CTF隐写术之总结 让你少走弯路

原创

艺博东 于 2020-10-04 11:29:32 发布

分类专栏： 网络攻防 文章标签： CTF

本文链接：https://blog.csdn.net/HYD696/article/details/108866839

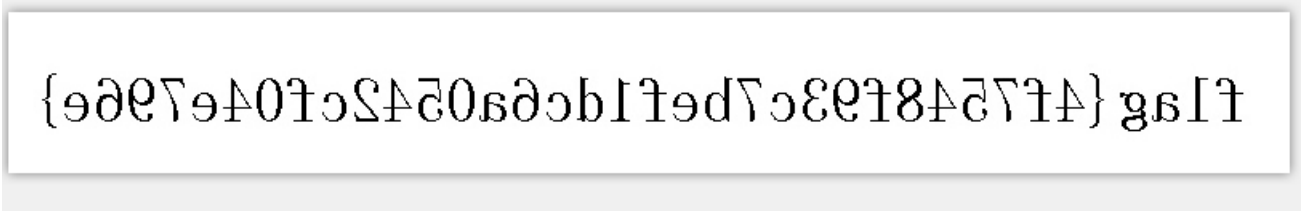
文章目录

一、reverseMe

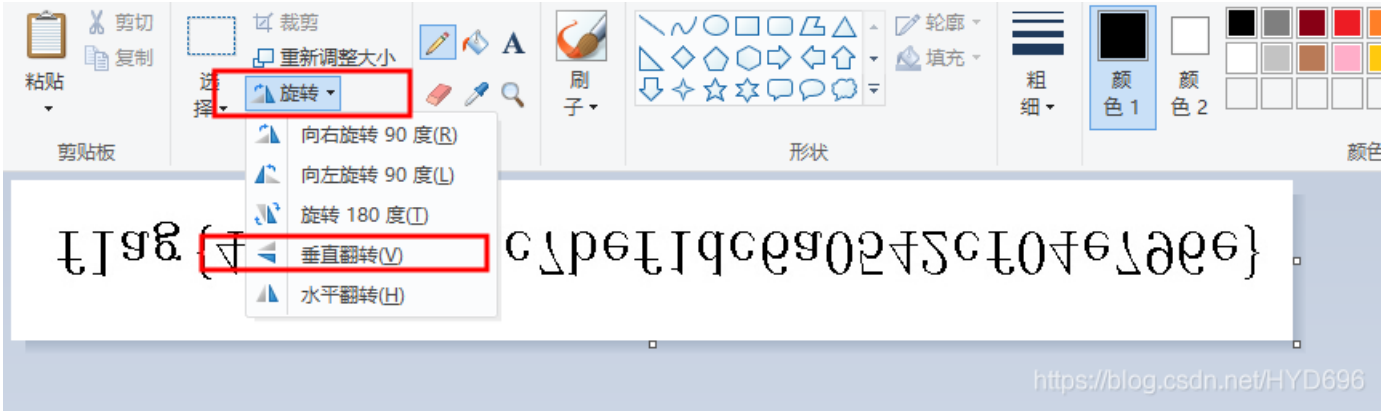
1、附件

链接：https://pan.baidu.com/s/1wO3WN3Ss19LHwjGfY0r4YQ

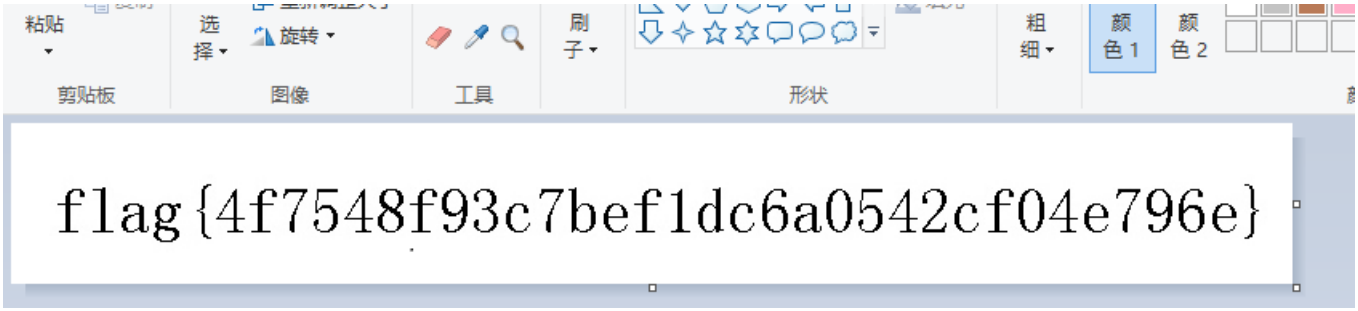
提取码：ed9n



2、用画笔工具打开—>旋转—>垂直旋转



3、效果



4、OK

flag{4f7548f93c7bef1dc6a0542cf04e796e}

二、a_good_idea

1、附件

链接：https://pan.baidu.com/s/1xC69L9r6qPe6jp8K1_lb3Q
提取码：ooit

2、题目描述： 汤姆有个好主意

3、是使用工具（1）stegsolve（2）binwalk

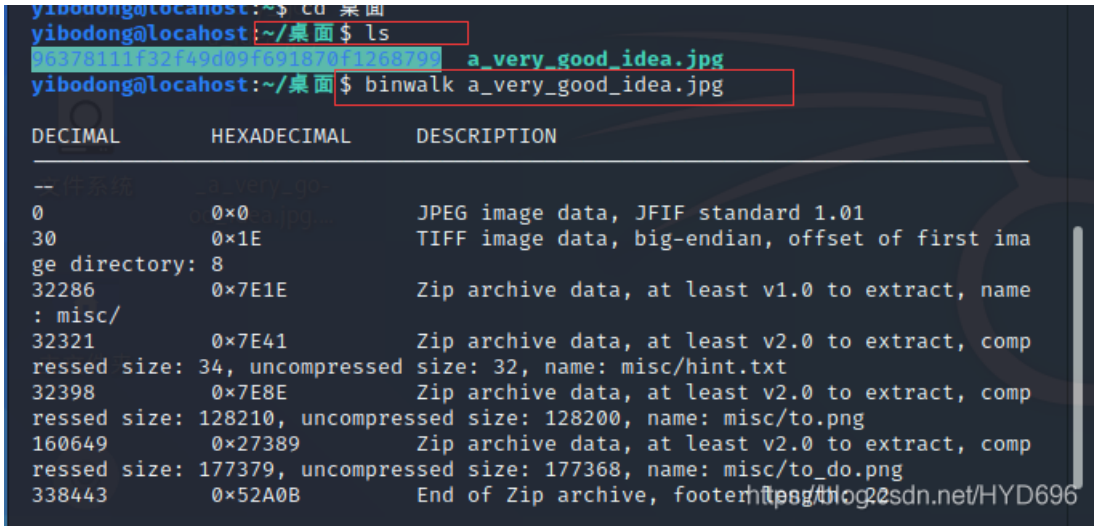
4、环境：kail Linux

5、拷贝到kail Linux里

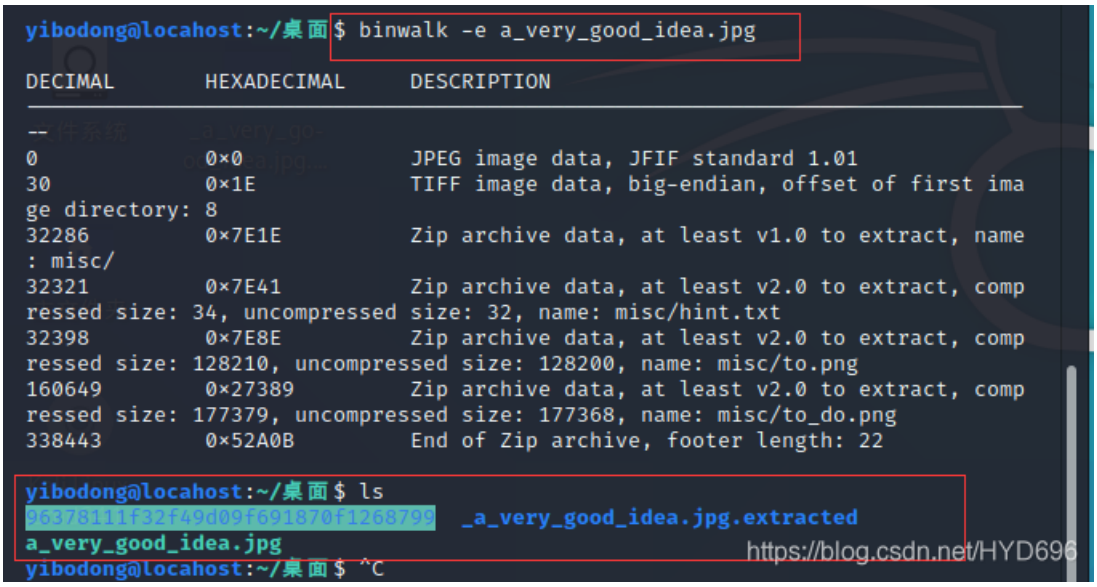
6、执行以下步骤

```
cd 桌面
ls
binwalk a_very_good_idea.jpg     //
binwalk -e a_very_good_idea.jpg  //可适用于压缩文件,如.zip的提取
ls
```

