




BUUCTF MISC刷题

原创

[五五六六0524](#)  已于 2022-03-17 19:12:44 修改  2117  收藏 2

分类专栏: [CTF积累及刷题](#) 文章标签: [安全](#)

于 2022-01-12 11:02:00 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/wow0524/article/details/122448957>

版权



[CTF积累及刷题](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

目录

[题1、LSB](#)

[题2、镜子里面的世界](#)

[题3、ningen](#)

[题4、面具下的flag](#)

[题5、FLAG](#)

[题6、假如给我三天光明](#)

[题7、九连环](#)

[题8、后门查杀](#)

[题9、webshell后门](#)

[题10、荷兰宽带数据泄露](#)

[题11、刷新过的图片](#)

[题12、被劫持的神秘礼物](#)

[题13: 认真你就输了](#)

[题14: snake](#)

[题15: 藏藏藏](#)

[题16: 佛系青年](#)

[题17: 菜刀666](#)

[题18: 被偷走的文件](#)

[题19: 你猜我是个啥](#)

[题20: 梅花香自苦寒来](#)

[题21: 秘密文件](#)

题22: just_a_rar
题23: 神奇的二维码
题24: 一叶障目
题25: 鸡你太美
题26: 穿越时空的思念
题27: excel破解
题28: find_me
题29: 纳尼
题30: outgess
题31、谁赢了比赛
题32、来题中等的吧
题33、我有一只马里奥
题34、[GXYCTF2019]gakki
题35、[SWPU2019]伟大的侦探
题36、[GUET-CTF2019]KO
题37、黑客帝国
题38、[MRCTF2020]ezmisc
题39、sqltest
题40、弱口令
题41、[HBNIS2018]caesar
题42、[HBNIS2018]低个头
题43、[SUCTF2018]single dog
题44、Mysterious
题45、喵喵喵
题46、[MRCTF2020]你能看懂音符吗
题47、NTFS数据流
题48、我吃三明治
题49、john-in-the-middle
题50、[安洵杯 2019]吹着贝斯扫二维码
题51、[ACTF新生赛2020]swp
题52、[GXYCTF2019]SXMgdGhpcyBiYXNIPw==

题1、LSB

StegSolve 1.3.3... File Analyse Help

- File Format
- Data Extract
- Stereogram Solver
- Frame Browser
- Image Combiner

Extract Preview

```
89504e470d0a1a0a 0000000d49484452 .PNG.... .IHDR
0000011800000118 080200000008ec7e .....~
db00000542494441 54789ceddd416e23 ....BIDA Tx...An#
391000416931ffff b2f707c480932e57 9..Ail.. ....W
cb1157c3564b5682 8702c9f7d7d70b ..W.VKV. ....
f837ffffdf403c027 1012048404012141 .7.....' .....!A
4048101012048404 012141e0cfe167ef @H.....!A...g.
f77bec39729383e6 c30775788cbbdfca .{.9r... .ux...
e5ffe5bbb7bcdff9 9f62458280902020 ..... .bE...
2408080902428280 9020202408080902 $.B.. . $.
```

Bit Planes

Alpha 7 6 5 4 3 2 1 0

Red 7 6 5 4 3 2 1 0

Green 7 6 5 4 3 2 1 0

Blue 7 6 5 4 3 2 1 0

Order settings

Extract By Row Column

Bit Order MSB First LSB First

Bit Plane Order

RGB GRB

RBG BRG

GBR BGR

Preview Settings

Include Hex Dump In Preview

Preview Save Text Save Bin Cancel

CSDN @五五六六0524

网上教程有很多，具体就是Analyse->Data Extract，选中RGB通道的0，然后Save Bin保存为png就行了

题2、镜子里面的世界

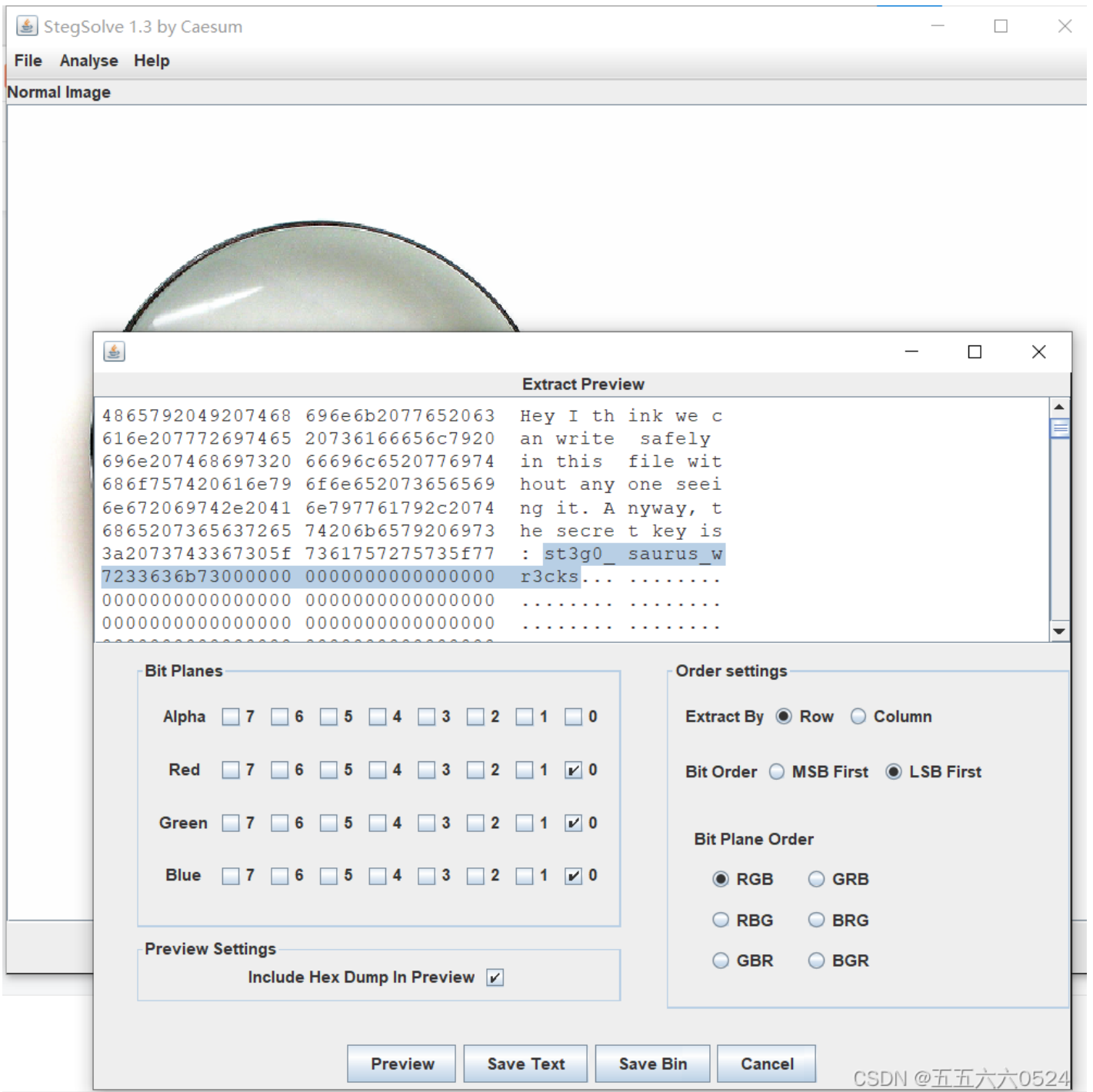
binwalk发现里面没有

```
(root@kali)-[~/Desktop]
└─# binwalk -e steg.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 800 x 600, 8-bit/color RGB, non-interlaced
83	0x53	Zlib compressed data, best compression

CSDN @五五六六0524

用stegsolve



题3、ningen

binwalk发现里面有一个压缩包，打开需要密码

```

(root@kali)-[~/home/kali/Desktop]
└─# binwalk -e 3.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01

WARNING: Extractor.execute failed to run external extractor 'jar xvf %e': [
Errno 2] No such file or directory: 'jar', 'jar xvf %e' might not be instal
led correctly
38689       0x9721      Zip archive data, encrypted at least v2.0 to ex
tract, compressed size: 50, uncompressed size: 38, name: ningen.txt
38871       0x97D7      End of Zip archive, footer length: 22

```

CSDN @五五六六0524

尝试爆破，根据提示应该是4位数，爆破得到密码8368，解开得到flag{b025fc9ca797a67d2103bfbc407a6d5f}

题4、面具下的flag

binwalk一下得到压缩包，用winhex打开发现是标准伪加密，09改成00就行

```
2:5860h: FE EF 2D FE 9F 25 FE 7F F8 BF 18 FF F7 16 FF CF
2:5870h: 13 FF 3F FD 5F 8C FF 7B 8B FF 17 89 FF 5F FE 2F
2:5880h: C6 FF BD C5 FF CB C4 FF 6F FF 17 E3 FF DE E2 FF
2:5890h: 55 E2 FF 8F FF 8B F1 7F 6F F1 FF 3A F1 FF D7 FF
2:58A0h: C5 F8 BF B7 F8 7F 93 F8 FF E7 FF 62 FC DF 9B FE
2:58B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00
2:58C0h: 00 00 00 00 00 00 00 00 00 00 90 F1 07 50 4B
2:58D0h: 01 02 3F 00 14 00 09 00 08 00 6C 87 42 49 56 A1
2:58E0h: A2 02 A7 58 02 00 00 00 30 00 09 00 24 00 00 00
2:58F0h: 00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67
2:5900h: 2E 76 6D 64 6B 0A 00 20 00 00 00 00 00 01 00 18
2:5910h: 00 B8 22 67 44 8B 1C D2 01 70 51 53 E0 85 1C D2
2:5920h: 01 70 51 53 E0 85 1C D2 01 50 4B 05 06 00 00 00
2:5930h: 00 01 00 01 00 5B 00 00 00 CE 58 02 00 00 00 00
```

.....ñ.PK
..?....l+BIV;
\$.SX...0...\$...
.....flag
.vmdk..
,"gD<.ò.pQSà...ò
.pQSà...ò.PK....
.....[...îX....

CSDN @五五六六0524

在kali中打开vmdk“7z x flag.vmdk -o.”，在key_part_one（Brainfuck编码）和key_part_two（Ook!编码）中分别得到flag的一半

题5、FLAG

binwalk一下，发现有zlib，怀疑是zsteg隐写

```
(kali@kali)-[~/桌面]
└─$ binwalk 1.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 664 x 586, 8-bit/color RGB, non-interlaced
41	0x29	Zlib compressed data, default compression

CSDN @五五六六0524

果然

```
(kali@kali)-[~/桌面]
└─$ zsteg 1.png
```

```
imagedata .. text: "KK<220\r\r"
b1,rgb,lsb,xy .. file: Zip archive data, at least v2.0 to extract
b1,bgr,msb,xy .. text: "saZ$S:'6"
b3,b,lsb,xy .. text: "#?/(9Rk;"
b3,rgb,lsb,xy .. text: "~G#\rwW:U"
b4,r,lsb,xy .. text: "Ewe##333#\ "#"
b4,r,msb,xy .. text: ";UUUUUUU"
b4,g,lsb,xy .. text: "yffgfTS22"
b4,g,msb,xy .. text: "gF87rqw@Bw"
b4,b,lsb,xy .. text: "ffffvvgwfvfw"
b4,rgb,msb,xy .. text: "Dsr@3%\ "7"
b4,bgr,msb,xy .. text: "vCp2C\"5'"
```

CSDN @五五六六0524

把这个通道中的zip提取出来，zsteg -e b1,rgb,lsb,xy 1.png -> out.zip，解压后得到一个1文件

```
(kali@kali)-[~/桌面]
└─$ file 1
```

```
1: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.24, BuildID[sha1]-8df45089fa39fec83423ec37a944e81065d16bee, not stripped
```

CSDN @五五六六0524

查找一下里面的字符，直接出，flag{dd0gf4c3tok3yb0ard4g41n~~~}


```

j1 69 B8 48 34 83 48 D3 01 E9 FC 59 | 4IHÓ i,H4IHÓ éúY
j1 50 4B 01 02 3F 00 14 00 01 08 08 | 1IHÓ PK ?
4B 8C 3A D5 7E 88 70 00 00 28 75 00 | HNSKI:Ö~lp (u
j0 00 00 00 00 00 00 20 00 00 00 22 | $ CSDN @五五六六0524

```

用steghide查找这张图“steghide info good.jpg”，密码为空，发现图片里面有ko.txt文件，提取出来“steghide extract -sf good.jpg”，得到bV1g6t5wZDJif^J7

```

(root@kali)-[~/home/kali/Desktop]
└─# steghide info good.jpg
"good.jpg":
  format: jpeg
  capacity: 1.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "ko.txt":
    size: 48.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

```

解压得到flag{1RTo8w@&4nK@z*XL}

现在遇到的图片隐写有LSB、steghide、zsteg，还不太懂他们之间有什么区别，什么时候应用，待查

题8、后门查杀

webshell会报毒，用火绒查杀一下得到具体路径，根据题目得到提示密码pass即flag，在kali里查找关键字pass，得到flag

风险项目	状态
<input checked="" type="checkbox"/> C:\Users\86139\Desktop\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d.rar >> html\include\include.php 后门病毒 Backdoor/PHP.WebShell.h	待处理 详情

```

kali@kali: ~/桌面/html/include
└─(kali@kali)-[~/桌面/html/include]
└─$ cat include.php | grep 'pass'
//echo encode_pass('angel');exit;
$pass = '6ac45fb83b3bc355c024f5034b947dd3'; //angel
    scookie('loginpass', '', -86400 * 365);
if($pass) {
    if ($pass == encode_pass($P['password'])) {
        scookie('loginpass', encode_pass($P['password']));
    }
    if (isset($_COOKIE['loginpass'])) {
        if ($_COOKIE['loginpass'] != $pass) {
            $dbpass = isset($_P['dbpass']) ? $_P['dbpass'] : '';
            $DB->connect($dbhost, $dbuser, $dbpass, $dbname);
            makeinput(array('name' => 'dbpass', 'size' => 15, 'value' => $dbpass));
            if ($dbhost && $dbuser && isset($dbpass)) {
                $DB->connect($dbhost, $dbuser, $dbpass, $dbname);
                seccparam('Readable /etc/passwd', @is_readable('/etc/passwd')
? "yes" : 'no');
            makeinput(array('name' => 'password', 'type' => 'password', 'size' => '20'));
            } elseif(function_exists('passthru')) {
                @passthru($cfe);
                return ' / <a href="#" title="User: '.$array['name'].
'#136#10Passwd: '.$array['passwd'].'#136#10Uid: '.$array['uid'].'#136#10gid: '.$array['gid'].'#136#10Gecos: '.$array['gecos'].'#136#10Dir: '.$array['dir'].'#136#10Shell: '.$array['shell'].'">'.$array['name'].'</a>';
function encode_pass($pass) {
    $pass = md5($k.$pass);

```

kali查找文件里的关键字：1、grep +'关键字' +文件名，2、cat +文件名 |grep +"关键字"，3、cat +文件名 |grep +"关键字" -A/B/C/v +数字 得到关键字之后/前/前后几行的内容，v是排除关键字那一行

kali查看当前文件夹中包含关键字的文件：grep -r '关键字'

kali查看文件内容：1、vim+文件名，2、cat +文件名，3、cat -n +文件名 显示行号

通配符：引自<https://blog.csdn.net/liyuru4/article/details/51834669>

1、“*”用于匹配文件中任意长度的字符串，可以代表很复杂很长的字符串。

例：*.cpp *.c

2、“?”和“*”类似，但只匹配一个字符。

例：\$ ls queue.?

