

[buuctf]msic2

原创

[pipasound](#)  已于 2022-04-22 07:26:32 修改  419  收藏

分类专栏: [刷题记录](#) 文章标签: [misc](#)

于 2022-04-19 09:56:46 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/qq_61109509/article/details/124265520

版权



[刷题记录](#) 专栏收录该内容

37 篇文章 2 订阅

订阅专栏

之前写的没了, 这里简单记一下思路

文章目录

[被劫持的神秘礼物](#)

[刷新过得图片](#)

[snake](#)

[\[BJDCTF2020\]认真你就输了](#)

[藏藏藏](#)

[被偷走的文件](#)

[佛系青年](#)

[菜刀666](#)

[你猜我是个啥](#)

[秘密文件](#)

[just_a_rar](#)

[鸡你太美](#)

[神奇的二维码](#)

[梅花香自苦寒来](#)

[\[ACTF新生赛2020\]outguess](#)

[gakki](#)

[\[ACTF新生赛2020\]base64隐写](#)

[伟大的侦探](#)

[你能看懂音符吗](#)

[你有没有好好学网课](#)

被劫持的神秘礼物

打开wireshark,找到账户密码,串在一起用MD5加密

刷新过得图片

参考文章

猜测该题可能为F5隐写，通过kail下载F5隐写工具来解题

下载完成后进入F5隐写工具文件夹

```
cd F5-steganography
```

在该文件夹下对其图片进行解析

```
java Extract /图片所在位置/Misc.jpg
```

解析后会出现一个output.txt文件在F5隐写工具文件夹下

打开该文件夹,发现该文件夹下还藏有一个flag.txt文件

利用binwalk对该文件夹进行分离,得到flag

snake

010editor有个base64编码，解密后是

```
What is Nicki Minaj's favorite song that refers to snakes?
```

原来是anaconda（蟒蛇）。考点是蛇加密算法，serpent算法

binwalk分离，给了cipher文件

cipher导进去，key就是anaconda

Input type: File

File: C:\fakepath\cipher Browse

Function: SERPENT

Mode: ECB (electronic codebook)

Key: anaconda (plain)

Plaintext Hex

> Encrypt! > Decrypt! ▶ 🔗

100%
File was uploaded.

Decrypted text:

00000000	43 54 46 7b 77 68 6f 5f 6b 6e 65 77 5f 73 65 72	CTF{who_knew_ser
00000010	70 65 6e 74 5f 63 69 70 68 65 72 5f 65 78 69 73	pent_CSDN: @pipasounds

拿到flag

[BJDCTF2020]认真你就输了

binwalk分离xls表

藏藏藏

binwalk分离两次得到个docx，打开是个二维码，扫描即可

被偷走的文件

看到压缩包直接分离他

```
.16.66.188      FTP      116 Response: 227 Entering Passive Mode
.16.66.10       TCP      66 37088 → 21 [ACK] Seq=7 Ack=51 Win=2
.16.66.10       FTP      81 Request: RETR flag.rar
16.66.188      TCP      66 21 → 37088 [ACK] Seq=51 Ack=22 Win=
```

是个加密压缩包。看了一下不是伪加密，那就暴力破解

佛系青年

考点zip伪加密与与佛论坛

菜刀666

之前专门写过

这篇文章

你猜我是个啥

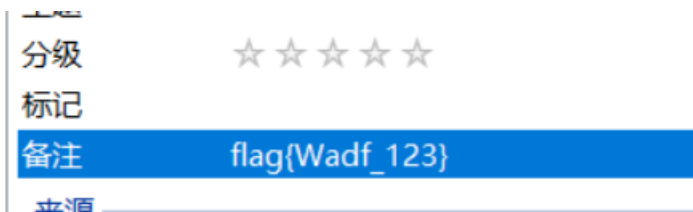
010打开发现flag

秘密文件

binwalk分离和暴力破解密码

just_a_rar

还是爆破题，最后记得 [看注释](#)