binwalk a_very_good_idea.jpg

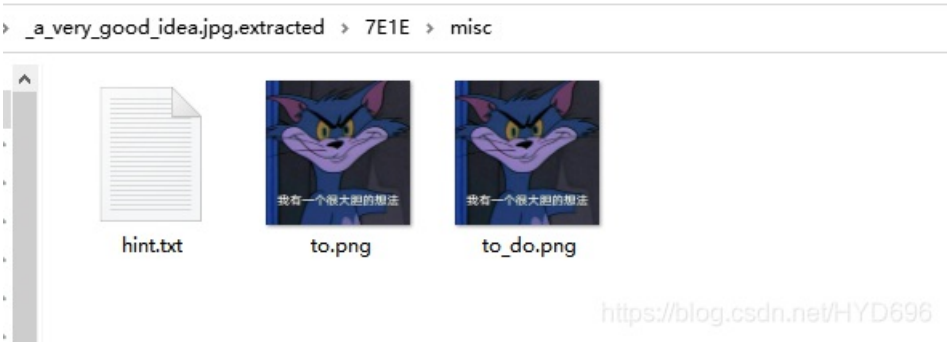


binwalk -e a_very_good_idea.jpg



7、把“_a_very_good_idea.jpg.extracted”文件拷贝到win系统

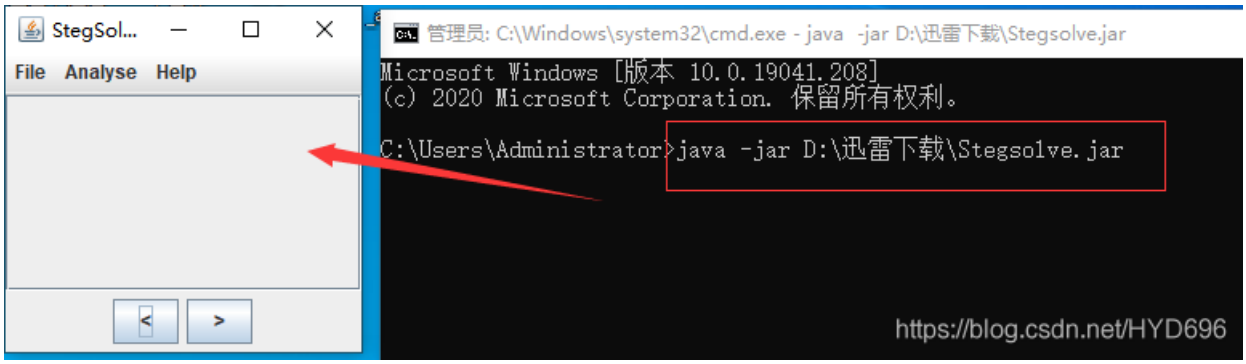
8、文件


_a_very_good_idea.jpg.extracted
7E1E
misc
hint.txt
to.png
to_do.png
我有一个很大胆的想法
我有一个很大胆的想法
https://blog.csdn.net/HYD696

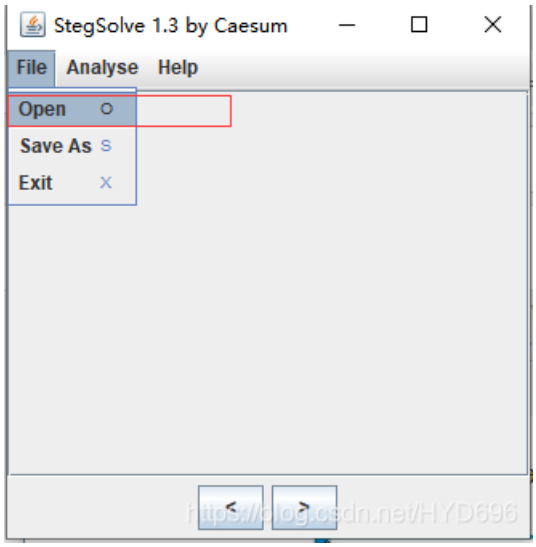
9、查看“hint.txt”


hint.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
try to find the secret of pixels
网易有道词典
词典
翻译
英汉互译
try to find the secret of pixels
试着找出像素的秘密
https://blog.csdn.net/HYD696