queue.c

3、“[]”用于匹配所有出现在方括号内的字符,一个文件只能匹配一个字符。

例：\$ ls text[1A]

text1 textA

4、“-”来指定一个字符集范围，所有包含在上下界(可以是数字或字母)之间的字符都会被匹配。

例：\$ ls text[1-3]

text1 text2 text3

题9、webshell后门

和上一题同样的做法

<input checked="" type="checkbox"/> 风险项目	状态
<input checked="" type="checkbox"/> C:\Users\86139\Desktop\827baa91-be16-43a4-8762-d215f5f55382.rar >> member\zp.php 后门病毒 Backdoor/PHP.WebShell.h	待处理 详情 CSDN @五五六六0524


```
root@kali: /home/kali/F5-steganography
文件 动作 编辑 查看 帮助

(kali@kali)-[~/F5-steganography]
└─$ sudo su
[sudo] kali 的密码:
(kali@kali)-[~/F5-steganography]
└─# java Extract /home/kali/桌面/Misc.jpg
Huffman decoding starts
Permutation starts
309504 indices shuffled
Extraction starts
Length of embedded file: 190 bytes
(1, 31, 5) code used

(kali@kali)-[~/F5-steganography]
└─#
```

CSDN @五五六六0524

题12、被劫持的神秘礼物

根据题目提示找账号密码，追踪tcp.stream eq 0，admina+adminb

```
Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · gift.pcapng

POST /index.php?r=member/index/login HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://192.168.60.123/index.php?r=member/index/login
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 192.168.60.123
Content-Length: 129
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=ubkh99eqgp4apge0n5stkimna4

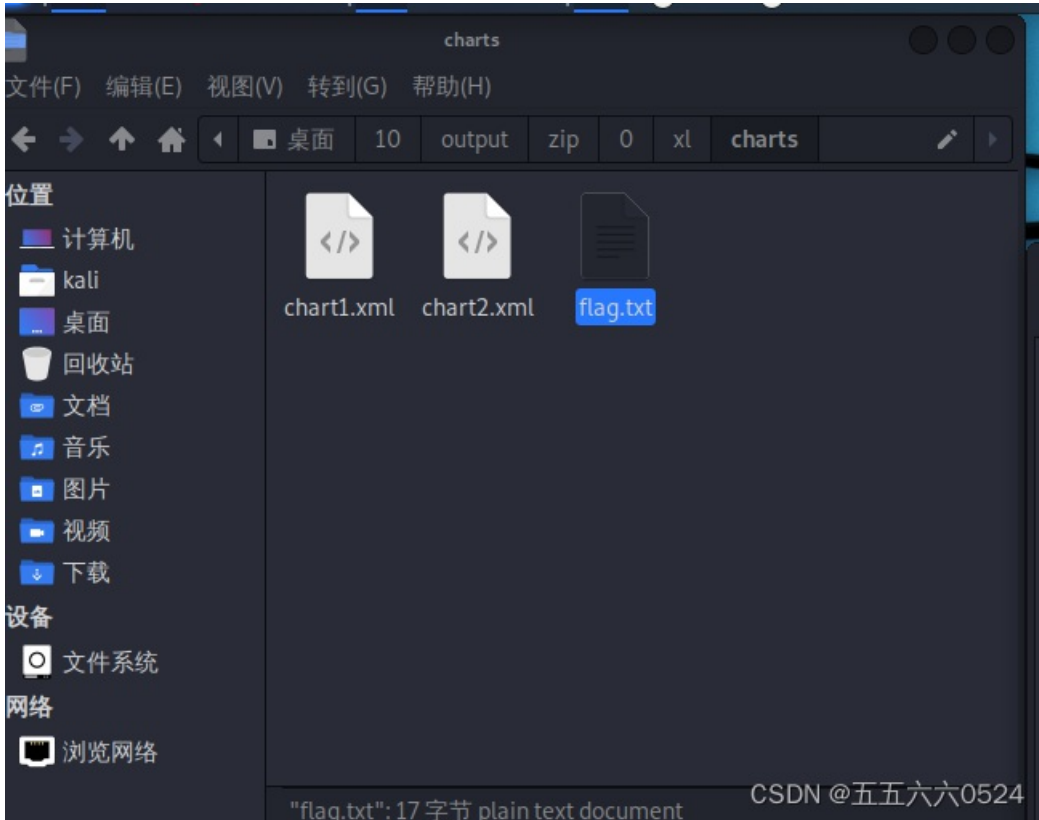
name=admina&word=adminb&cooktime=0&checkcode=5129&returnurl=http%3A%2F%2F192.168.60.123%2Findex.php%3Fr%3Ddefault%2Findex%2FindexHTTP/1.1 302 Found
Date: Wed, 03 Dec 2014 05:51:53 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Set-Cookie: yx_auth=da73XtTCqWpRWn%2Fi54TTa1mwjLXu6Iffs392Ux2o4RQXyF08uwKAN0Teu8Lae0Hr07AdsDITqLLmrc6lItPgiqV5BA6J3Q4Mw; path=/
location: http://192.168.60.123/index.php?r=default/index/index
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

CSDN @五五六六0524

用32位小写MD5哈希一下得到flag{1d240aafe21a86afc11f38a45b541a49}

题13：认真你就输了

直接拖进kali里，binwalk发现里面有东西，foremost分离，真不好找，flag{M9eVfi2Pcs#}



题14: snake

foremost分离得到key和cipher，key里面是base64加密的，解密后得到

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

找到这个人于蛇相关的最喜欢的歌，找了个[wpbuuctf-misc-snake 详解 - junlebao - 博客园](#)，是anaconda，加密算法是Serpent，也有蛇的意思，flag{who_knew_serpent_cipher_existed}

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 pent _ cipher _ exis ted }
00000010	70 65 6e 74 5f 63 69 70 68 65 72 5f 65 78 69 73	
00000020	74 65 64 7d 00 00 00 00 00 00 00 00 00 00 00 00	

[\[Download as a binary file\] \[?\]](#) Inactive

Checkout ?

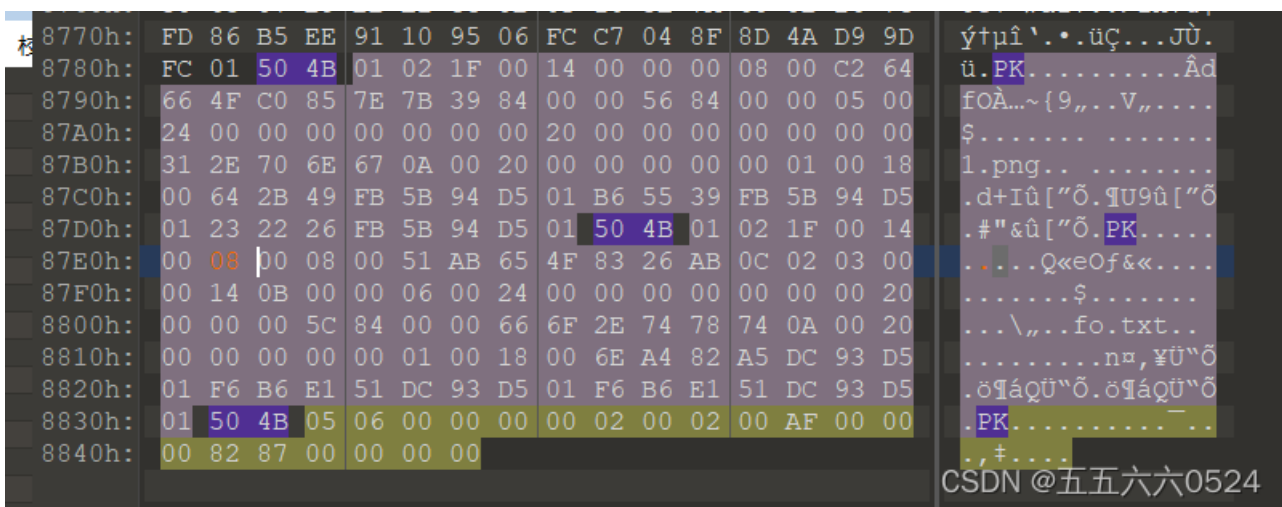
CSDN @五五六六0524

题15: 藏藏藏

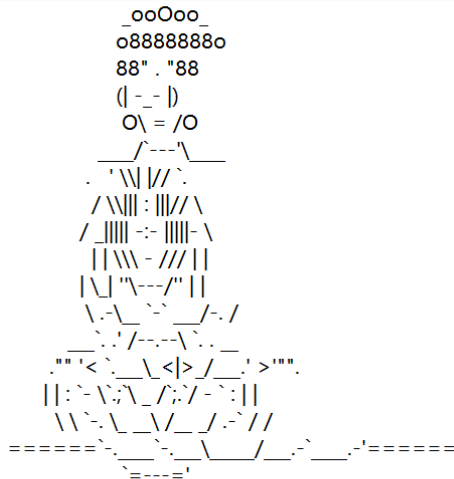
binwalk一下那张图，发现有压缩包，解压之后得到福利.docx，无法直接打开，又binwalk一下发现里面有东西，改后缀，在/word/media/里有一张二维码，一扫就出来了，flag{you are the best!}

题16: 佛系青年

还以为第图片隐写，找了半天没看出来啥，最后根据wp发现是伪加密，09改成08即可



解压得到一张图和一个文本



佛祖保佑 永无BUG
 写字楼里写字间，写字间里程序员；
 程序人员写程序，又拿程序换酒钱。
 酒醒只在网上坐，酒醉还来网下眠；
 酒醉酒醒日复日，网上网下年复年。
 但愿老死电脑间，不愿鞠躬老板前；
 奔驰宝马贵者趣，公交自行程序员。
 别人笑我忒疯癫，我笑自己命太贱；
 不见满街漂亮妹，哪个归得程序员？

佛曰：遮等諳勝能礙嶙藐哆娑梵迦侄羅哆迦梵者梵楞蘇涅侄室實真鉢朋能。奢但俱道怯都諳怖梵尼怯一罰心鉢謹鉢薩苦奢夢怯帝梵遠朋陀諳陀穆諳所訥知涅侄

把佛曰的内容用与佛论禅翻译一下即可与佛论禅

flag{w0_fo_ci_Be1}

题17: 菜刀666

wireshark打开，搜了一下，在tcp.stream eq 1里找到flag.txt，扔kali里分离得到一个压缩包，暴力破解破不开，需要找密码


```
Date: Fri, 08 Dec 2017 11:41:29 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 180
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
->|./ 2017-12-08 11:38:58 0 0777
../ 2017-12-08 11:39:10 4096 0777
1.php 2017-12-08 11:33:16 33 0666
flag.txt 2017-12-08 11:35:29 17 0666
hello.zip 2017-12-08 09:32:36 224 0666
|<-POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; c
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 725
```

```
aa=@eval.
(base64 decode($ POST[action])):&action=0GluaV977X0oTmRnc
```

在tcp.stream eq 7里找到一大堆字符串，z1翻译是D:\wamp64\www\upload\6666.jpg7，z2应该就是这张图了，从FFD8复制到FFD9，扔winhex里粘帖至新文件，命名成666.jpg，得到解压密码

```
...RidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNVZG...
...3D&z1=RDpdc2FtcDY0XHd3d1x1cGxvYWRCnJyY2Ni5qcGc%3D&z2=FFD8FFE000104A46...
...010101010101010101010101010101010101010101010101010101010101010101...
...001108013901E203012200021101031101FFC4001F000001050101010101000000...
...A1082342B1C11552D1F02433627282090A161718191A25262728292A343536373839=
```



CSDN @五五六六0524 解压得flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}

题18: 被偷走的文件

扔kali里分离提取出来一个rar压缩包，爆破得密码5790，解压得flag{6fe99a5d03fb01f833ec3caa80358fa3}



题19: 你猜我是个啥

下载下来是一个压缩包，打不开，显示文件已损坏，扔winhex里一看文件头是“89504E47”，改后缀为png出现一个二维码，扫了一下是“flag不在这”，扔kali里binwalk一下，发现zlib标识，zsteg

隐写

```

(kali@kali)-[~/桌面]
└─$ binwalk attachment.png

```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 245 x 256, 8-bit/color RGBA, non-interlaced
41	0x29	Zlib compressed data, default compression

CSDN @五五六六0524

直接出，flag{i_am_flg}

```

(kali@kali)-[~/桌面]
└─$ zsteg attachment.png
[?] 24 bytes of extra data after image end (IEND), offset = 0x4b5
extradata:0 .. text: "\r\n%00*aflag{i_am_flg}\r\n"

```

CSDN @五五六六0524

题20: 梅花香自苦寒来

binwalk没有发现什么，winhex一下发现里面有一大堆数字，很奇怪，剩下的就不太会了，<https://www.cnblogs.com/harmonica11/p/11365812.html>flag{40fc0a979f759c8892f4dc045e28b820}

题21: 秘密文件

在wireshark里搜了一下flag，发现，应该是传输的rar

```
Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng

220 HI, i know you are a hacker who is trying to hack me ,but can u find where is the flag?a
USER ctf
331 Password required for ctf
PASS ctf
230 Client :ctf successfully logged in. Client IP :172.16.66.100
PORT 172,16,66,100,30,158
200 Port command successful.
LIST
150 Opening ASCII mode data connection for directory list.
226 Transfer complete.
PORT 172,16,66,100,30,162
200 Port command successful.
RETR 6b0341642a8ddcbeb7eca927dae6d541.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete.
QUIT
220 Bye
```

CSDN @五五六六0524

foremost分离出来，爆破一下，密码是1903，flag{d72e5a671aa50fa5f400e5d10eedeaa5}

题22: just_a_rar

解压出来是4位数.rar，爆破得密码是2016，解压得到一张图片，放winhex里直接得flag{Wadf_123}

```
-----
00001040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00001070 00 00 00 00 00 00 00 00 00 00 00 00 00 66 00 6C 00
00001080 61 00 67 00 7B 00 57 00 61 00 64 00 66 00 5F 00
00001090 31 00 32 00 33 00 7D 00 00 00 FF E1 08 DD 68 74
000010A0 74 70 3A 2F 2F 6E 73 2E 61 64 6F 62 65 2E 63 6F
000010B0 6D 2F 78 61 70 2F 31 2E 30 2F 00 3C 3F 78 70 61
000010C0 63 6B 65 74 20 62 65 67 69 6E 3D 27 EF BB BF 27
000010D0 20 69 64 3D 27 57 35 4D 30 4D 70 43 65 68 69 48
-----
```

f l
a g { W a d f _
1 2 3 } y á Ýht
tp://ns.adobe.co
m/xap/1.0/ <?xpa
cket begin='i>¿'
id=WSM0pCehIn

题23: 神奇的二维码

解压得到一张二维码，扫了一下，什么也没有

Free Online Barcode Reader

To get such results using [ClearImage SDK](#) use [TBR Code 103](#).

If your **business** application needs barcode recognition capabilities, email your technical questions to support@inlittersearch.com, email your sales inquiries to sales@inlittersearch.com

File: **BitcoinPay.png** New File

Pages: **1** Barcodes: **1**


Barcode: 1 of 1 Page 1 of 1

Type: **QR**

Length: 25 Rotation: none

Module: 11.6pix Rectangle: {X=15,Y=15,Width=368,Height=368}

`swpuctf{flag_is_not_here}`



CSDN @五五六六0524





binwalk一下发现里面有rar，奇怪的是foremost提取不出来，binwalk -e +文件名提取出来了

```
(kali@kali)-[~/桌面]
└─$ binwalk 1.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 400 x 400, 8-bit/color RGBA, non-interlaced
28932	0x7104	RAR archive data, version 5.x
29034	0x716A	RAR archive data, version 5.x
94226	0x17012	RAR archive data, version 5.x
99220	0x18394	RAR archive data, version 5.x

