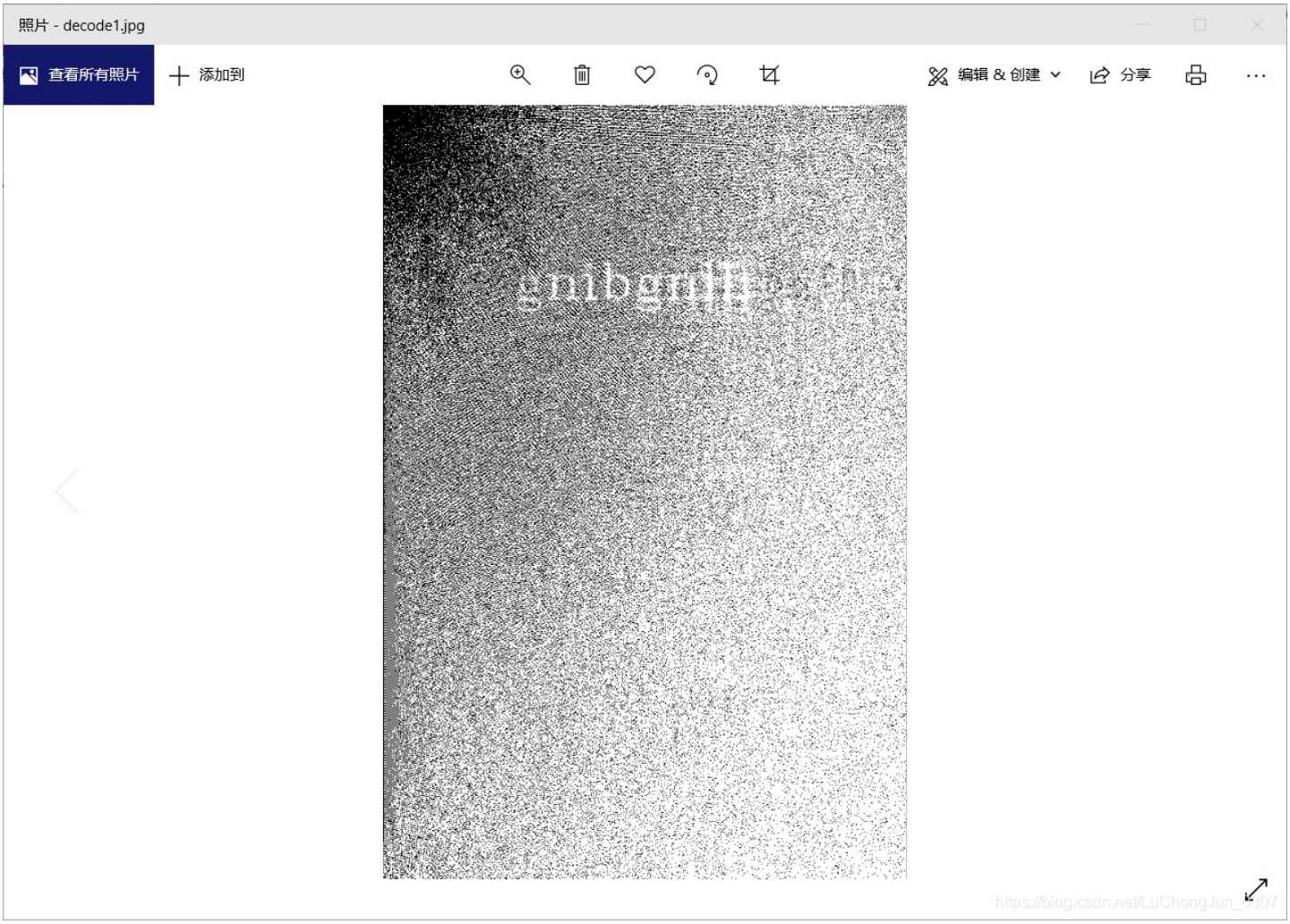
2.我的心是冰冰的

拿到题目，一个图片一个压缩包，压缩包是加密过的，那么正常思路就是从图片里拿到压缩包的密码，尝试了各种各样的隐写方式，都没解出来，赛后才知道这是java盲水印，只能一个一个试...，

```
java -jar BlindWaterMark.jar decode -c bingbing.jpg 1.jpg
```