10、打开工具“Stegsolve”，直接在cmd下输入“java -jar D:\迅雷下载\Stegsolve.jar”（路径）

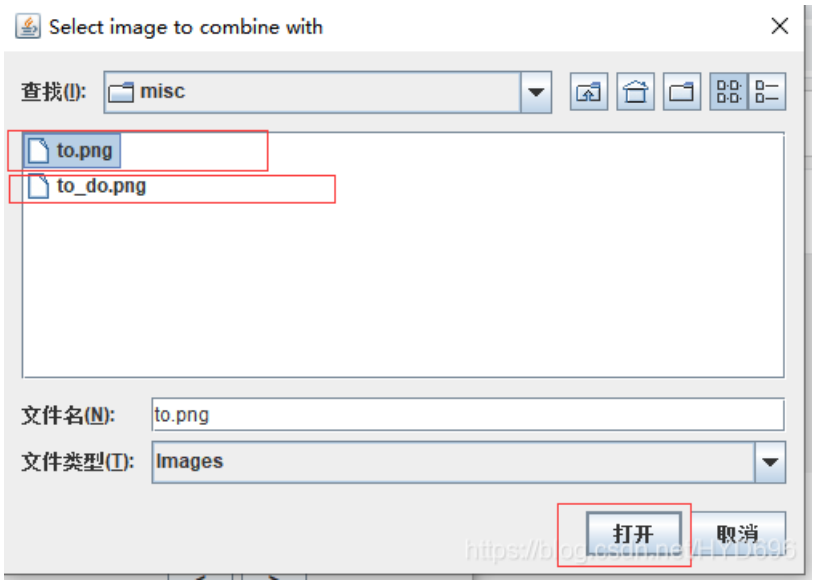


11、File—>Open—>图片

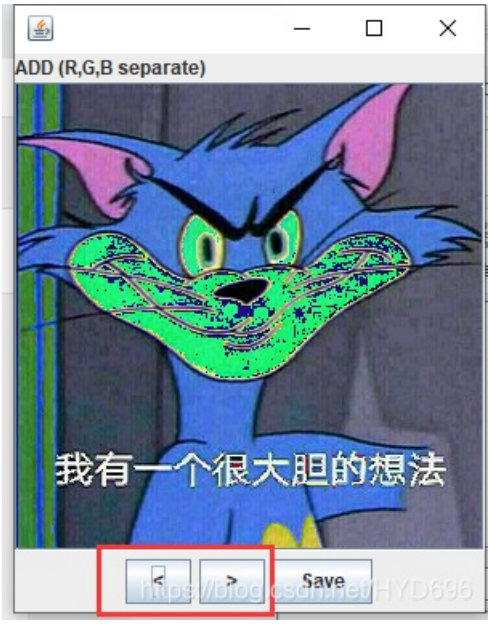


12、Image Combiner

13、打开图片



14、按左右键，会跳出二维码



15、二维码

16、用微信扫一扫，flag就出来了

17、OK

NCTF{m1sc_1s_very_funny!!!}

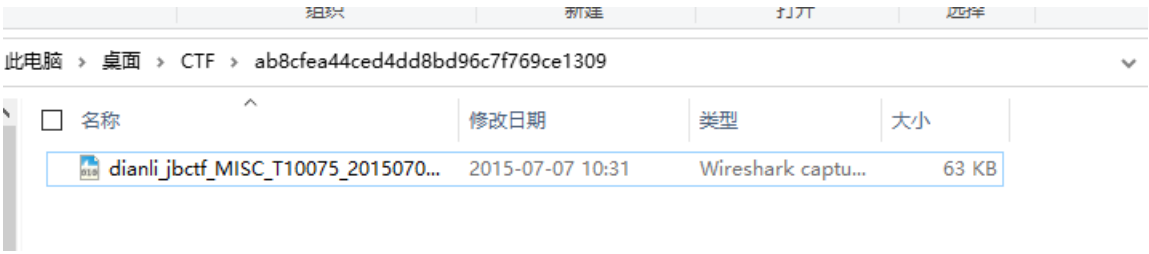
三、wireshark-1

题目来源： 广西首届网络安全选拔赛
题目描述： 黑客通过wireshark抓到管理员登陆网站的一段流量包
题目附件： 提取文件