CSDN @五五六六0524

得到4个压缩包

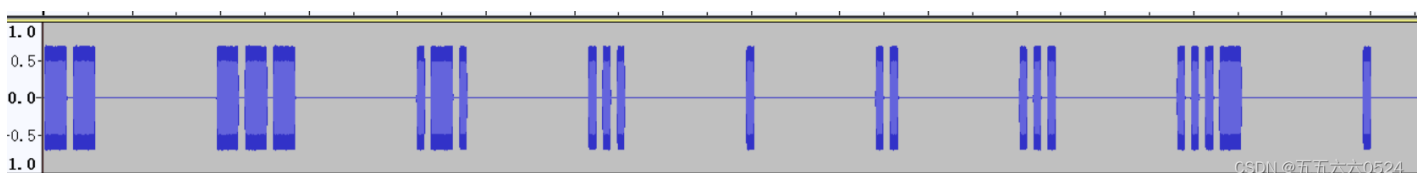
-  716A.rar
 -  7104.rar
 -  17012.rar
 -  18394.rar
- CSDN @五五六六0524

17012.rar解压得到flag.docx，里面是base64，一直解密解密，（这位写了一个脚本，还挺好用的[BUUCTF: \[SWPU2019\]神奇的二维码_末初·mochu7-CSDN博客_buuctf神奇的二维码](#)），得到comEON_YOUAreSOSoS0great

7104.rar解压得到encode.txt，YXNkZmdoamtsMTIzNDU2Nzg5MA==，base64解密得asdfghjkl1234567890

716A.rar解压得到一张图和一个加密的rar，密码就是asdfghjkl1234567890，两张图一样，没啥用

18394.rar的密码就是comEON_YOUAreSOSoS0great，解压得到good.mp3，用Audacity打开，



摩斯密码，解密一下就行，flag{morseisveryeasy}

题24: 一叶障目

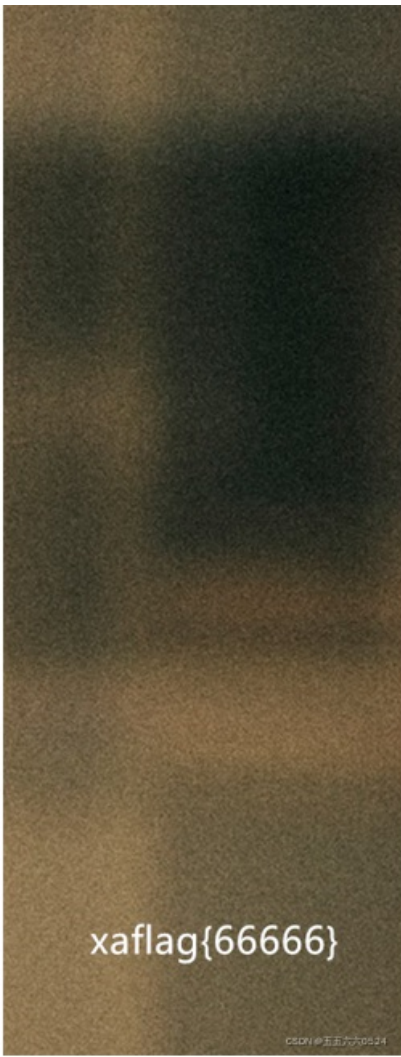
扔kali里说CRC错误



找了个脚本[Buuctf 一叶障目_Dexret的博客-CSDN博客_buuctf一叶障目](#)

```
#coding=utf-8
import zlib
import struct
#读文件
file = '1.png' #注意, 1.png图片和脚本在同一个文件夹下哦~
fr = open(file, 'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\x', '').replace("b'", '0x').replace("'", ''))
#crc32key = 0xCBD6DF8A #补上0x, copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x00\x01\xF1\x08\x06\x00\x00\x00') #hex下copy grep
n = 4095 #理论上0xffffffff,但考虑到屏幕实际, 0xfff就差不多了
for w in range(n):#高和宽一起爆破
    width = bytearray(struct.pack('>i', w))#q为8字节, i为4字节, h为2字节
    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]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width,height)
            #写文件
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png', 'wb')#保存副本
            fw.write(newpic)
            fw.close
```

校验过后出了一张图片, flag{66666}



题25: 鸡你太美

下载下来是两张动图，扔kali里binwalk一下，关键应该在篮球副本的那张图

```

kali@kali: ~/桌面/attachment (1)
文件 动作 编辑 查看 帮助
(kali@kali)-[~/桌面/attachment (1)]
└─$ binwalk 1.gif
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0             0x0             GIF image data, version "89a", 180 x 320

kali@kali)-[~/桌面/attachment (1)]
└─$

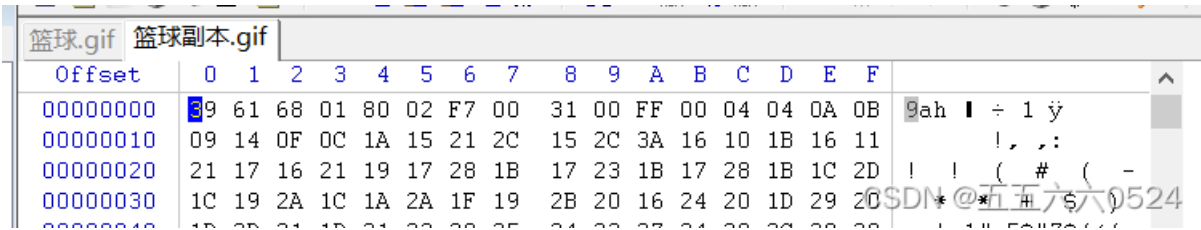
kali@kali: ~/桌面/attachment (1)
文件 动作 编辑 查看 帮助
(kali@kali)-[~/桌面/attachment (1)]
└─$ binwalk 2.gif
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
4985629      0x4C131D       gzip compressed data, has header CRC, last modified: 2007-04-12 01:45:04
5901030      0x5A0AE6       Certificate in DER format (x509 v3), header length: 4, sequence length: 3072
10737487     0xA3D74F       MySQL ISAM index file Version 8

kali@kali)-[~/桌面/attachment (1)]
└─$ foremost 2.gif
Processing: 2.gif
|*|

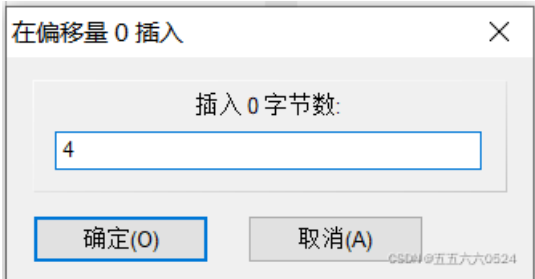
kali@kali)-[~/桌面/attachment (1)]
└─$
  
```

扔winhex里，篮球副本少了个“47494638”的文件头

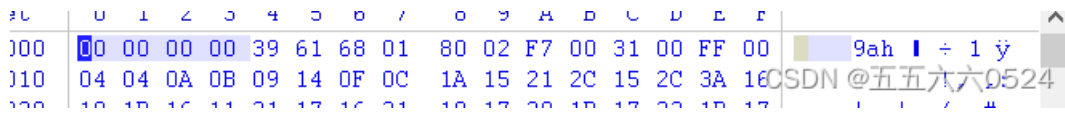
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	47	49	46	38	39	61	B4	00	40	01	F6	31	00	1C	18	25	GIF89a' @ 01 %
00000010	1D	1A	2B	1E	1F	36	21	1C	2C	24	1E	34	28	23	39	36	+ 6! , \$ 4(#96
00000020	28	39	27	26	43	3C	2D	43	45	37	4D	51	43	56	56	4E	09 50 7E 70 C7 V0
00000030	67	6A	58	6D	78	64	78	77	6D	80	8A	74	80	88	7A	87	~ i Y a d r o m m l l + l l l



选中开头第一个，编辑-粘贴0字节-插入4个字节



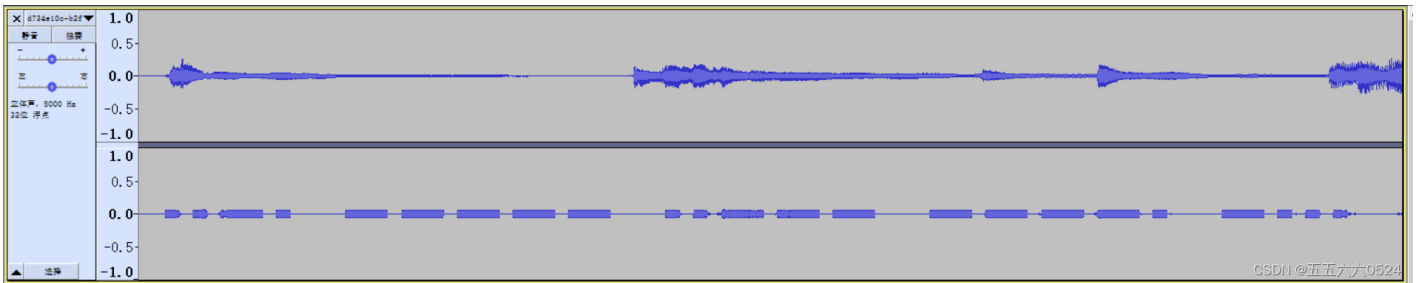
然后变成这样，直接把“00000000”修改成“47494638”，然后保存就行了



篮球副本上出现flag，flag{zhi_yin_you_are_beautiful}



题26: 穿越时空的思念



摩斯密码解密, flag{f029bd6f551139eedeb8e45a175b0786}

题27: excel破解

flag{office_easy_cracked}

attachment.xls																	
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000422A0	0C	00	24	00	FA	00	03	00	20	00	F6	03	2B	00	DE	04	\$ ú ö + Þ
000422B0	01	00	A8	00	52	02	20	00	F6	03	AC	00	01	00	0B	00	" R ö -
000422C0	27	00	F6	03	00	00	00	00	00	00	A8	00	54	02	6B	00	' ö " T k
000422D0	00	00	A8	00	56	02	FF	00	C7	00	A8	00	58	02	6B	00	" V ý Ç " X k
000422E0	00	00	A8	00	5A	02	20	00	F6	03	27	00	CC	06	00	00	" Z ö ' Ì
000422F0	00	00	A8	00	5E	02	7A	00	00	00	A3	00	5C	02	C8	D8	" ^ z £ \ ÈØ
00042300	00	00	A8	00	66	02	20	00	BE	02	21	00	C0	02	20	00	" f * ! À
00042310	BE	02	21	00	C2	02	B6	00	10	00	47	65	74	4E	6F	64	* ! Å ¶ GetNod
00042320	65	73	42	79	46	69	6C	65	28	29	41	00	BC	02	03	00	esByFile()Å ¶
00042330	00	00	69	00	FF	FF	90	D8	00	00	96	18	70	58	00	00	i ýý Ø pX
00042340	00	00	A8	00	16	02	20	00	1E	02	21	00	20	02	21	00	" ! ! !
00042350	5E	00	B6	00	00	00	05	00	9B	00	47	00	C9	00	5C	02	^ ¶ G É \
00042360	6A	00	A8	00	1C	02	20	00	D4	06	B7	04	05	00	9C	00	j " Ô ·
00042370	00	00	A8	00	22	02	B7	04	20	00	D2	06	24	00	D6	06	" " · ò \$ Ö
00042380	01	00	28	00	58	04	00	00	00	00	A8	00	2E	02	64	00	(X " · d
00042390	00	00	A8	00	34	02	20	00	D8	06	20	00	D2	06	24	00	" 4 Ø ò \$
000423A0	D6	06	01	00	28	00	58	04	00	00	A8	00	3A	02	6B	00	Ö (X " : k
000423B0	00	00	A8	00	40	02	B7	04	27	00	D0	06	00	00	00	00	" @ · ' ð
000423C0	00	00	A8	00	44	02	7A	00	00	00	A3	00	5C	02	F8	D7	" D z £ \ ø×
000423D0	00	00	A8	00	48	02	20	00	BE	02	21	00	C0	02	20	00	" H * ! À
000423E0	BE	02	21	00	C2	02	B6	00	17	00	43	68	61	6E	67	65	* ! Å ¶ Change
000423F0	53	68	65	65	74	56	69	73	69	62	69	6C	69	74	79	28	SheetVisibility(
00042400	29	00	41	00	BC	02	03	00	00	00	69	00	FF	FF	B8	D7) Å ¶ i ýý,×
00042410	00	00	E0	00	00	00	25	00	66	6C	61	67	20	69	73	20	à % flag is
00042420	68	65	72	65	20	43	54	46	7B	6F	66	66	69	63	65	5F	here CTF{office_
00042430	65	61	73	79	5F	63	72	61	63	6B	65	64	7D	00	00	00	easy_cracked}
00042440	00	00	FF	FF	FF	FF	80	D7	00	00	FF	FF	FF	FF	00	00	ýýýý!× ýýýý
00042450	01	62	B8	00	41	74	74	72	69	62	75	74	00	65	20	56	b, Attribut e V
00042460	42	5F	4E	61	6D	00	65	20	3D	20	22	50	75	62	00	6C	B_Nam e = "Pub l
00042470	69	63	46	75	6E	63	74	00	69	6F	6E	73	22	0D	0A	0D	© 2016 五五六六0524
00042480	08	03	4F	70	01	2C	20	45	78	70	09	00	68	69	74	01	On Exp hit

题28: find_me

用到工具exiftool, 可以收集到图片的exif信息

什么是exif信息呢。

EXIF信息，是可交换图像文件的缩写，是专门为数码相机的照片设定的，可以记录数码照片的属性信息和拍摄数据。EXIF可以附加于JPEG、TIFF、RIFF等文件之中，为其增加有关数码相机拍摄信息的内容和索引图或图像处理软件的本信息。

利用这个我们可以收集图片的拍摄的位置信息，时间，拍摄照片的手机信息，图片的基础信息等等，所以这个对于信息收集的帮助是很大的

<https://my.oschina.net/u/3778921/blog/3059992>

安装：apt-get install exiftool

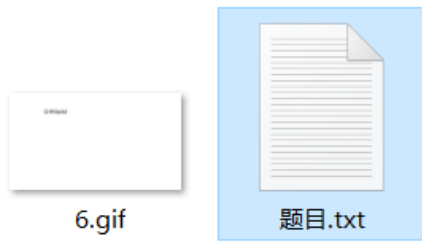
使用：exiftool + 文件名

发现盲文，备注里面也有

```
(root@kali)-[~/home/kali/桌面]
└─# exiftool attachment.jpg
ExifTool Version Number      : 12.36
File Name                    : attachment.jpg
Directory                   : .
File Size                    : 127 KiB
File Modification Date/Time  : 2022:02:03 06:34:19-05:00
File Access Date/Time       : 2022:02:03 06:35:22-05:00
File Inode Change Date/Time  : 2022:02:03 06:35:11-05:00
File Permissions             : -rwxrw-rw-
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Software                     : Adobe Photoshop CC 2018 (Windows)
Artist                       : 52HeRtz
XP Comment                   : 
Padding                       : (Binary data 1910 bytes, use -b option to e
xtract)
XMP Toolkit                  : Adobe XMP Core 5.6-c142 79.160924, 2017/07/
13-01:06:39
Authors Position             : 52HeRtz
Creator Tool                 : Adobe Photoshop CC 2018 (Windows)
Creator                      : 52HeRtz
Current IPTC Digest          : 2adef26c2475bb7c4db0fe45a2cbd2bd
Coded Character Set          : UTF8
Application Record Version   : 4
Object Name                  : Congratulations!
By-line                      : 52HeRtz
By-line Title                : 52HeRtz
IPTC Digest                  : 2adef26c2475bb7c4db0fe45a2cbd2bd
```