地址:java盲水印

得到



后面几个看不清楚盲猜一下,gnibgnib，得到密码，打开压缩包得到一个流量包，查看发现是键盘流量，tshark梭一把:

```
tshark -r bingbing.pcapng -T fields -e usb.capdata > data
```

脚本梭一把（这里我用的是神师傅的脚本，很舒服，一把梭）:得到

```
666c61677b3866396564326639333365662<DEL>3134613864303532336430333439653132393963 7d
```

DEL说明把2删掉，拿这串数字十六进制转字符得到
flag:flag{8f9ed2f933ef14a8d0523d0349e1299c}

3.歪比歪比

因为没报名，直接从别的师傅那拿了文件，是一个流量包（据说下载下来的还得改后缀）。随便选了一个追踪TCP流得到:

```
Surprise
Wabby Wabby:
j 29
z 31
7 25
e 31
l 23
6 37
4 32
p 38
h 27
g 26
x 28
i 25
u 27
n 25
8 36
0 24
o 23
c 28
y 24
1 29
b 26
m 27
2 28
v 25
d 33
f 28
9 33
t 21
w 22
a 31
r 24
s 16
k 32
5 25
q 23
3 32
{ 1
- 4
} 1
Wabby Wabbo:
0111110001000011001010001111011110101010011011011110100000110010111101000010010010001100001110010000011110011101
1011110110011111010000001110101000001011010010001111000000000101001101001010010111011100100011000111000100101110
0110001110011001101001100010101010001101111000111111111011100101110001010010111110000101101100100100100001011111
0101110111010111100010111011000011001011001101001010010111111001110101000110001001001100101110111101111000110010
0101111110001111100001010011001001000010011101001010111111011111100111010111010000001001001000111111110010001011
1010100100110111000101110110100100100101101000010111111100101111110011001010011111111000100110010001001001001111
0111110110110001101000010010110110001011010000100011010111110101110000110000010001111111110000101000100101101111
0001111001011010110011000101010110001100100111110010100111101001000110001011111101110110110000110110101000110111
0001000101000101000000000110100101001010011111101001011011001111010010101001010100101010001010101101001111000100
0011000100001010111001110001100101100001010111011110110111110000001011011111011101101000111111110100111100110011
1011111001111001011011011010101001100011001001101010111100000111111111000111100111010100111101010101111001111000
0100011111011111010001001111001100001000010000110010111110101011010110001110001001010000111000100101011001001001
```

```
0100010101101101001110000101111110101010110110110000010011000111000010001001101101101101100111000011000011010101
1110101011001010000110110010110001011011101000111100011001111011111011000100110110000111010101101111101001111111
1110000100011100000100101111101111001011010101111000111000110101001100010111110000111111101110011010100100001111
1101111111011001111110001110111110110010111000111011011110010101010110011001110110011110001111010000011010101000
1111101110111001011001001001000011111010100111011111001100111000000101001010001111001000110010111110000001111111
1100000001111111110111011111100111010010000010000001101111101000000001111010111011110110101100111101101010111100
0010110001101000111000111000001110110111000100011110101100100100011100111100101101010010110101011111110011100100
0001110110110101011011101110000010011001101110010001110010000001110001100101100001001000100010011110101010001011
0111100000011010111001110100101110011011110110111110000111100011000110101000011110010001111000110011011100110101
1100010101011110111111111100101100101010001101110101101101010101001110100001101011000100001111011011100101011000
0010010000110110001110111011100110011011101000000101000001011110100000001000011001101101111010011101000000101101 1
0101110100110111000000100111100011101001110001011111010101101110100110100110000110001101100101100010010001011011 1
1000010010001011110100010111010100101100101111010100001110111100000010010110101111001011000100011111100100000010 1
1100101110100011011011111011101110000101011001000010101010010100100010111010011001010101010011111100000100110100
1111010100100100111001011010011101111011000011110100001001111110001111111001111010011101011010011100010001111010 0
1110011110101111111111111110110101000000010100010010011110100110011011101011101011101100000100111110111100100000101
0110001101100000101100010011111111110111010110000101011111101110010111011111111001110111010010001110111101101111
0100101111001100011001100001001101100100110001001011111000011010000111011110011011010010101001011100100110010111
1010010001001111111100001011110101011000000111010100011101101011110011010100100111000111000100111111000100001001 1
0111101001110111110001011111100110000110100010001010001100111000110010010110001110111001011010001100011100110111
0101010100101001110111010010011110101110101001101010101011110111101011010000011111001111110100110101111010001010 1
1111101011100101101101001100011001111110111110010011110110110111011111101011101010010010111011100001110000100100 0
0111000101011101001111100110011001011111101101001111010000100010000110111110000011010110111010110001110011111110 0
0001111001000101101001011111110101010111001000000101001111101110010100010110101010110110100010100011001110110101
0110001100101011101110111100000000101000001111001101001100001111111101001110111001001110000011010011101111000000101
0101100000010000100001110111000011111111001001010011111110101011000000000001110110100001011001001110011100000010111
0110000011011010101100101100011100111111001010111100101101110100001000110001110111001010011100001111100111000110
0111110110111101010101011001000101011010001100000010001111110011001101111111010110010001111001100111110001110011
1000100110111001000100110110001100001001011111001111101111010100100011010100111001100010110011110001000110111101
0001110101110101011111111000001111011011101111000001011110011001110001101011110111111010000000100011111001011000 1
1110001101011111101111111011111011101010001101001000111000101111110101000110011000111011111110111111010000111101 1
1100101000111011101111110101011001110001011001000100111010010111100111110011111011100011101111111011100111100010 1
1001001101101010001110010101010101011000000010101110011011111100111100101001110000101011110011100110110111110011 0
1110011111001000000000111101011000111110001101010011011000010100100100111011111111001000000001010011111111010110 0
0010100000011101001010011110010110110010010010111001011111110
surprise message len: 1000
```