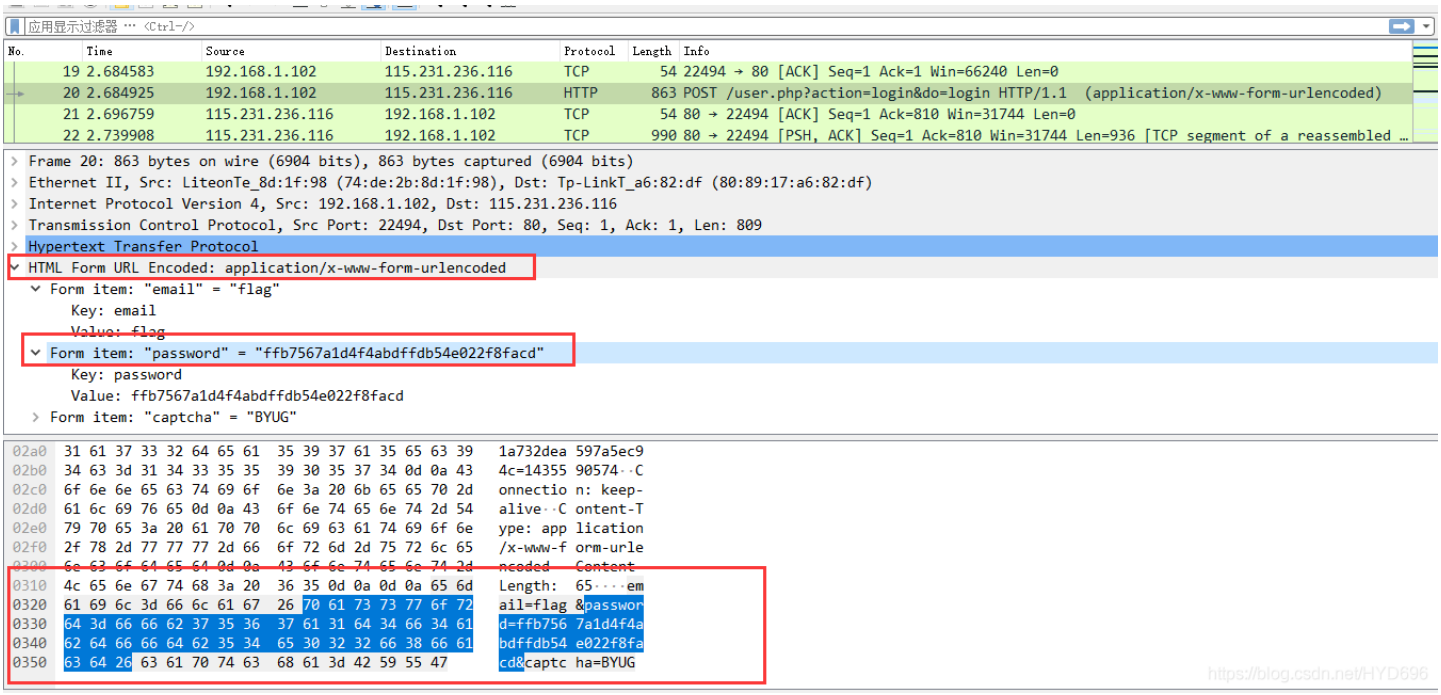
1、附件

链接：https://pan.baidu.com/s/1lAFQl2o1iGETeWnhxNl10A
提取码：qzad

2、文件



3、用wireshark软件打开



Form item: “password” = “ffb7567a1d4f4abdffdb54e022f8facd”

4、OK

flag{ffb7567a1d4f4abdffdb54e022f8facd}

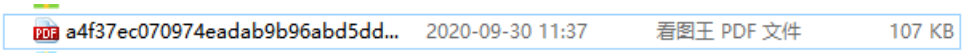
四、小小的PDF

难度系数： ★★★
题目附件： 附件1

1、附件1

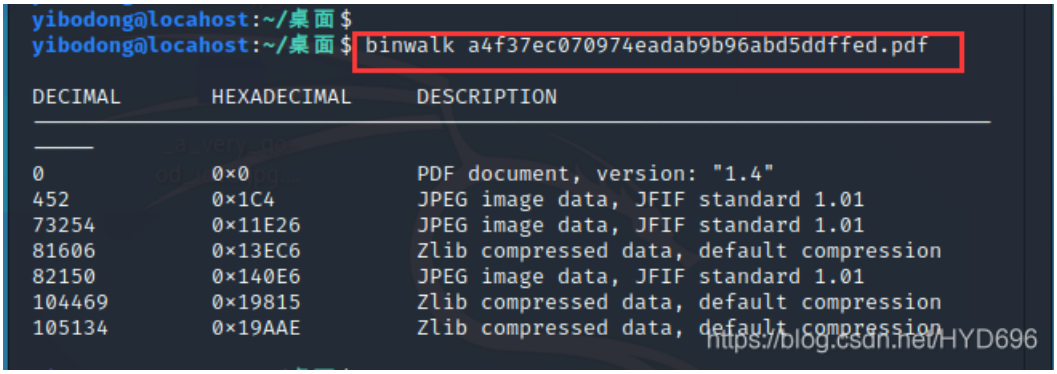
链接：https://pan.baidu.com/s/1j4uMJsci5gXZFcAcEgj9ig
提取码：3aw8