鸡你太美

恢复gif头就行

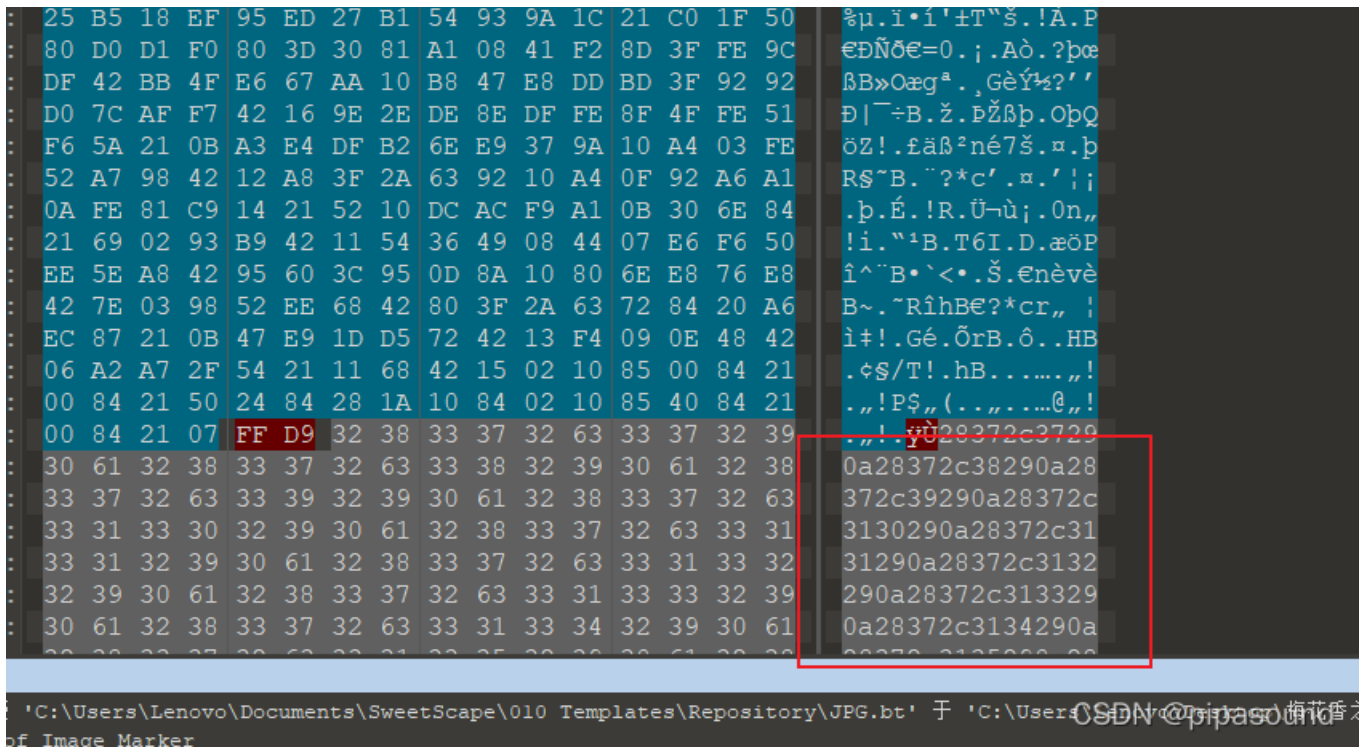
神奇的二维码

扫描没用，直接binwalk分离，发现四个压缩包，挨个解密，全是base64编码。每个解密都对着上一个的密码到最后一个是个音频，转摩斯电码即可

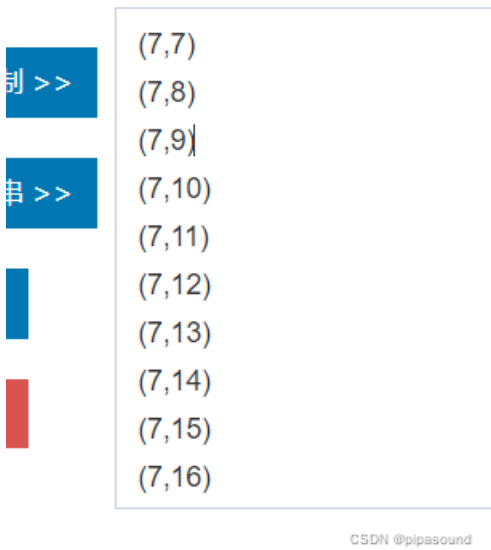
梅花香自苦寒来

打开图片，翻看010editor

```
: 13 EC 83 2F CD 5B 9D AA B4 9E C6 50 2E 68 C4 87 .if/í[.ª'žEP.hÄ#
: 13 E8 D2 56 C8 41 88 B8 A6 46 05 42 3B 53 77 F4 .èÒVÈA^,¡F.B;Swô
: 47 E6 A9 FF 00 76 B7 FE 4B FF 00 A2 D9 1C D0 63 Gæ@ý.v·pKý.çÛ.Đc
: F9 AA 7F DD AD FF 00 92 FF 00 E8 B2 A0 69 53 73 ùª.Ý-ý.'ý.è² iSs
: DF FC 57 3E A1 92 4D 27 7D 36 5C B4 20 C8 57 A7 BúW>¡'M'}6\`ÈWŞ
: 80 4B 81 EE D2 3F 64 FC FA 5F F5 8D 1E EB 44 2A €K.îÒ?diúú_õ...èD*
```



把这些十六进制复制出来，十六进制转asc码



看到了这么多坐标，可以想到绘图，描出二维码。用python里的matplotlib模块格式要改成这样



代码

```
import matplotlib.pyplot as plt
import numpy as np

x,y=np.loadtxt('./1.txt',delimiter=',',unpack=True)
plt.plot(x,y,'.')
plt.show()
```