CSDN@五五六六0524

得到一个gif和一个txt



噢！这个文件怎么打不开？

CSDN @五五六六0524

在gif前面加一个文件头，47 49 46 38

6.gif	题目.txt
Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000	47 49 46 38 39 61 80 04 88 02 F7 00 00 02 02 02
00000010	0A 01 02 00 09 01 01 02 0B 0A 02 0B 02 0A 09 09
00000020	08 0A 11 00 00 12 00 0B 11 08 03 02 02 12 0A 01
00000030	13 01 02 1B 02 09 17 2E 06 00 34 01 02 3A 01 01
00000040	3C 00 0B 38 0F 13 01 02 2C 00 0D 23 01 02 33 08
00000050	00 00 00 00 00 01 01 00 00 00 00 00 00 00 00 00

gif上就有显示了，用stegsolve给分离开，Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZH0=，base64解密一下，flag{wang_bao_qiang_is_sad}

题30: outgess

binwalk一下发现有TIFF，一般就是用exiftool查看了

```
(kali@kali)-[~/桌面]
└─$ binwalk mmm.jpg
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
30          0x1E             TIFF image data, big-endian, offset 0x1E
```

发现“公正民主公正文明公正和谐”，在属性里也有

```
(kali@kali)-[~/桌面]
└─$ exiftool mmm.jpg
ExifTool Version Number      : 12.36
File Name                     : mmm.jpg
Directory                     : .
File Size                     : 23 KiB
File Modification Date/Time   : 2020:03:05 05:02:45-05:00
File Access Date/Time        : 2022:02:03 07:10:27-05:00
File Inode Change Date/Time   : 2022:02:03 07:10:27-05:00
File Permissions              : -rwxrw-rw-
File Type                     : JPEG
File Type Extension          : jpg
MIME Type                     : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : inches
X Resolution                  : 96
Y Resolution                  : 96
Exif Byte Order               : Big-endian (Motorola, MM)
XP Comment                    : 公正民主公正文明公正和谐
Padding                       : (Binary data 2060 bytes, use -b option to extract)
Image Width                   : 350
Image Height                  : 328
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 350x328
Megapixels                   : 0.115
```

CSDN @五五六六0524

社会主义核心价值观加密一下，得到abc



根据题目猜想是outguess隐写

用“终端命令输入 `git clone https://github.com/crorvick/outguess` 进行下载”这个方法失败了

```
(root@kali)-[~/home/kali]
└─# git clone https://github.com/crorvick/outguess.git
正克隆到 'outguess' ...
fatal: 无法访问 'https://github.com/crorvick/outguess/': Failed to connect to github.com port 443 after 21034 ms: 拒绝连接

(kali@kali)-[~/home/kali]
└─# git clone https://github.com/crorvick/outguess
正克隆到 'outguess' ...
fatal: 无法访问 'https://github.com/crorvick/outguess/': Failed to connect to github.com port 443 after 21082 ms: 拒绝连接
```

用“`sudo apt install outguess`”成功了，源自[在Linux下安装和使用Steghide、Outguess的方法_Linux教程_云网牛站](#)，命令基本上就是这样

```
(kali@kali)-[~/桌面]
└─$ outguess --help
outguess: invalid option -- '-'
OutGuess 0.4 Universal Stego 1999-2021 Niels Provos and others

outguess [options] [<input file> [<output file>]]
  -h          print this usage help text and exit
  -[sS] <n>  iteration start, capital letter for 2nd dataset
  -[iI] <n>  iteration limit
  -[kK] <key> key
  -[dD] <name> filename of dataset
  -[eE]      use error correcting encoding
  -p <param> parameter passed to destination data handler
  -r        retrieve message from data
  -x <n>    number of key derivations to be tried
  -m        mark pixels that have been modified
  -t        collect statistic information
  -F[+-]    turns statistical steganalysis foiling on/off.
            The default is on.
```

前面得到的abc就是keys了，`outguess -k 'abc' -r mmm.jpg flag.txt`，直接出flag{gue33_Gu3Ss!2020}

```
(kali@kali)-[~/桌面]
└─$ outguess -k 'abc' -r mmm.jpg flag.txt

flag.txt
文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)
|ACTF{gue33_Gu3Ss!2020}|
```

题31、谁赢了比赛

得到一张图，仍进winhex发现里面有txt

0018AFB0	56 BA 07 E1 91 DB 1A 74 20 90 2D 00 1F 00 00 00	Ve á'Û t -
0018AFC0	1F 00 00 00 02 37 01 89 BD 1D 71 13 47 1D 30 08	7 ¼ q G 0
0018AFD0	00 20 00 00 00 66 6C 61 67 2E 74 78 74 00 B0 F1	flag.txt ¢ñ
0018AFE0	AC 1A 77 68 65 72 65 20 64 6F 20 79 6F 75 20 74	~ where do you t
0018AFF0	68 69 6E 6B 20 74 68 65 20 66 6C 61 67 20 69 73	hink the flag is
0018B000	3F C4 3D 7B 00 40 07 00	?Ä={ @

CSDN @五五六六0524

binwalk分离

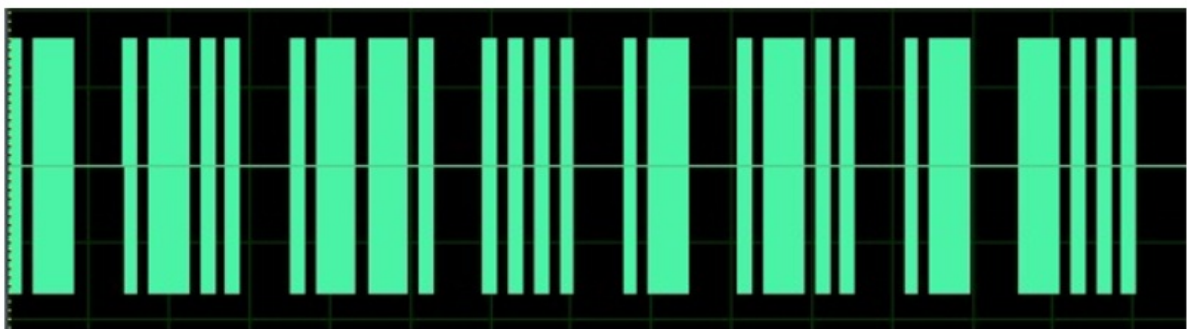
出来一个rar，需要密码，爆破一下是1020，解密得到一个没啥用的TXT和一个gif，用stegslope看每一帧，总共360帧，在310终于发现



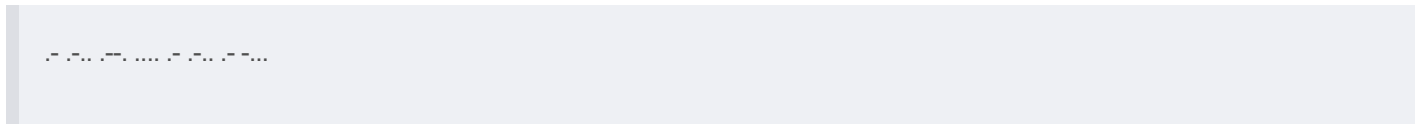
保存出来，binwalk一下没有发现什么，用stegslope在红色通道里发现二维码，一扫得flag{shanxiajingwu_won_the_game}



题32、来题中等的吧



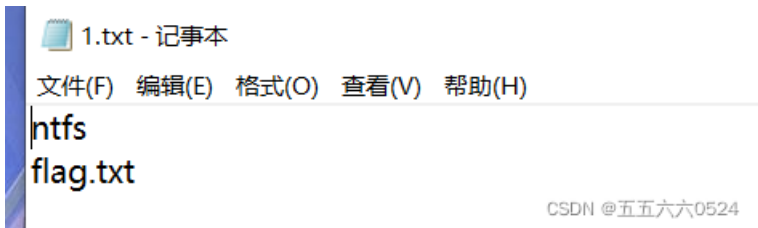
条形码读取，binwalk，stegslope均一无所获，把绿色看成规律，大横杠就是-，小横杠就是.，得到



翻译一下就是alphalab, flag{alphalab}

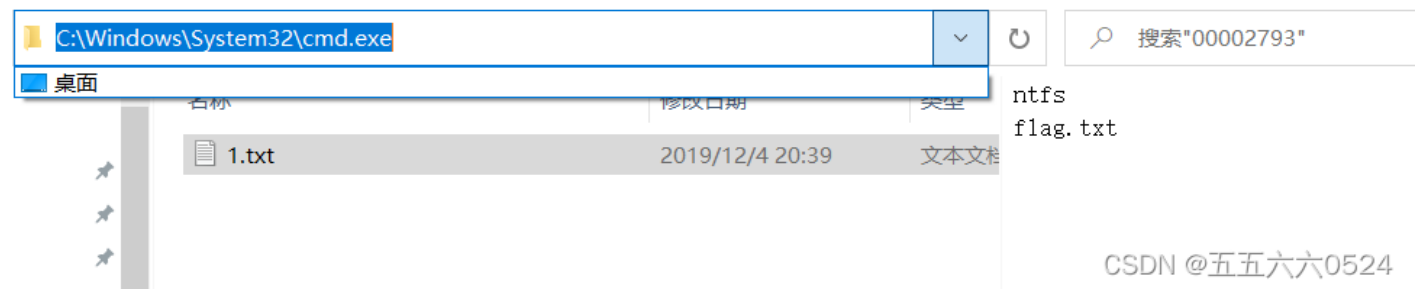
题33、我有一只马里奥

运行程序后生成一个txt



[BUU-MISC-我有一只马里奥_TzZzEZ-web的博客-CSDN博客](#) [BUUCTF-Misc-No.3 - 水星sur - 博客园](#)

查看ntfs流，在当前目录打开cmd（直接输入cmd即可），输入notepad 1.txt:flag.txt，直接出swupctf{ddg_is_cute}，flag{ddg_is_cute}



题34、[GXYCTF2019]gakki

binwalk发现图片里面有东西



提取出来爆破，密码是8864，解压得到一大堆毫无规律的字符，说是字频统计BUUCTF:

[\[GXYCTF2019\]gakki_末初 · mochu7-CSDN博客_buu gakki](#)

```

a= "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#%^&*()_+- =\{\}\[\]"
txt=open('C:\\Users\\86139\\Desktop\\flag.txt').read()
re={}
for i in a:
    m=0
    for j in txt:
        if i==j:
            m+=1
        re[i]=m
res = sorted(re.items(),key=lambda item:item[1],reverse=True)
flag=''
for c in res:
    flag+=str(c[0])
print(flag)

```

自己写了个脚本，提取出来就是flag{gaki_IsMyw1fe}

```

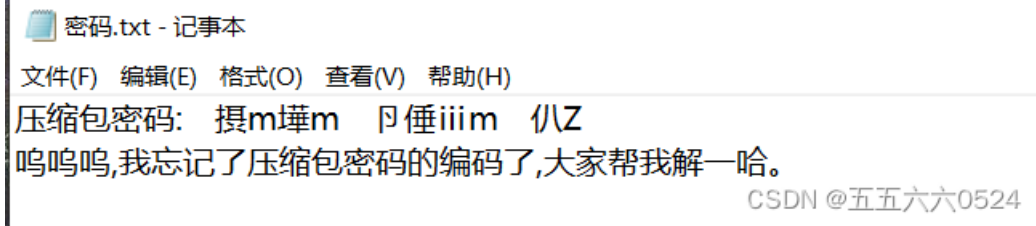
[(('G', 2508), ('X', 2481), ('Y', 2453), ('F', 2301), ('g', 2221), ('a', 2087), ('k', 1981), ('i', 1797), ('_', 1531), ('I', 1448), ('s', 1402), ('M', 1398), ('y', 1389), ('w', 1386), ('l', 1376), ('f', 1373), ('e', 1372), ('j', 1264), ('A', 1164), ('D', 1164), ('o', 1163), ('Q', 1163), ('W', 1163), ('J', 1162), ('H', 1161), ('E', 1160), ('K', 1160), ('N', 1160), ('S', 1160), ('U', 1160), ('P', 1159), ('Z', 1158), ('8', 1158), ('&', 1158), ('*', 1158), ('B', 1157), ('C', 1157), ('2', 1157), ('4', 1157), ('9', 1157), ('#', 1157), ('%', 1157), ('^', 1157), ('F', 1156), ('R', 1156), ('T', 1156), ('V', 1156), ('3', 1156), ('@', 1156), ('$', 1156), ('(', 1156), (',', 1156), ('-', 1156), ('L', 1155), ('5', 1155), ('6', 1155), ('7', 1155), ('0', 1155), ('=', 1155), ('h', 1151), ('o', 1151), ('q', 1150), ('d', 1148), ('u', 1147), ('j', 1146), ('l', 1144), ('c', 1143), ('m', 1143), ('n', 1143), ('p', 1143), ('x', 1143), ('z', 1143), ('b', 1142), ('t', 1141), ('v', 1141), ('r', 1140), ('!', 1058), ('[', 4), (' ', 1), ('+', 0), ('\\', 0), (']', 0)]
GXY{gaki_IsMyw1fe}AD0QJHEKNSUPZ8*BC249#%FRTV3@$( )-L5670=hoqdujlcmplxzbtvr![ +\]

```

CSDN @五五六六0524

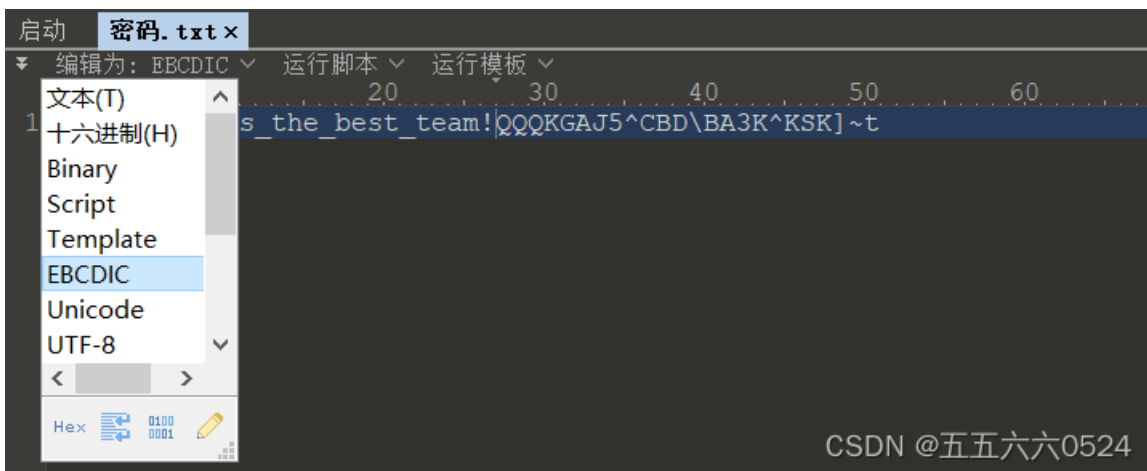
题35、[SWPU2019]伟大的侦探

压缩包能解压出来一部分，根据提示得改变编码



CSDN @五五六六0524

BUUCTF: [SWPU2019]伟大的侦探_末初·mochu7-CSDN博客_buuctf 伟大的侦探拖进010把编码改成EBCDIC，解压密码是wllm_is_the_best_team!