2、文件

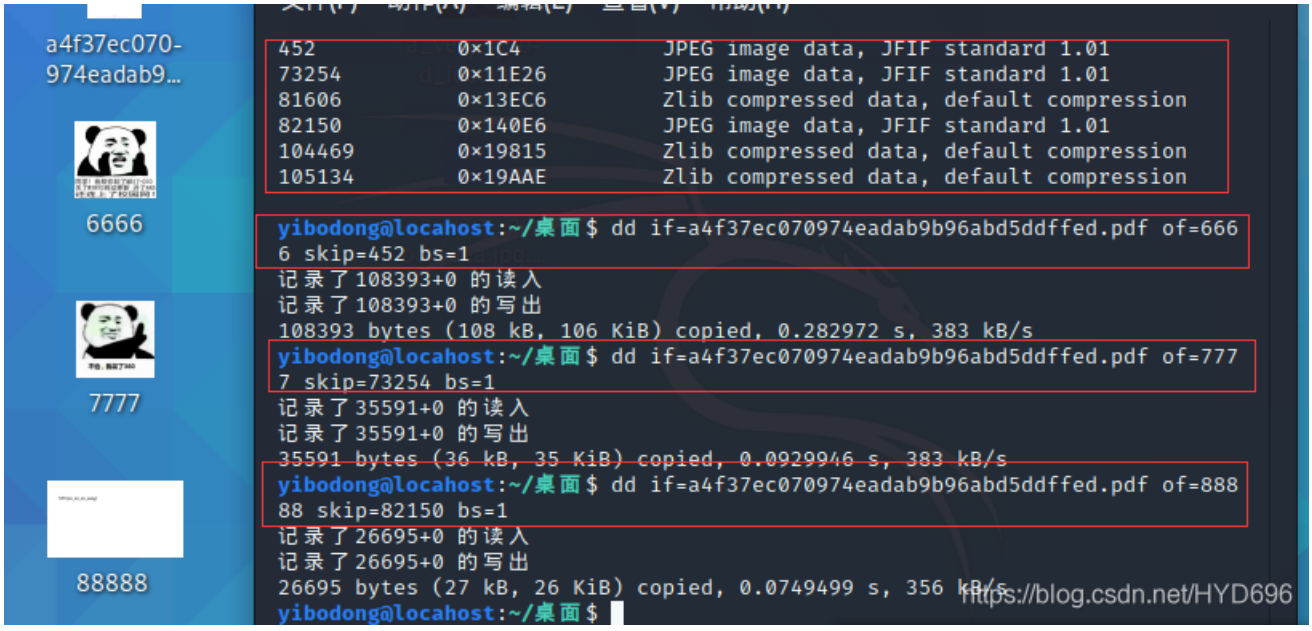


3、拷贝到kail Linux里

4、binwalk XXX.xxx



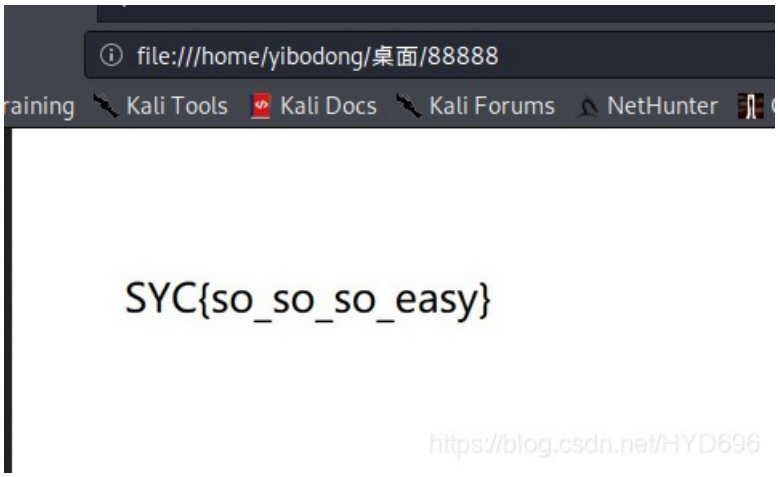
5、提取



dd if=XXX11.jpg of=XXX22.jpg skip=XX6666 bs=1

dd命令详解，if是指输入文件，of是指输出文件，skip是指从输入文件开头跳过blocks个块后再开始复制，bs设置每次读写块的大小为1字节 。

6、88888



7、OK

SYC{so_so_so_easy}

五、打开电动车

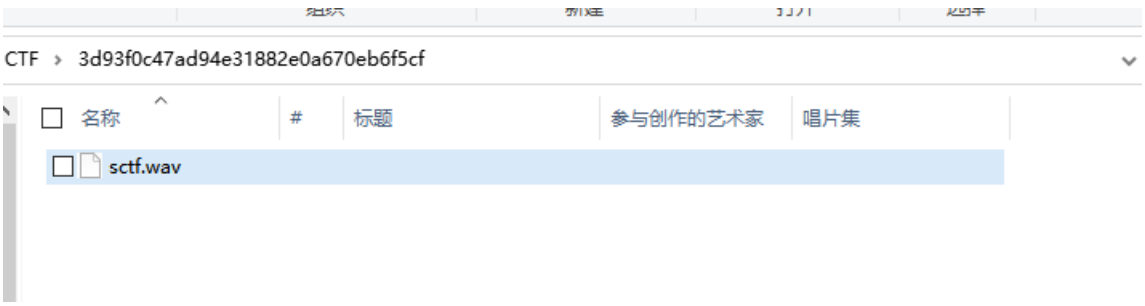
难度系数： ★★★★
题目描述： 截获了一台电动车的钥匙发射出的锁车信号，3分钟之内，我要获得它地址位的全部信息。flag内容二进制表示即可。