得到二维码

[ACTF新生赛2020]outguess

里面有很多文件，但主要是这个



社会主义核心价值观在线解密：<http://ctf.ssleye.com/cvencode.html>

解码abc

结合题目名字，对这张图片进行使用outguess导出隐写内容(kali)

```
outguess -k 'abc' -r mmm.jpg flag.txt
```

gakki

先binwalk 分离和四位数爆破，发现一堆无规律字符 借助大佬脚本统计

```
# -*- coding:utf-8 -*-
#Author: mochu7
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- =\\{\}\[\]"
strings = open('C:/Users/lenovo/Desktop/_wolaopo.jpg.extracted/218E8/flag.txt').read()

result = {}
for i in alphabet:
    counts = strings.count(i)
    i = '{0}'.format(i)
    result[i] = counts

res = sorted(result.items(),key=lambda item:item[1],reverse=True)
for data in res:
    print(data)

for i in res:
    flag = str(i[0])
    print(flag[0],end="")
```

[ACTF新生赛2020]base64隐写

扫描二维码得到个网址，打开看到大量base64.还是大佬解密

```

def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res

def solve_stego():
    with open('ComeOn!.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)

def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str

if __name__ == '__main__':
    solve_stego()

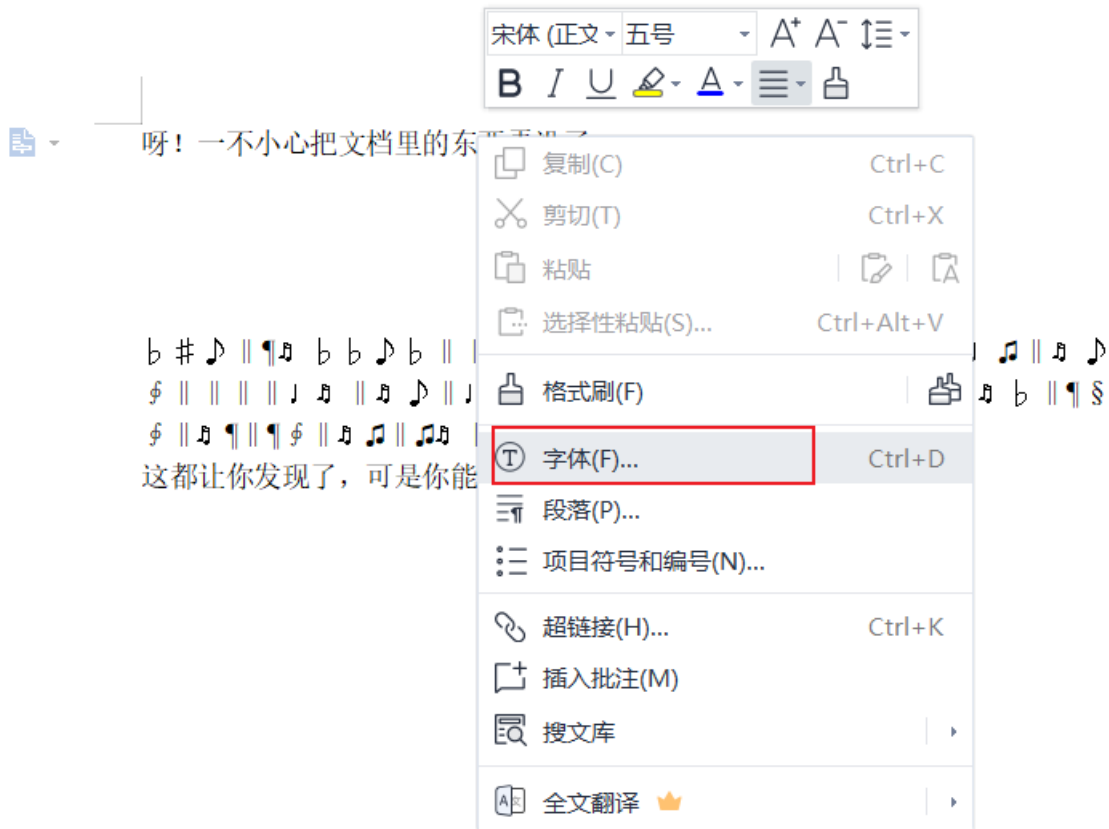
```

伟大的侦探

考点:

摩尔福斯小人密码

修复rar文件头 52 61 72 21 1A 07 00 ， 出现一个文档，发现有些字被隐藏了



CSDN @pipasound

取消隐藏，音乐字符解码

你有没有好好学网课

- 敲击码

敲击码

```
1 | ..... ./... ./... ./... ./...
```

敲击码(Tap code)是一种以非常简单的方式对文本信息进行编码的方法。因该编码对信息通过使用一系列的点击声音来编码而命名,

敲击码是基于5×5方格波利比奥斯方阵来实现的, 不同点是是用K字母被整合到C中。

敲击码表:

1	2	3	4	5	
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Bash

<https://blog.csdn.net/mochu7777777>

/ 为划分

```
1 | ..... ./... ./... ./... ./... ./... ./...
2 | 5,2 3,1 3,1 3,2
3 | W L L M
```

CSDN @pipasound