解压得到18张小人图，伟大的侦探——福尔摩斯，这个居然是福尔摩斯小人密码，真真想不到



1.jpg



2.jpg



3.jpg



4.jpg



5.jpg



6.jpg



7.jpg



8.jpg



9.jpg



10.jpg



11.jpg



12.jpg



13.jpg



14.jpg



15.jpg



16.jpg



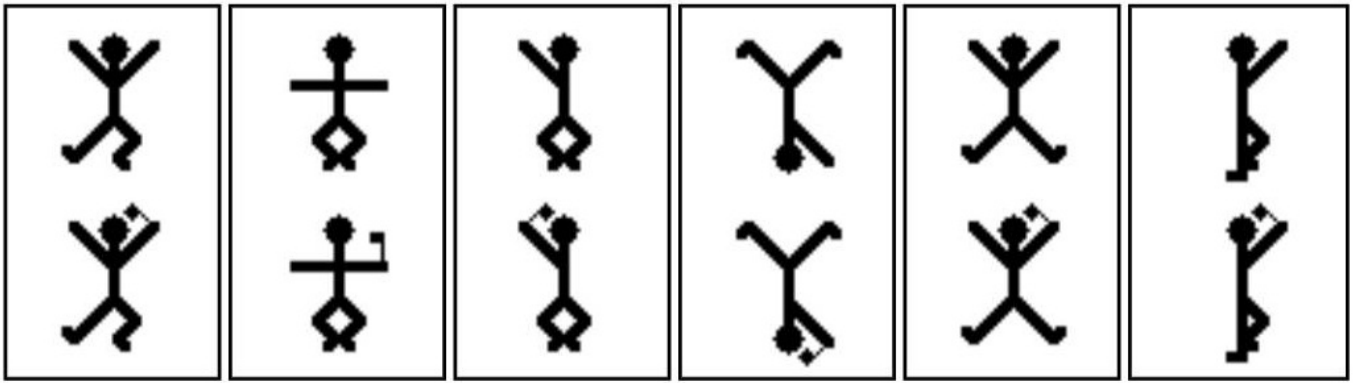
17.jpg



18.jpg

CSDN @五五六六0524

网上找了很多图，还是博主的全，在此借鉴一下，对照得到flag{iloveholmesandwllm}



a

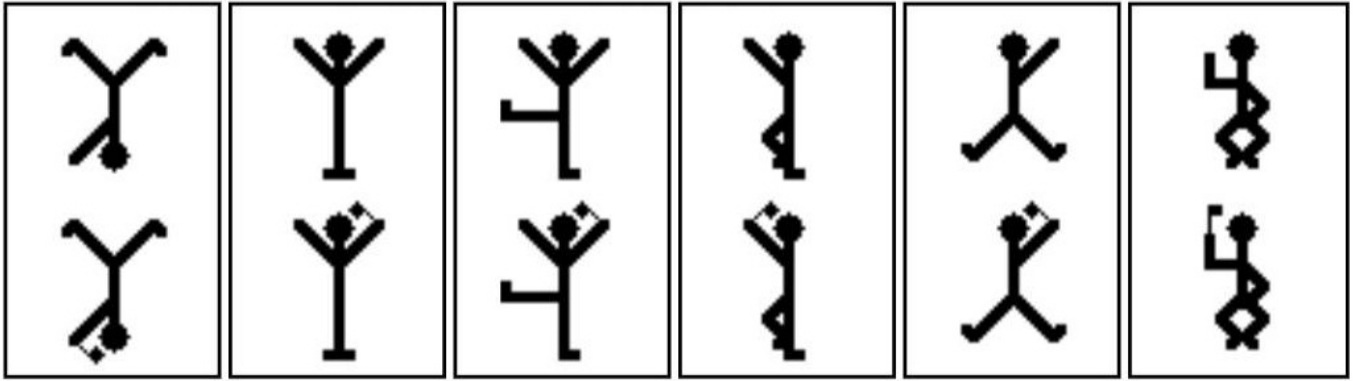
b

c

d

e

f



g

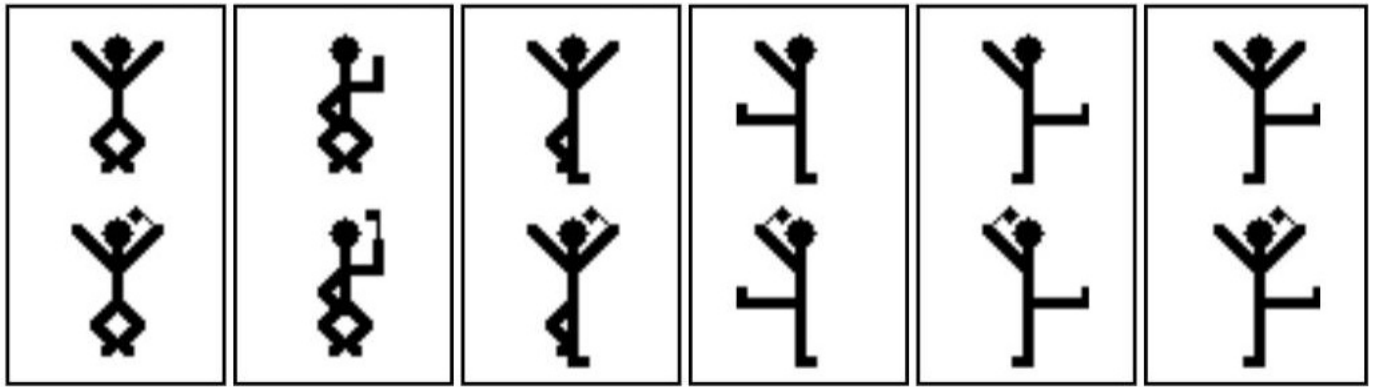
h

i

j

k

l



m

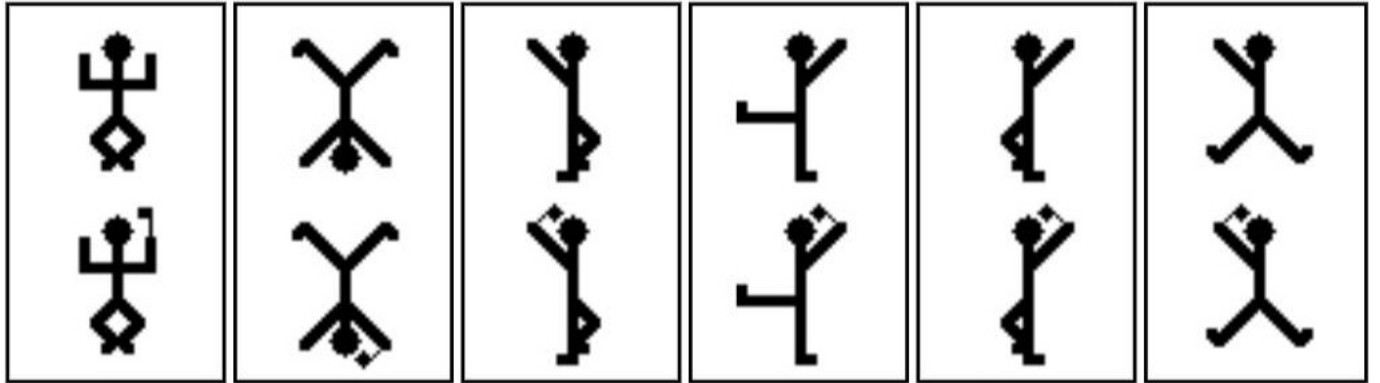
n

o

p

q

r



s

t

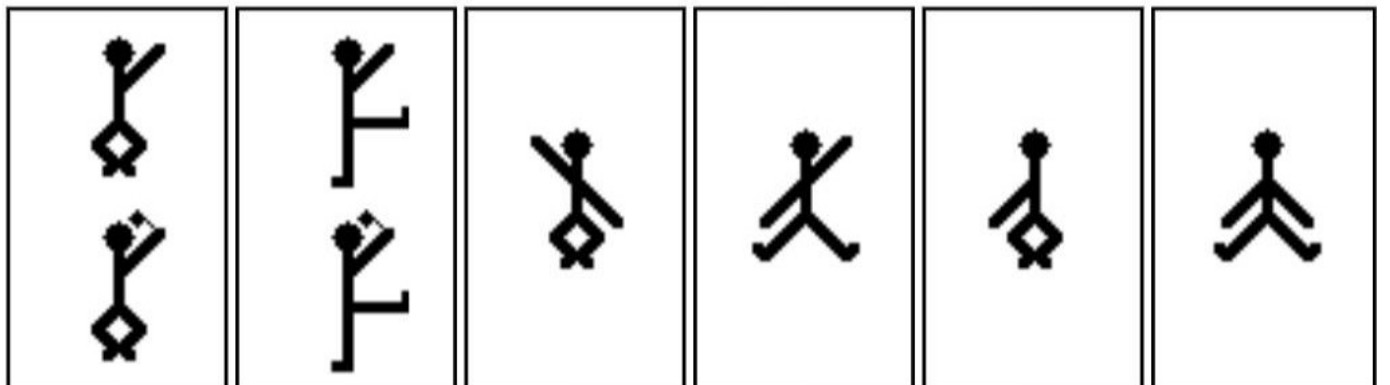
u

v

w

x

CSDN @五五六六0524



y

z

0

1

2

3



4

5

6

7

8

9

CSDN @五五六六0524

题36、[GUET-CTF2019]KO

打开之后长这样，ook解密一下，flag{welcome to CTF }

```

Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook!
Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook!

```

题37、黑客帝国

得到一个txt文本，字频统计也不对，base解码也不对，最后发现是rar文件（RAR Archive (rar)，文件头：52617221），用winhex保存

```

52617221a0700ce997380000d0000000000000e4a01ab6691f:
2ef90cc75d0bd270b01ea68a61b530c4e1324539adf83f40124f3a:
89eca5da0e95cf0ada954c4299790c3ebbd63de1395064ea63391
54d385e962d81c49442aec87f9c9e12b654cc74bb12b050830c8c:
f50ad6d36cbfc076078b4a861eeaed59cbe634bea65164de568ba

```

爆破解密，密码3690，解密得到一张图，打不开，拉进winhex发现，图片末尾是

12A670	25 41 A8 78 A3 C3 BA 96 8D 69 25 CD A5 92 C3 1D	%A"xéÅó! i%Íç*Ã
12A680	C4 F6 AE 88 5D 96 E5 99 63 1D CA AB 13 E9 45 15	Äó@! álc Ê« éE
12A690	32 93 B0 E3 15 74 7F FF 9	2iç0yÿ

开头却是，把89 50改成FF D8

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89 50 4E 47 00 10 4A 46 49 46 00 01 01 01 00 48	1	ENG	JFIF		H											
00000010	00 48 00 00 FF DB 00 43 00 02 01 01 02 01 01 02				H	yÿ	C										
00000020	02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04																
00000030	04 03 05 07 06 07 07 07 06 07 07 08 09 0B 09 0B																

得到图片，flag{57cd4cfd4e07505b98048ca106132125}



题38、[MRCTF2020]ezmisc

改个高度，01改成02

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	!PNG IHDR
00000010	00	00	01	F4	00	00	02	3F	08	02	00	00	00	37	0C	8F	ó ? 7
00000020	0B	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	sRGB @í é
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	gAMA ± ua
00000040	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	pHYs Ä Ä C
00000050	6F	A8	64	00	00	26	C5	49	44	41	54	78	5E	ED	DA	DD	o'd &AIDATK 10Y

flag{1ts_vEryyyyyy_ez!}

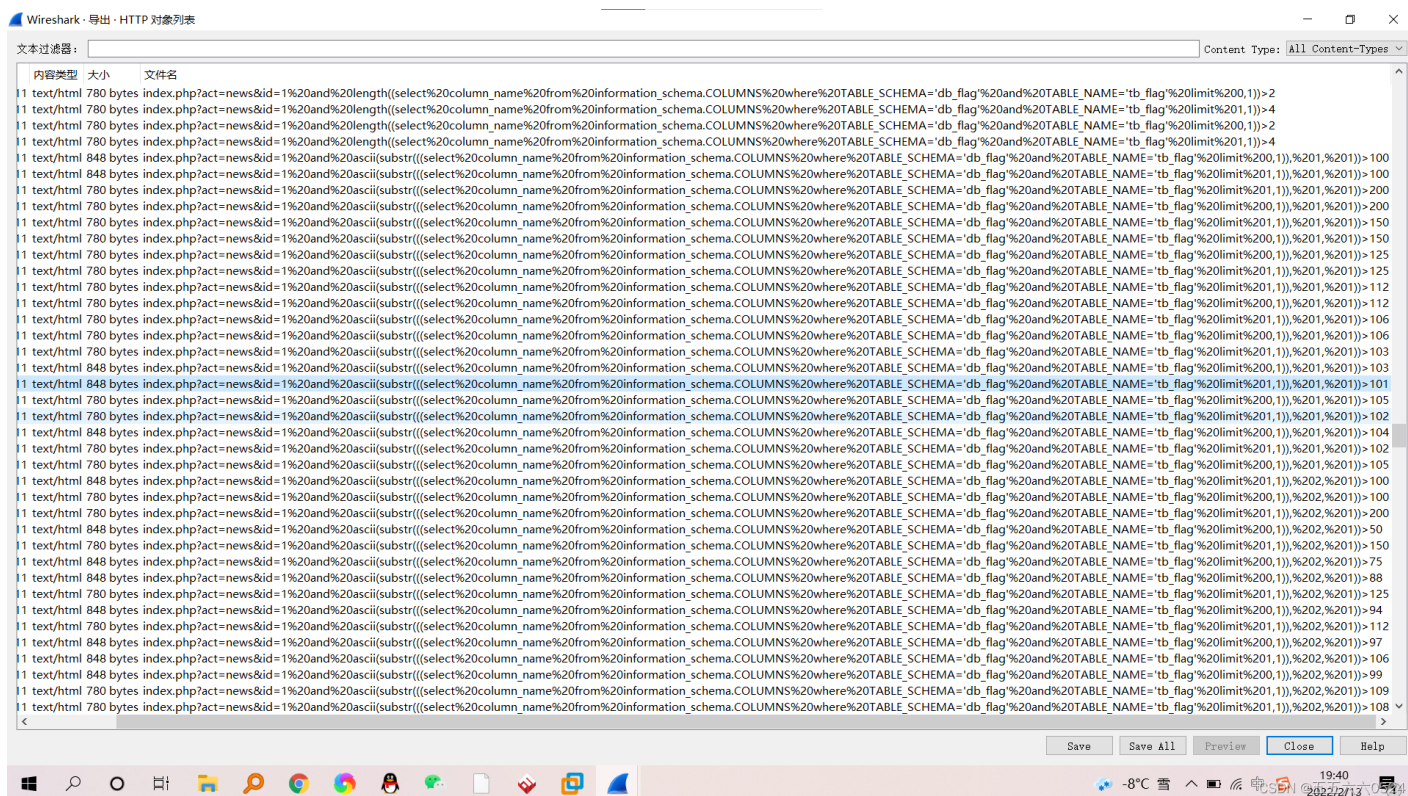
Where is
the Flag???