题目附件： 附件1

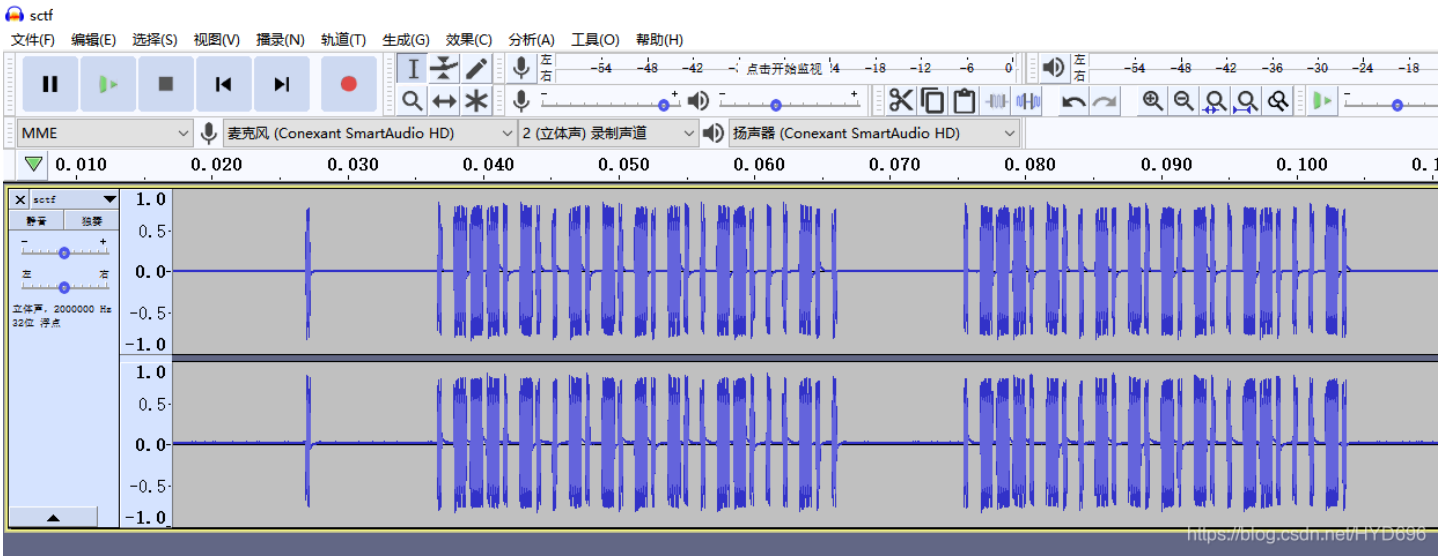
1、附件1

链接：https://pan.baidu.com/s/1GYynVG0Q9PBj5hlrz7pQmQ
提取码：czvo

2、文件



3、用“Audacity”软件打开以及分析



信号！短的一段表示是0，长的一段表示是1，得到如下一段：

0 01110100101010100110 0010 0

一个是PT2242的，前面4bit表示同步码，中间的20bit表示地址码，后面的4bit表示功能码，后面最后一个是停止码。

4、OK

sctf{01110100101010100110}

六、gif

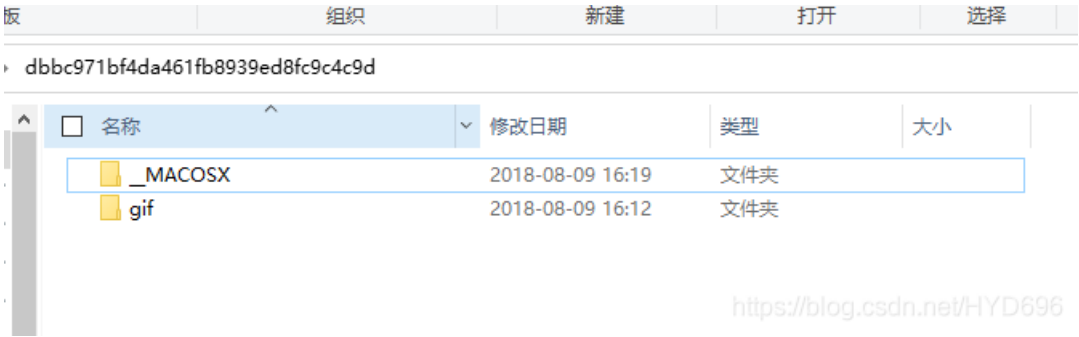
难度系数： ★★★★
题目描述： 菜狗截获了一张菜鸡发给菜猫的动态图，却发现另有玄机
题目附件： 附件1