什么玩意这是。观察到{ }后面都是1联想到flag格式也是只有一个{和一个}，赛后了解到哈夫曼编码，说权重可能更好理解，直接上从或或师傅博客偷来的脑王的脚本

```
import copy
import re

def dfs(c, d):
    if len(c.keys()) == 1:
        # g = {'j':29,'z':31,'7':25,'e':31,'l':23,'6':37,'4':32,'p':38,'h':27,'g':26,'x':28,'i':25,'u':27,'n':25
,'8':36,'0':24,'o':23,'c':28,'y':24,'1':29,'b':26,'m':27,'2':28,'v':25,'d':33,'f':28,'9':33,'t':21,'w':22,'a':31
,'r':24,'s':16,'k':32,'5':25,'q':23,'3':32,'{':1,'-':4,'}':1,}
        # num = 0
        # for k in g.keys():
        #     num += g[k] * len(d[k])
        # print(num)
        # print(c, d)
        g = {}
        for k in d.keys():
            g[d[k]] = k
        a = '011111000100001100101000111101111010101001101101111010000011001011110100001001001000110000111001000
001111001110110111101100111110100000011101010000010110100100011110000000001010011010010100101110111001000110001 1
```

```
1000100101110011000111001100110100110001010101000110111100011111111101110010111000101001011111000010110110010010
0100001011111010111011101011110001011101100001100101100110100101001011111100111010100011000100100110010111011110
1111000110010010111111000111110000101001100100100001001110100101011111101111110011101011101000000100100100011111
1110010001011101010010011011100010111011010010010010110100001011111110010111111001100101001111111100010011001000
1001001001111011111011011000110100001001011011000101101000010001101011111010111000011000001000111111111000010100
0100101101111000111100101101011001100010101011000110010011111001010011110100100011000101111110111011011000011011
0101000110111000100010100010100000000011010010100101001111110100101101100111101001010100101010010101000101010110
1001111000100001100010000101011100111000110010110000101011101111011011111000000101101111101110110100011111111010
0111100110011101111110011110010110110110101010011000110010011010101111000001111111110001111001110101001111010101 0
1111001111000010001111101111101000100111100110000100001000011001011111010101101011000111000100101000011100010010
10110010010010100010101101101001110000101111110101010110110110000001001100011100001000100110110110110110011100001
10000110101011110101011001010000110110010110001011011101000111100011001111011110110001001101100001110101011011111
1010011111111111100001000111000000100101111110111100101101010111100011100011010100110001011111000011111110111001101
01001000011111101111111011001111110001110111111011001011100011101101111001010101011001100111011001111000111101000
00110101010001111101110111001011001001001000011111010100111011111100110011100000010100101000111100100011001011111
0000001111111110000000111111111011101111110011101001000001000000110111110100000000111101011101111011010110011110
1101010111100001011000110100011100011100000111011011100010001111010110010010001110011110010110101001011010101111
1110011100100000111011011010101101110111000001001100110111001000111001000000111000110010110000100100010001001111
010101000101101111000000110101110011101001011100110111101101111000011110001100011010100001111001000111100011001
10111001101011100010101011110111111111110010110010101000110111010110110101010100111010000110101100010000111101101
11001010110000001001000011011000111011101110011001101110100000001010000001011110100000001000011001101101111010011101
00000001011011010111010011011100000100111100011101001110001011111010101101110100110100110000110001101100101100010
0100010110111100001001000101111010001011101010010110010111101010000111011110000010010110101111001011000100011111
1001000000101110010111010001101101111101110111000010101100100001010101001010010001011101001100101010101001111110