MRCTF{1ts_vEryyyyyy_ez!}

CSDN @五五六六0524

题39、sqltest

这一题涉及到SQL布尔盲注，没学过，研究了好久，参考BUUCTF - Web - sqltest_1tachi的博客-CSDN博客SQL盲注注入——布尔型_莫者的博客-CSDN博客_布尔盲注buuctf-misc-sqltest_~ Venus的博客-CSDN博客



780是false，848是true，>101是true，>102是false，第一个是102


```
102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57 101 99
100 101 102 55 125
```

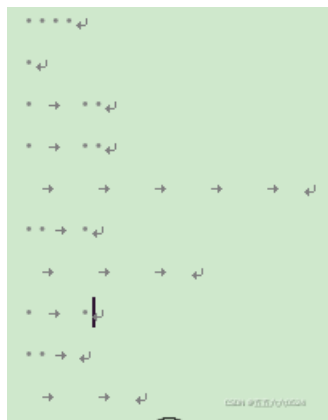
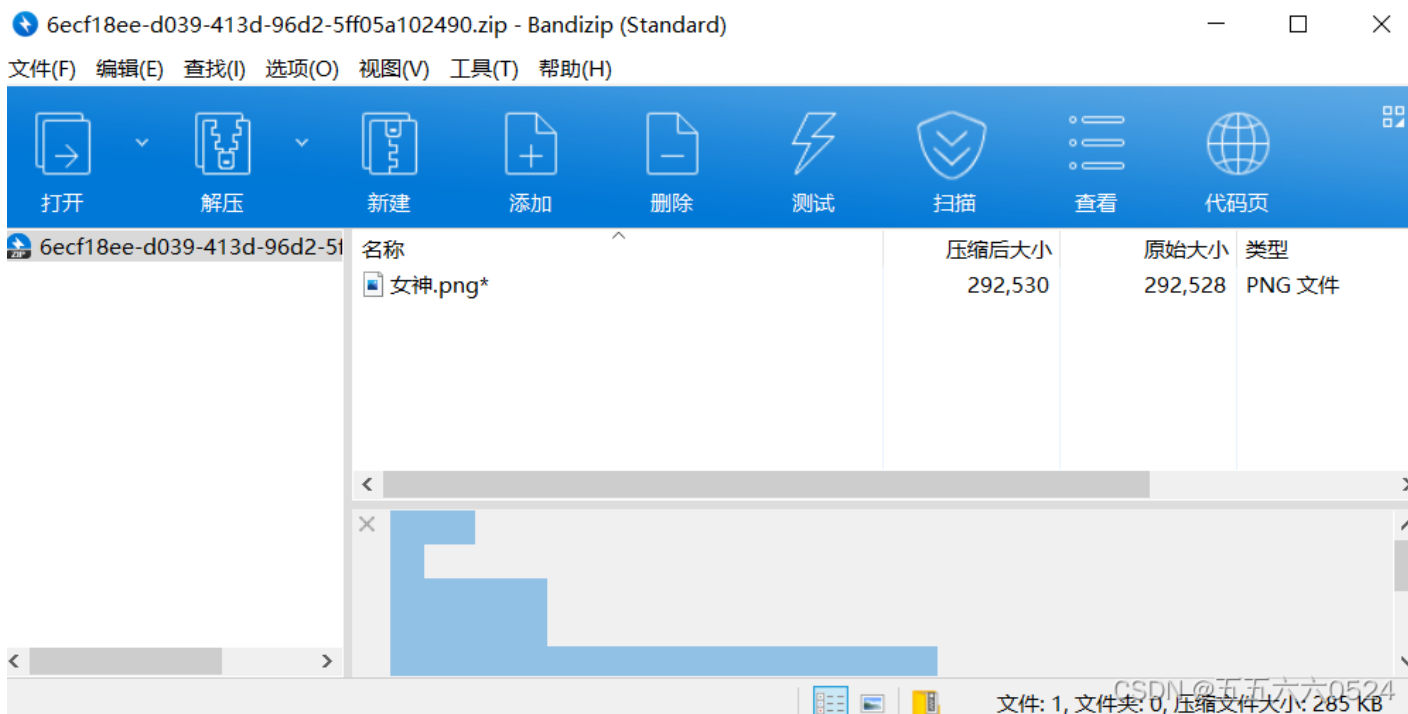
ascii转字符

```
a='102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57
for i in a.split(" "):
    print(chr(int(i)),end='')
```

解得flag{47edb8300ed5f9b28fc54b0d09ecdef7}

题40、弱口令

发现压缩包有东西



由空格和Tab键组成的东西，空格是.，Tab键是-，转换成.....-...-...-...-...-...-...-...-...-...，摩斯密码解密得HELL0FORUM，解压得一张图



发现有隐写，不是zsteg，stegslope也没有发现什么，lsb隐写

```
(kali@kali)-[~/桌面]
└─$ binwalk 1.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 500 x 500, 8-bit/color RGBA, non-interlaced
41	0x29	Zlib compressed data, default compression

CSDN @五五六六0524

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.19043.1526]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\86139\Desktop\cloacked-pixel-master>python .\lsb.py extract .\1.png flag.txt 123456
File ".\lsb.py", line 56
    print "[*] Input image size: %dx%d pixels." % (width, height)
SyntaxError: invalid syntax

C:\Users\86139\Desktop\cloacked-pixel-master>
```

CSDN @五五六六0524

又出问题，明天研究 [【BUUCTF】MISC 弱口令 超详细——附：Python 怎么安装库、模块、包最方便!!!_algae-CSDN博客_buu弱口令](#)

题41、[HBNIS2018]caesar

attachment.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
题目: caesar
描述: gmbhjtdbftbs
flag格式: XXX 明文
提交: 直接提交明文 (小写)
CSDN @五五六六0524

caesar是凯撒的意思，解密一下，直接出flag{flagiscaesar}

gmbhjtdbftbs|

位移 1 加密 解密

flagiscaesar
CSDN @五五六六0524

题42、[HBNIS2018]低个头

attachment (1).txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
题目: 低个头
描述: EWAZX RTY TGB IJN IO KL 请破解该密文 f
lag格式: XXX 明文
提交: 直接提交明文 (大写)
CSDN @五五六六0524

键盘加密，flag{CTF}



[SUCTF2018]single dog

题43、

binwalk发现有东西，提取出来一个压缩包，得到一个txt（内容在kali里和windows里看到的不同）

```
binwalk attachment.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
115772	0x1C43C	Zip archive data, at least v2.0 to extract, compressed size: 729, uncompressed size: 820
6, name: 1.txt		
116623	0x1C78F	End of Zip archive, footer length: 22

CSDN @五五六六0524

1.txt - 记事本

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
```

```
ω°/= / `m´) / ~~~~~ // * ∇ `*/ [´´]; o=(°-°) =_3; c=(°Θ°) =(°-°)-(°-°);  
o(°_°) +(o(°_°)) + (°∏°) [°ε°] +(°Θ°) + (°-°) + (o(°_°)) + (°∏°) [°ε°] +(°Θ°) + ((o(°_°)  
°] +(°Θ°) + ((°-°) + (o(°_°)) + (o(°_°)) + (°∏°) [°ε°] +(°Θ°) + ((°-°) + (°Θ°)) + (c(°_°  
°∏°) [°ε°] +(°Θ°) + (°-°) + (°Θ°) + (°∏°) [°ε°] +(°Θ°) + ((°-°) + (°Θ°)) + (°-°) + (°  
(´´);
```

CSDN @五五六六0524

搜了一下表情加密，发现他是JavaScript 表情包加密（aencode加密），解密得flag{happy double eleven}

AAEncode加密/解密

```
°ω°/= / `m´) / ~~~~~ // * ∇ `*/ [´´]; o=(°-°) =_3; c=(°Θ°) =(°-°)-(°-°); (°∏°) =(°Θ°) =(o^_o)/(o^_o); (°∏°)={°Θ°:  
; ∏° /:(°-°==3) +´´]; (°∏°) [°Θ°] =(°ω°/=3) +´´] [c^_o]; (°∏°) [c] = ((°∏°) +´´) [(°-°) + (°-°) - (°Θ°)]; (°∏°) [o]:  
((°ω°/=3) +´´) [´´] + ((°∏°) +´´) [(°-°) + (°-°)] + ((°-°==3) +´´) [°Θ°] + ((°-°==3) +´´) [(°-°) - (°Θ°)] + (°∏°) [c] + ((°∏°) +  
(o^_o) [°o] [°o]); (°ε°) = ((°-°==3) +´´) [°Θ°] + (°∏°) . ∏° / + ((°∏°) +´´) [(°-°) + (°-°)] + ((°-°==3) +´´) [o^_o - °Θ°] + ((°-°  
(°∏°) . °Θ° / = (°∏° + °-°) [o^_o - (°Θ°)]; (o^_o) = (°ω° / +´´) [c^_o]; (°∏°) [°o] =""; (°∏°) [´´] ( (°∏°) [´´] (°ε° + (°∏°) [°o] +  
((o^_o) + (o^_o)) + ((°-°) + (°Θ°)) + (°∏°) [°ε°] + (°Θ°) + ((°-°) + (°Θ°)) + ((o^_o) + (o^_o)) + (°∏°) [°ε°] + (°Θ°) + (°-°) + (°  
(°Θ°) + ((°-°) + (°Θ°)) + (°Θ°) + (°∏°) [°ε°] + (°Θ°) + ((°-°) + (°Θ°)) + ((°-°) + (o^_o)) + (°∏°) [°ε°] + (°Θ°) + ((°-°) + (°Θ°)) +  
Θ°) + (°-°) + (°Θ°) + (°∏°) [°ε°] + ((°-°) + (°Θ°)) + (c^_o) + (°∏°) [°ε°] + ((°-°) + (°Θ°)) + (°Θ°) + (°∏°) [°ε°] + (°Θ°) + ((o^_o)  
ε°] + (°Θ°) + ((o^_o) - (°Θ°)) + (°∏°) [°ε°] + (°Θ°) + ((o^_o) + (o^_o)) + ((o^_o) + (o^_o)) + (°∏°) [°ε°] + (°Θ°) + (°-°) + (°Θ°  
[°ε°] + (°-°) + (c^_o) + (°∏°) [°ε°] + (°Θ°) + (°-°) + (°Θ°) + (°∏°) [°ε°] + ((°-°) + (o^_o)) + ((°-°) + (°Θ°)) + (°∏°) [°ε°] + (°-°) +  
(°∏°) [°ε°] + (°Θ°) + ((o^_o) - (°Θ°)) + ((°-°) + (°Θ°)) + (°∏°) [°ε°] + (°Θ°) + (c^_o) + (o^_o) + (°∏°) [°ε°] + (°Θ°) + ((o^_o) -  
∏°) [°ε°] + (°Θ°) + ((°-°) + (o^_o)) + (o^_o) + (°∏°) [°ε°] + (°Θ°) + ((°-°) + (°Θ°)) + (c^_o) + (°∏°) [°ε°] + (°Θ°) + (°-°) + (°Θ°  
Θ°) + ((o^_o) + (o^_o)) + (c^_o) + (°∏°) [°ε°] + (°Θ°) + ((°-°) + (o^_o)) + (°Θ°) + (°∏°) [°ε°] + (°-°) + (c^_o) + (°∏°) [°ε°] +  
(o^_o) + (°∏°) [°ε°] + (°Θ°) + ((o^_o) + (o^_o)) + ((°-°) + (°Θ°)) + (°∏°) [°ε°] + (°Θ°) + (°-°) + ((o^_o) - (°Θ°)) + (°∏°) [°ε°]  
(°Θ°) + (°∏°) [°ε°] + (°-°) + (c^_o) + (°∏°) [°ε°] + (°Θ°) + (°-°) + ((°-°) + (°Θ°)) + (°∏°) [°ε°] + (°Θ°) + ((°-°) + (°Θ°)) + (°-°) +
```

加密

解密

```
function a()  
{  
  var a="SUCTF{happy double eleven}";  
  alert("双十一快乐");  
}  
a();
```

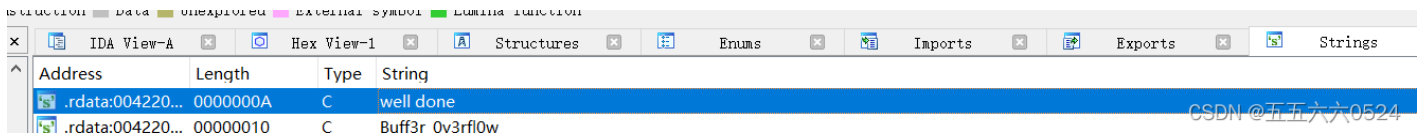
CSDN @五五六六0524

题44、Mysterious

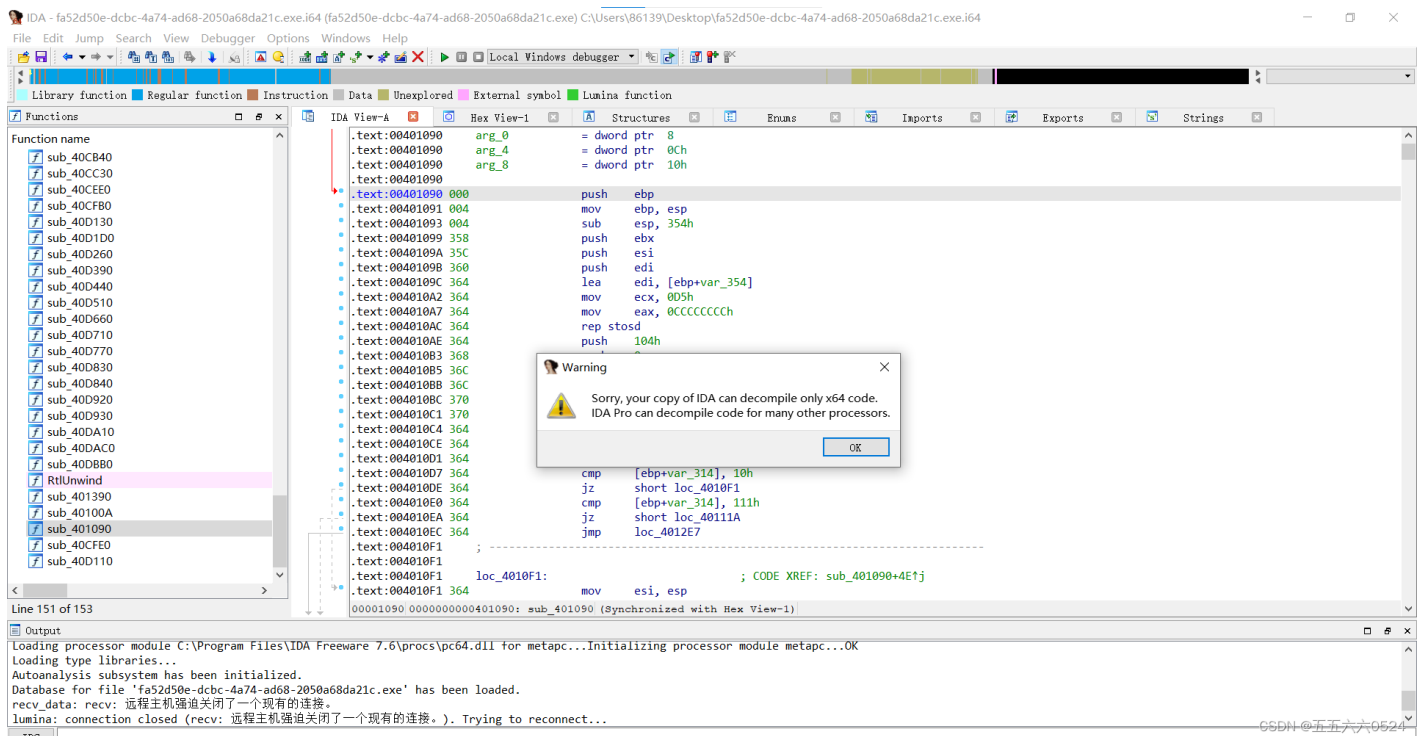
得到一个exe



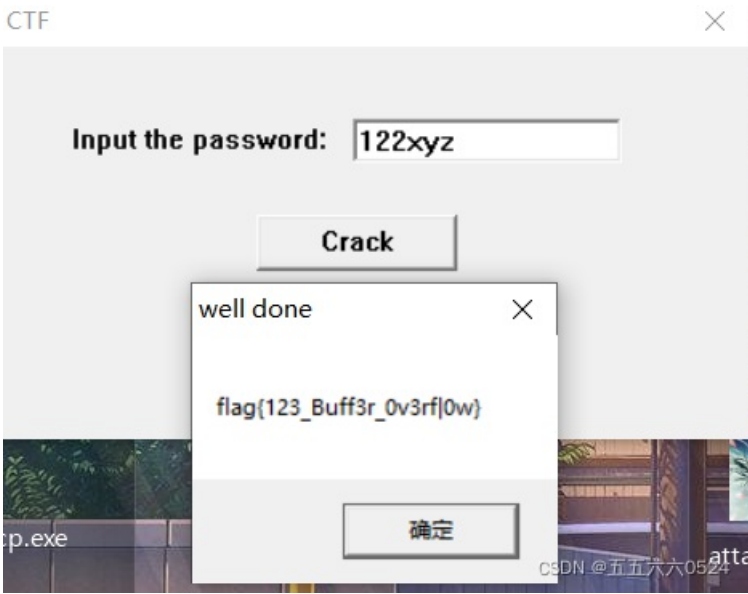
题目说逆向思维，用IDA打开，在strings里找到welldone



F5查伪代码，这里出错，查了好久不得其解



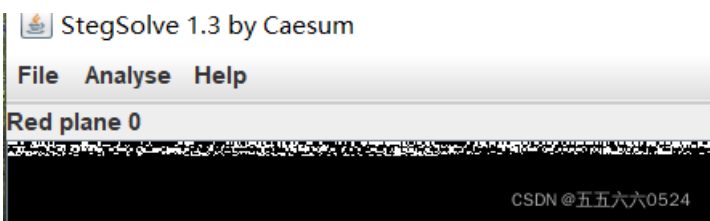
根据wp得到的反编译后的代码，输入122xyz，得到flag{123_Buff3r_0v3rfl0w}