密码学范畴

1、附件1

链接：https://pan.baidu.com/s/1Kc1XFjn6mpLaeUyJ518Mew
提取码：h16i

2、文件

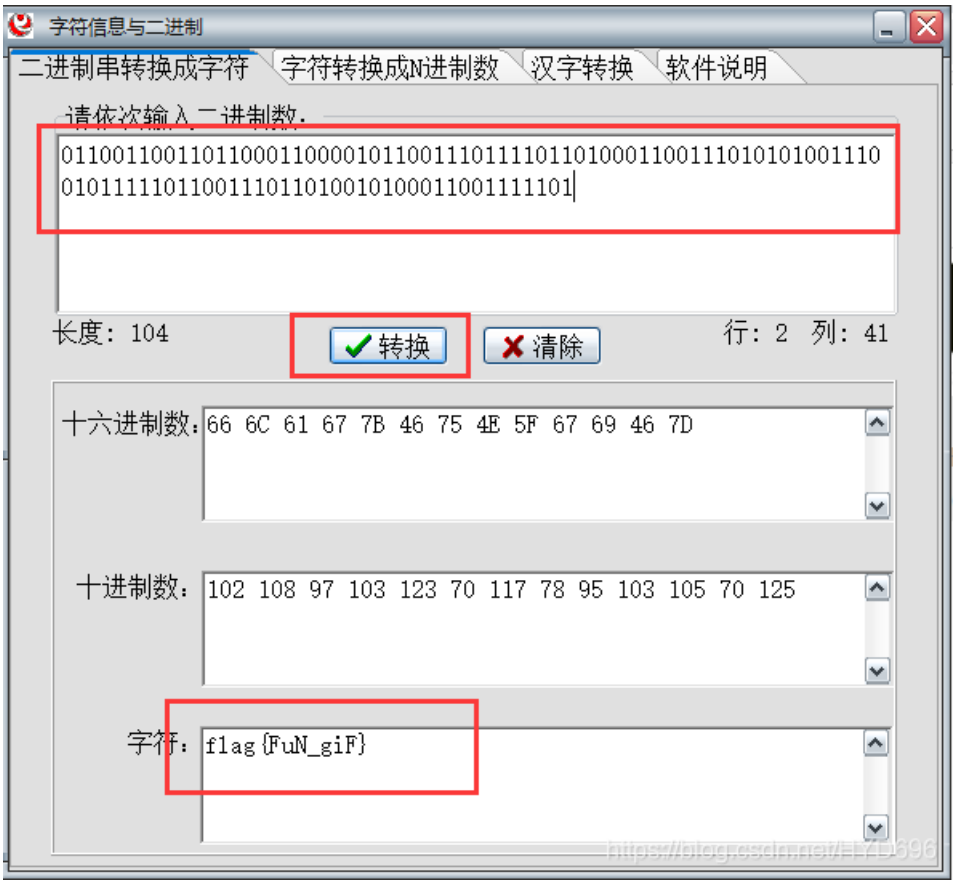


3、查看gif文件

打开gif文件出现很多黑白.jpg；
联想到二进制，白色图片代表0，黑色图片代表1。

01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101

4、二进制转字符串



5、OK

flag{FuN_giF}

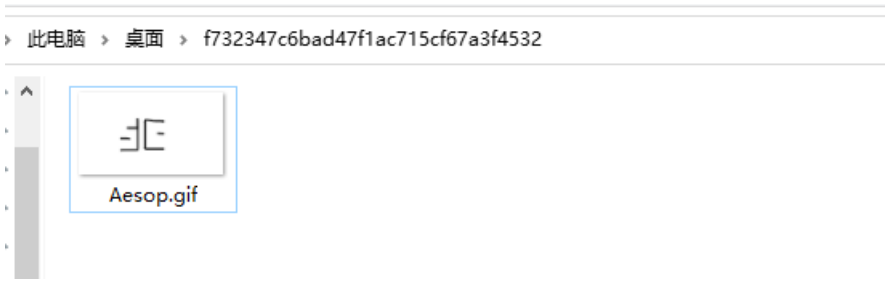
七、Aesop_secret

难度系数： ★
题目来源： 2019_ISCC
题目附件： 附件1

1、附件

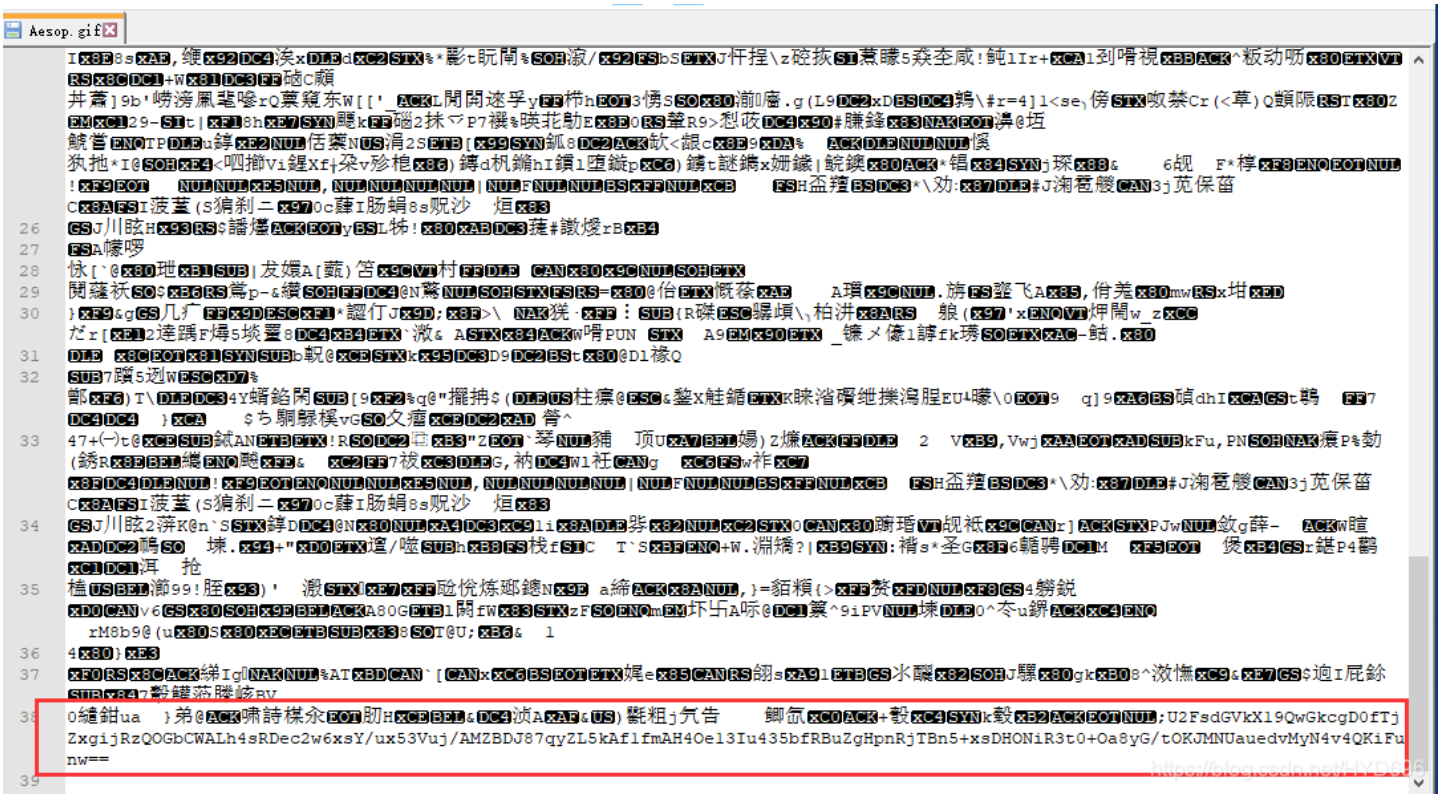
链接：https://pan.baidu.com/s/18nqlaEvi_lb0RtKNuHR_Ww
提取码：pvdf

2、文件



解压之后发现是一张动态图片。

3、用notepad软件打开



发现前面是乱码，但最后不是乱码。

U2FsdGVkX19QwGkcgD0fTjZxgijRzQOGbCWALh4sRDec2w6xsY/ux53Vuj/AMZBDJ87qyZL5kAf1fmAH4Oe13Iu435bfRBuZgHpnRjTBn5+xsDHONiR3t0+Oa8yG/tOKJMNUauedvMyN4v4QKiFunw==

4、AEC算法解密

在线AEC解密，密码为ISCC。

U2FsdGVkX18OvTUlZubDnmvk2lSAkb8Jt4Zv6UWpE7Xb43f8uzeFRUKGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

5、继续解密

6、OK

flag{DugUpADiamondADeepDarkMine}

八、结论

（一）常用的工具/软件/环境

1、kail Llnux（渗透必备）
2、Stegsolve
3、winhex
4、wireshark
5、画笔工具
6、burpsuite
7、Audacity
8、字符信息与二进制
9、notepad
10、md5破解工具
11、Md5加密
12、csrss

（二）隐写术可以用图片、音频、视频为载体将数据隐藏在其中，在图片最为常见。

（三）一般破解隐写术的方法