00001001101001111010100100100111001011010011101111011000011110100001001111110001111110011110100111010110100111000
100011111010011100111101011111111111111011010100000001010001001001111010011001101110101110101110110000010011111011
1100100000010101100011011000000101100010011111111110111010110000101011111101110010111011111111100111011101001000111
01111011011110100101111001100011001100001001101100100110001001011111100001101000011101111001101101001010100101110
01001100101111101001000100111111100001011110101011000000111010100011101101011110011010100100111000111000100111111
0001000001001101111010011101111110001011111110011000011010001000101000110011100011001001011000111011100101101000110
0011100110111010101010010100111011101001001111010111010100110101010101111011101011010000011111001111110100110101
11101000101011111101011100101101101001100011001111101111110010011110110110111011111101011101010010010111011100001
1100001001000011100010101110100111110011001100101111110110100111101000010001000011011110000011010110111010110001
110011111110000011100100010110100101111111010101011100100000010100111110111001010001011010101011011010001010001
1001110110101011000110010101110111011110000000101000001111001101001100001111111010011101110010011100000110100111
0111100000101010110000010000100001110111000011111110010010100111111101010110000000000111011010000101100100111001
1100000010111011000001101101010110010110001110011111100101011110010110111010000100011000111011100101001110000111
11001110001100111110110111101010101011001000101011010001100000001000111111001100110111111101011001000111100110011
11100011100111000100110111001000100110110001100001001011111100111110111101010010001101010011100110001011001111000
1000110111101000111010111010101111111110000011110110111011110000010111100110011100011010111101111111010000000100011
11100101100011110001101011111110111111101111101110101000110100100011100010111111010100011001100011101111110111111
01000011110111100101000111011101111110101011001110001011001000100111010010111100111110011111011100011101111111011
100111100010110010011011010100011100101010101010110000000101011100110111111001111100101001110000101011110011100110
1101111100110111001111100100000000011110101100011111000110101001101100001010010010011101111111001000000010100111
1111110101100001010000001110100101001111001011011001001001011100101111110'
        m = ''
        st = 0
        while st < len(a):
            ed = st + 5
            while ed <= len(a):
                if a[st:ed] in g.keys():
                    m += g[a[st:ed]]
                    break
                else:
                    ed += 1
            st = ed
        print(re.findall(r'flag\{[a-f0-9-]*\}', m)[0])

    else:
        k0 = list(c.keys())[0]
```

```
        k1 = list(c.keys())[1]
        if c[k0] > c[k1]:
            k0, k1 = k1, k0
        for k in list(c.keys())[2:]:
            if c[k] < c[k1]:
                if c[k] < c[k0]:
                    k0, k1 = k, k0
                else:
                    k1 = k
        for a in k0:
            d[a] = '0' + d[a]
        for a in k1:
            d[a] = '1' + d[a]
        c[k0+k1] = c[k0]+c[k1]
        del c[k0]
        del c[k1]
        dfs(copy.deepcopy(c), copy.deepcopy(d))

c = {'j':29,'z':31,'7':25,'e':31,'l':23,'6':37,'4':32,'p':38,'h':27,'g':26,'x':28,'i':25,'u':27,'n':25,'8':36,'r
':24,'o':23,'c':28,'y':24,'1':29,'b':26,'m':27,'2':28,'v':25,'d':33,'f':28,'9':33,'t':21,'w':22,'a':31,'0':24,'s
':16,'k':32,'5':25,'q':23,'3':32,'{':1,'-':4,'}':1,}
d = {}
for k in c.keys():
    d[k] = ''
dfs(copy.deepcopy(c), copy.deepcopy(d))
# print(c)
```

得到flag:flag{50d477a2-6r36-dra9-9d63-49c2e9e5d1e5}

ps : tql !