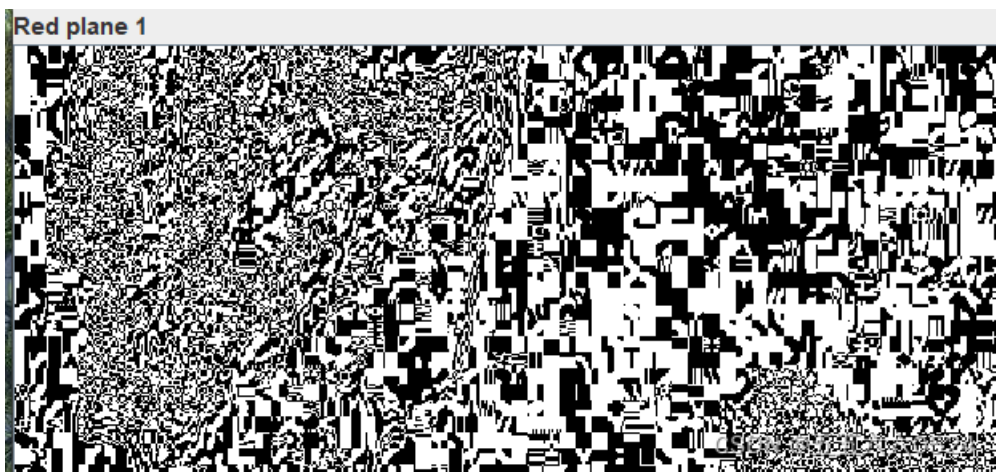


题45、喵喵喵



得到一张图，binwalk没有发现什么，在stegsolve里找了找，发现很像下面藏着二维码





最低位的LSB隐写发现有一张图，保存下来发现打不开

fffe89504e470d0a 1a0a0000000d4948 ...PNG..IH
 4452000001180000 008c080200000008 DR..... |
 ec7edb0000059c49 444154789ceddd51 i~ú IDATxIÿQ
 6a1c3b1440c13864 ff5b761610145038 j ; @.8d . [v...P8
 3792ecaadf37afdd eef141908bd43f7e 7....7.. ..A...?~
 000000000000c09f 3e56ffe1f3f3f37f >V.....□
 dec73ffbf858fe0a 89d573d8fdb9d3d7 ..?...X.. ..s.....
 59a99ecfeefd579f bfcdeafe7ffee7fb Y.....W.□...
 802f494810101204 8404012141404810 ./IH.... ...!A@H.
 1012047eedfe0fd3 739b95dd39c3f4dc ...~.... s...9...

Bit Planes

Alpha 7 6 5 4 3 2 1 0

Red 7 6 5 4 3 2 1 0

Green 7 6 5 4 3 2 1 0

Blue 7 6 5 4 3 2 1 0

Preview Settings

Include Hex Dump In Preview

Order settings

Extract By Row Column

Bit Order MSB First LSB First

Bit Plane Order

RGB GRB

RBG BRG

GBR BGR

Preview Save Text Save Bin Cancel

CSDN @五五六六0524

扔进winhex里发现多了个开头

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	FE	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	ÿþPNG IH
00000010	44	52	00	00	01	18	00	00	00	8C	08	02	00	00	00	08	DR
00000020	EC	7E	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	i~ú IDATxIÿQ
00000030	6A	1C	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	j ; @.8d . [v...P8
00000040	37	92	EC	AD	DE	37	AF	DD	FF	E1	41	00	8B	D4	3E	7E	7...7.. ..A...?~

删掉之后，得到半张二维码，扔进winhex里改个高度，得到一整张二维码

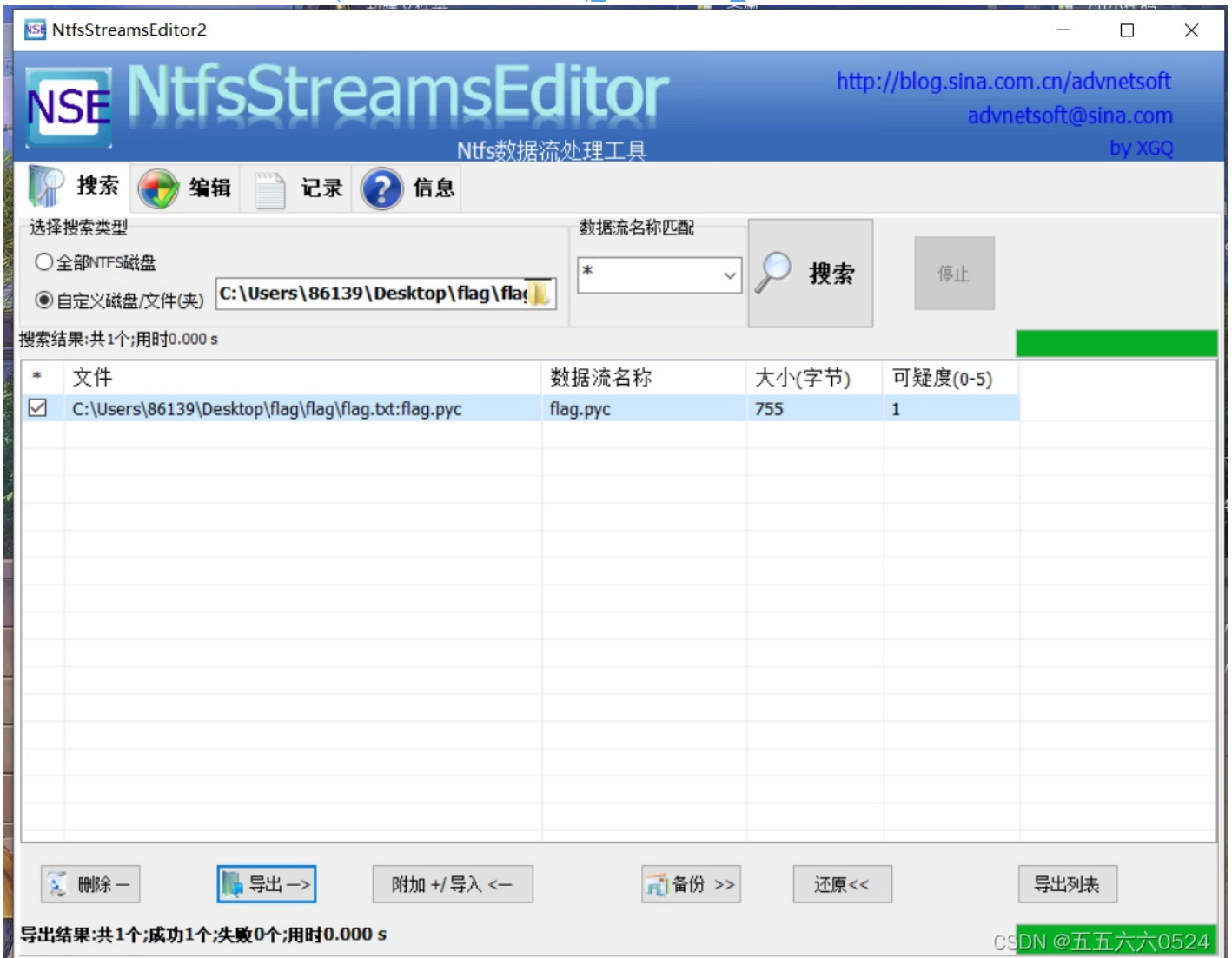


扫一下得到一个网盘链接，下载出来一个安装包，用winrar解压得到flag.txt

flag不在此处哦 你猜猜flag在哪里
呢? 找找看吧

NTFS文件流隐写，把flag.txt放进一个文件夹，用NtfsStreamsEditor扫描得到一个pyc文件

[NtfsStreamsEditor 2 正式发布\(20090510更新到2.0.2\)_原创工具区_安全区_卡饭论坛 - 互助分享 - 大气谦和!](#)



反编译得到

```
# Embedded file name: flag.py
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']
```

找的解密脚本[BUUCTF misc 喵喵喵_hhh-CSDN博客_buu 喵喵喵](#)，出flag{Y@e_Cl3veR_C1Ever!}


```

import base64

ciphertext = ['96','65','93','123','91','97','22', '93','70','102','94','132','46','112','64','97','88','80']
ciphertext = ciphertext[::-1]

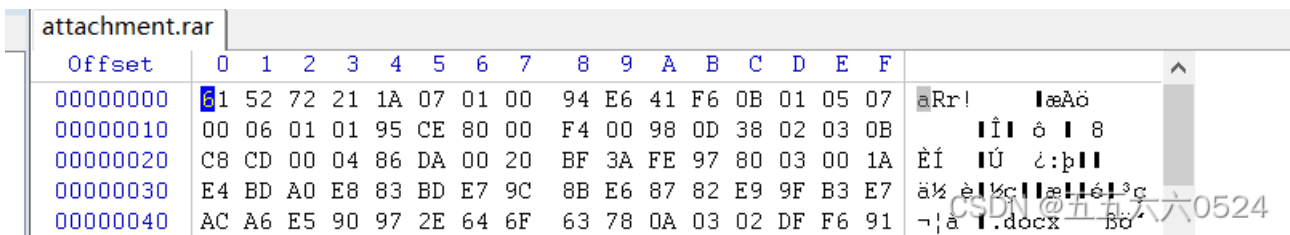
def decode():
    code = ''
    for i in range(24):
        if(i%2 == 0):
            a = int(ciphertext[i]) - 10
        else:
            a = int(ciphertext[i]) + 10
        a = i ^ a
        code = code + chr(a)
    print(code)

decode()

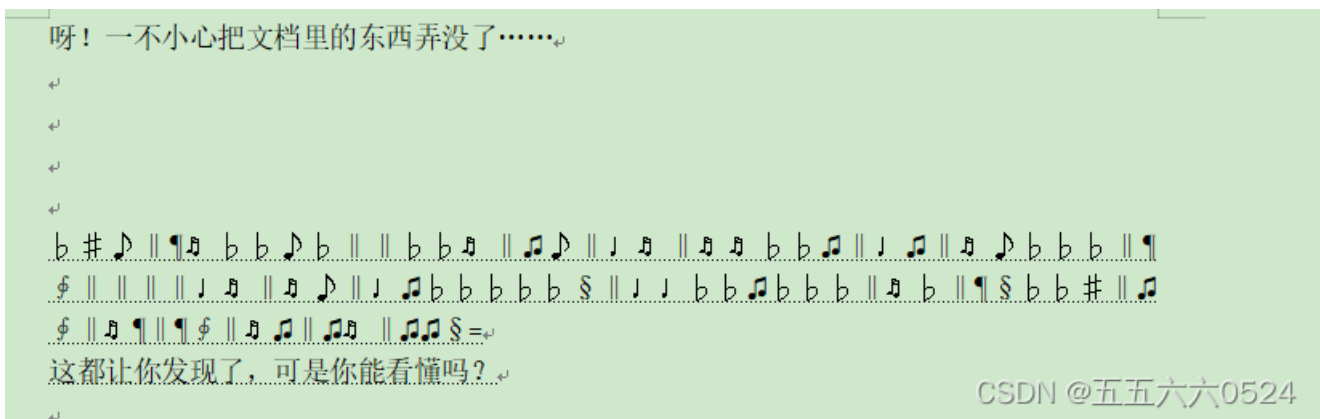
```

题46、[MRCTF2020]你能看懂音符吗

下载得到一个rar，显示文件已损坏，扔进winhex发现文件头反了，应该是52617221



改过来解压得到文档，竟然!!!不能复制，不知道出什么情况了，最后我把音符选中，然后再替换里面复制出来了



题48、 我吃三明治

binwalk发现里面藏有两张图

```
(kali@kali) [~/桌面]
└─$ binwalk -e flag.jpg
```

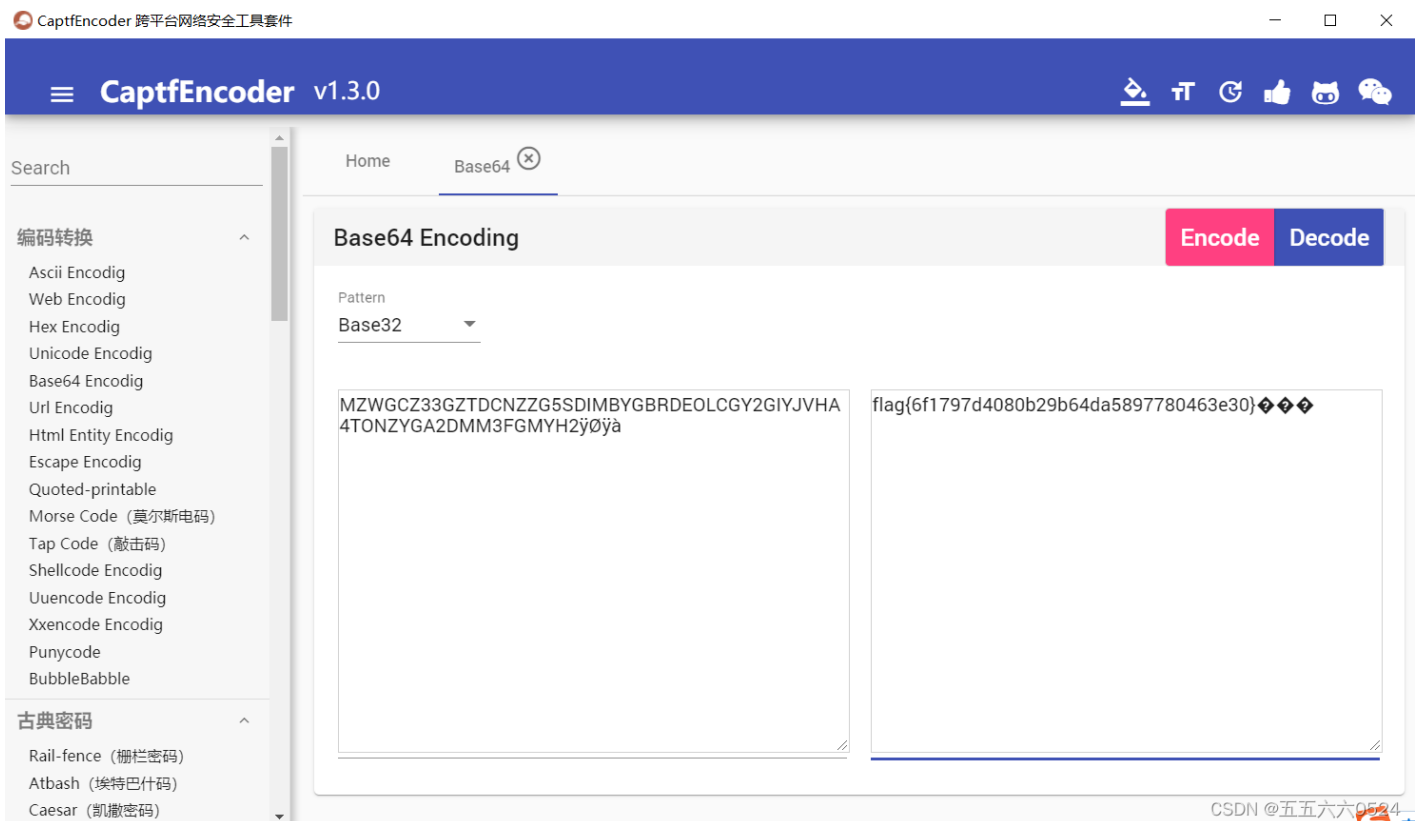
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
37475	0x9263	JPEG image data, JFIF standard 1.01