1、或将图片放在kali Linux系统中，执行binwalk xxx.jpg命令 查看图片的隐藏文件

2、使用StegSolve工具对图像进行分通道扫描

3、在windows系统命令行下使用F5-steganography-master进行jpg图像是否为F5算法隐写

4、在kali系统中使用outguess-master工具，检测是否为guess算法隐写

5、利用WinHex打开图像，搜索CTF查看是否存在相关信息

6、一般破解隐写术的方法

（1）查看图像—>属性—>详细信息是否包括隐藏内容

（2）利用WinHex打开图像，搜索CTF查看是否存在相关信息

（3）检查图像开始标志和结束标志是否正确，若不正确修改图像标志恢复图像，打开查看是否存在ctf或flag等信息

JPEG/JPG(2 bytes)
文件头标识 FF D8
文件结束标识 FF D9

GIF(6 bytes)
文件头标识 47 49 46 38 39(37) 61
文件结束标识 01 01 00 3B

PNG(8 bytes)
文件头标识 89 50 4E 47 0D 0A 1A 0A

BMP(2 bytes)
文件头标识 42 4D

ZIP Archive (zip)
文件头：50 4B 03 04

RAR Archive (rar)
文件头：52617221

XML (xml)
文件头：3C3F786D6C

HTML (html)
文件头：68746D6C3E

（四）常用的在线加解密算法等在线工具

1、在线AES加密 | AES解密 - 在线工具：
https://www.sojson.com/encrypt_aes.html

2、md5在线解密破解,md5解密加密
https://www.cmd5.com/

3、Base64加密、解密–站长工具
http://tool.chinaz.com/Tools/Base64.aspx

4、ASCI在线转换器，ASCII码
https://www.sojson.com/ascii.html

5、在线RSA加密解密,RSA2加密解密
https://www.bejson.com/enc/rsa/

6、16进制转换，16进制转换文本
https://www.sojson.com/hexadecimal.html

7、python反编译–在线工具
https://tool.lu/pyc/

8、在线工具，对称加密、非对称加密、证书工具、SSL检测、SSL漏洞
https://www.ssleye.com/

我是艺博东！欢迎你和我一起讨论，我们下期见。