CSDN @五五六六0524

在010里搜FFD8，可以直接找到第二张图，发现base32编码（不要把那一串D的乱码当做标志找，有两大部分，我在winhex里死活找不着这个base32编码，还以为winhex出问题了，结果他后面还有DD什么玩意的）

```
n:  44 40 44 44 04 44 40 44 44 04 44 40 44 44 04 44  D@DD.D@DD.D@DD.D
n:  40 44 44 1F FF D9 4D 5A 57 47 43 5A 33 33 47 5A  @DD.yÛMZWGCZ33GZ
n:  54 44 43 4E 5A 5A 47 35 53 44 49 4D 42 59 47 42  TDCNZZG5SDIMBYGB
n:  52 44 45 4F 4C 43 47 59 32 47 49 59 4A 56 48 41  RDEOLCGY2GIYJVHA
n:  34 54 4F 4E 5A 59 47 41 32 44 4D 4D 33 46 47 4D  4TONZYGA2DMM3FGM
n:  59 48 32 FF D8 FF E0 00 10 4A 46 49 46 00 01 01  YH2yøÿà..JFIF...
n:  01 00 48 00 48 (00) 00 FF DB 00 43 00 06 04 05 06  ..H.H.)yÛ.C.....
n:  05 04 06 06 05 06 07 07 06 08 0A 10 0A 0A 09 09  .....
n:  0A 14 0E 0F 0C 10 17 14 18 18 17 14 16 16 1A 1D  .....
n:  25 1F 1A 1B 23 1C 16 16 20 2C 20 23 26 27 29 2A  :CSDN@五五六六0524
```

解码flag{6f1797d4080b29b64da5897780463e30}



题49、 john-in-the-middle

下载得到一个流量包，扔进wireshark里没有搜出来什么有用的东西，扔进kali里提取出来几张图片



00000308.png



00000403.png



00000644.png



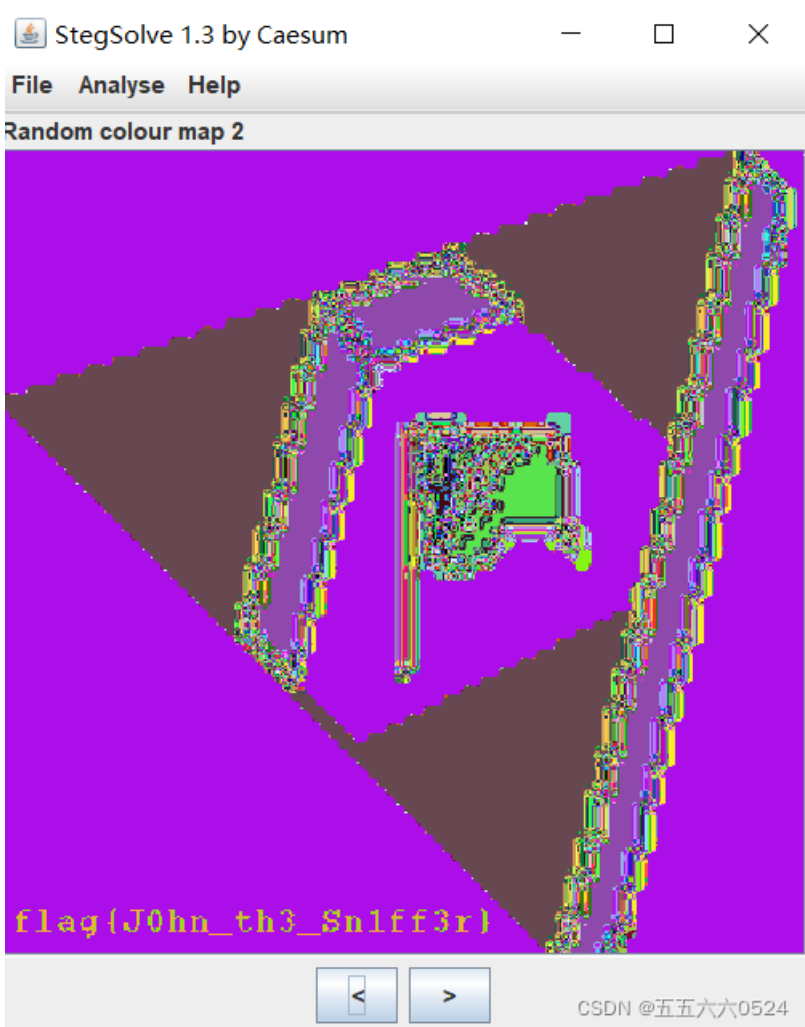
00000650.png



00000656.png

CSDN @五五六六0524

第一张里面有一个旗子，flag就是夺旗嘛，扔进stegsolve果然有收获，flag{J0hn_th3_Sn1ff3r}



题50、[安洵杯 2019]吹着贝斯扫二维码

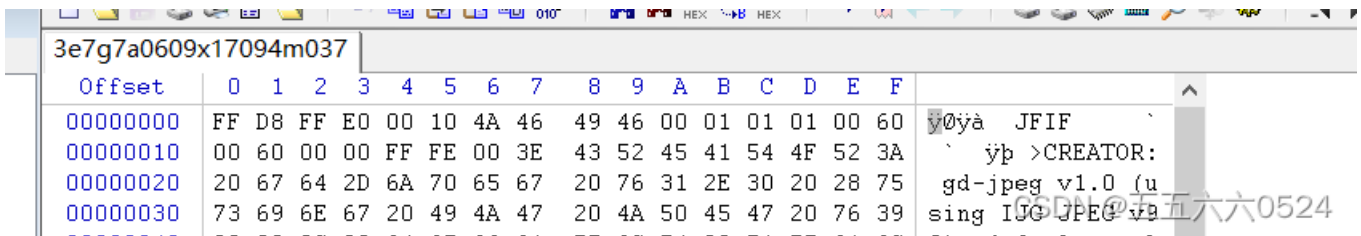
解压得到一堆乱码的文件和一个flag.zip，题目说和base有关，猜想可能是文件名连在一起然后解密，得到之后发现不对

```
# -*- coding: utf-8 -*-
import os

def file_name(file_dir):
    for root, dirs, files in os.walk(file_dir):
        #print(root) #当前目录路径
        #print(dirs) #当前路径下所有子目录
        #print(files) #当前路径下所有非目录子文件
        flag=''
        for a in files:
            flag=flag+a
        print(flag)

file_dir='C:\\Users\\86139\\Desktop\\吹着贝斯扫二维码'
file_name(file_dir)
```

把文件扔进winhex发现是图片，全加后缀，得到一堆二维码的残片，拼的眼睛疼，最后放弃了



```
import os
path = 'C:\\Users\\86139\\Desktop\\吹着贝斯扫二维码'

for i in os.listdir(path):
    if i == 'flag.zip':
        continue
    else:
        oldname = os.path.join(path,i)
        newname = os.path.join(path,i+'.jpg')
        os.rename(oldname,newname)
```

扫码是BASE Family Bucket ??? 85->64->85->13->16->32

工具: [base编码转换-base64编码与解码-在线工具](#)、CaptfEncoder

flag.zip的注释

GNATOMJVIQZUKNJXGRCTGNRTGI3EMNZTGNBTKRJWGI2UIMRRGNBDEQZWGI3DKMSFGNCDMRJTIIK

转base32

3A715D3E574E36326F733C5E625D213B2C62652E3D6E3B7640392F3137274038624148

转base16

:q]>WN62os<^b]!;,be.=n;v@9/17'@8bAH

转root13

:d]>JA62bf<^o]!;,or.=a;i@9/17'@8oNU

转base85

PcTvdWU4VFJnQUByYy4mK1lraTA=

转base64

<+oue8TRgA@rc.&+Yki0

转base85

ThisIsSecret!233

解压flag{Qr_ls_MeAn1nGful}

题51、[ACTF新生赛2020]swp

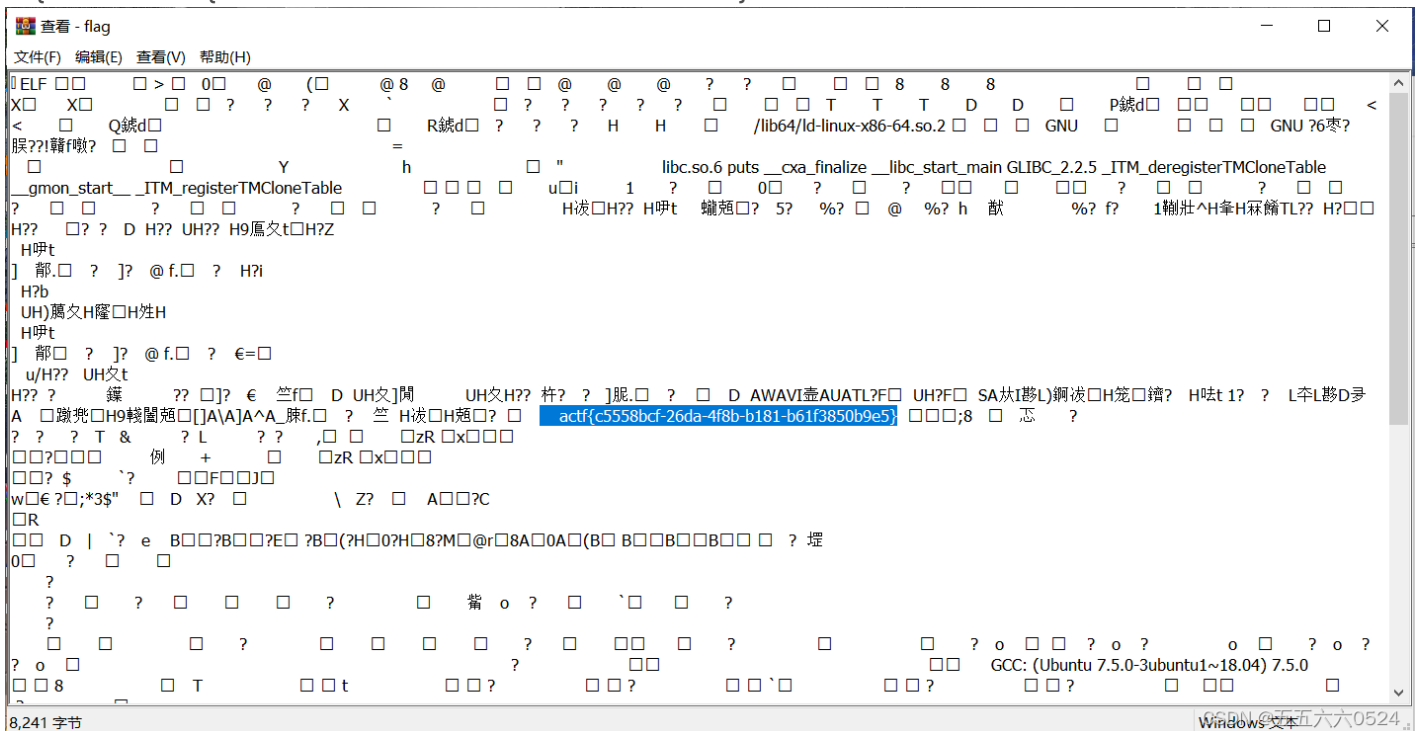
解压得到流量包，http导出对象，得到一堆图片和一个zip，zip用winhex打开，发现0304和0102后面都是0000，伪加密，改一下加密位00改成08

secret.zip	Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
	00000000	50	4B	03	04	14	00	00	08	08	00	F0	B2	3E	50	D8	E0	PK
	00000010	57	83	6E	09	00	00	00	40	00	00	09	00	00	00	2E	66	Win @ .f
	00000020	6C	61	67	2E	73	77	70	ED	59	6B	6C	1C	57	15	DE	D9	lag.swpiYkl W PÙ
	00000030	F5	63	7D	63	CF	4E	1E	4D	EC	24	C8	9B	34	41	49	8A	8c}cIN MiSE!4AI!
	00000040	D7	AF	D8	DD	50	4C	BD	EB	47	C6	95	9D	04	77	93	A6	×0YPL!eGF! w!!
	00000050	0F	67	3C	FB	B2	57	EC	C3	DA	9D	05	3B	80	1A	E1	34	g<u^wiAU -; ä4

发现能打开flag

..	文件				
.flag.swp *	16,384	2,414	SWP 文件	2020/1/30 22:...	8357E0D8
flag	8,241	2,329	文件	2020/1/30 22:...	1E267A74

搜{，直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}



swp放到linux是一个隐藏文件(ls -a, swp文件确实存在)，linux下非正常退出vi编辑文本后会自动生成.swp文件
使用vim -r 文件名 恢复flag文件

[BUUCTF Misc \(二\) -布布扣-bubuko.com](#)

题52、[GXCTF2019]SXMgdGhpcyBiYXNIPw==

题目base64解码Is this base?, 解压得到一个flag.txt, base64直接解不对

Base64 Encoding

Encode Decode

Pattern
Base64

```
Q2V0dGUgbnVpdCwK
SW50ZW5hYmxlIGluc29tbnllLAp=
TGEgZm9saWUgbWUgZ3VldHRlLAo=
SmUgc3VpcyBjZSBxdWUgamUgZnVpcwP=
SmUgc3ViaXMsCt==
Q2V0dGUgY2Fjb3Bob25pZSwK
UXVpIG1lIHJjaWUgbGEgdOmUmnRlLAp=
QXNzb21tYW50ZSB0YXJtb25pZSwK
RWxsZSBtZSBkaXQsCo==
VHUgcGFpZXJhcyB0ZXMgZGVsaXRzLAp=
UXVvaSBxdSdpbCBhZHZpZW5uZSwK
T24gdHJh5Y2Y2vbmUgc2VzIGNoYeWNR25lcywK
U2VzIHBlaw5lcywK
SmUgdm91ZSBtZXMgbnVpdHMsCm==
QSBsJ2Fzc2FzeW1waG9uaWUscI==
QXV4IHJlcXVpZW1zLAr=
VHVhbnQgcGFyIGRlcGl0LAQ=
```

```
Cette nuit,
Intenable insomnie,
S H Y H Y ] K R 7 V 2 6 R V R
R g V 0 ) + P ] H X Y K
] Z H Y H Y H H : e & K 7 6 FR
& R V R R F B Tu paieras
tes delits,
T]
[ H ] ! [ Y Y [ K 9 y c k H \ ] y
c k \ \ Z [ \ H Y Y \ Z ]
P ] ^ \ ] Z Y \
G V B " F W B
p + R H Y \ ] Z
Y \ ( ) U \ ] ^ ] Z
H Z [ Y
[ Z K Q q a * Q e
```

CSDN @五五六六0524

base64隐写base64隐写解密代码_Root_5476-CSDN博客_base64隐写解密

```

'''
base64隐写解密
'''

base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

flag=''
with open('C:\\Users\\86139\\Desktop\\flag.txt','r') as f:
    for line in f.readlines():
        line=line[:-1]
        num=line.count('=')
        if num == 0 :
            continue
        lastchar = line[-(num+1)]

        #print(line,num,lastchar)
        myindex = base64chars.index(lastchar)
        #print(myindex)
        bin_str = bin(myindex)[2:].zfill(6)
        #print(bin_str)
        flag+=bin_str[6-2*num:]
        #print(bin_str[6-2*num:])
print(''.join([chr(int(flag[i:i + 8], 2)) for i in range(0, len(flag), 8)]))

```

直接出GXY{fahzhenhaoting}