攻防世界misc高手进阶篇教程（1）

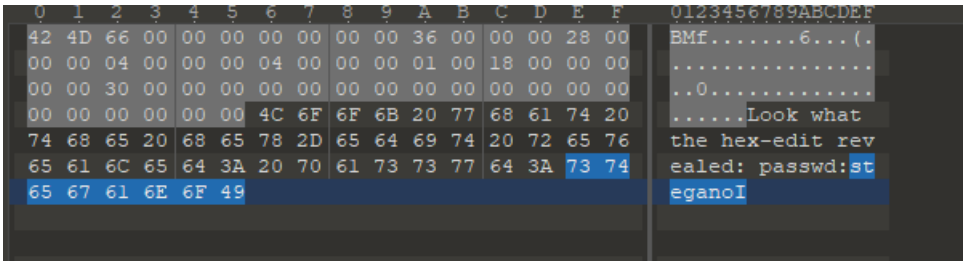
原创

锋刃科技 于 2020-05-24 16:46:14 发布 1904 收藏 5
文章标签： 攻防世界 ctf

本文链接：https://blog.csdn.net/xuandao_ahfengren/article/details/106316990

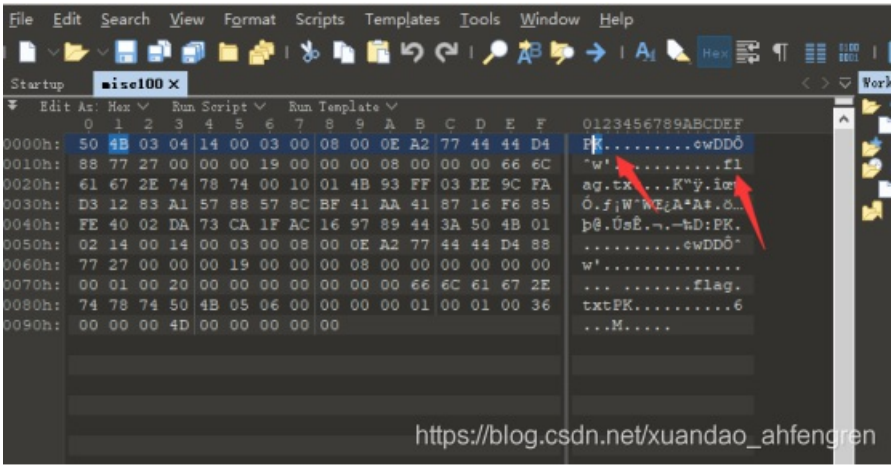
Training-Stegano-1z

直接用winhex打开即可

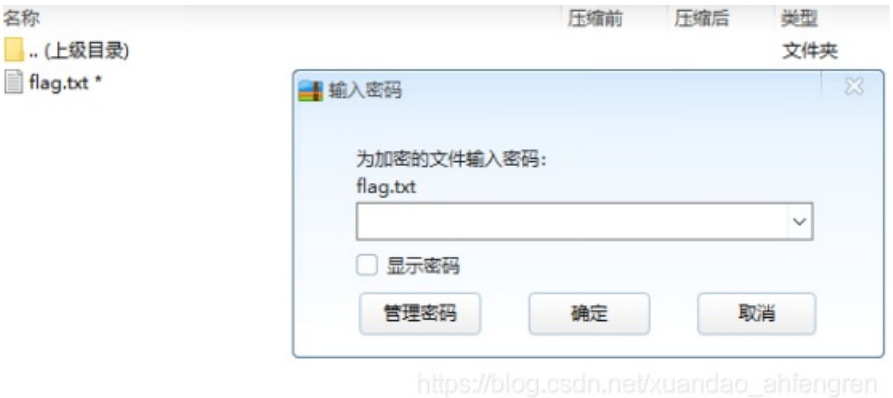


János-the-Ripper

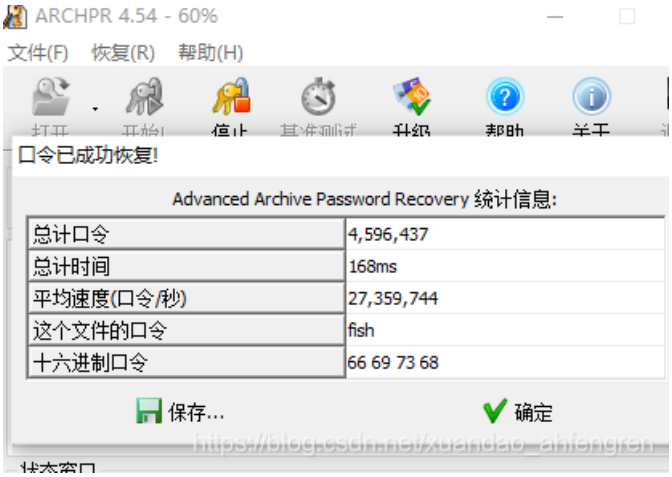
用winhex打开发现flag.txt和PK头，也就是压缩包嘛，直接保存为zip打开



发现需要密码

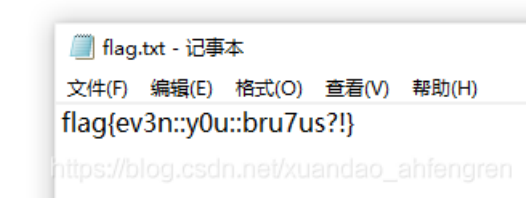


用ARCHPR爆破密码



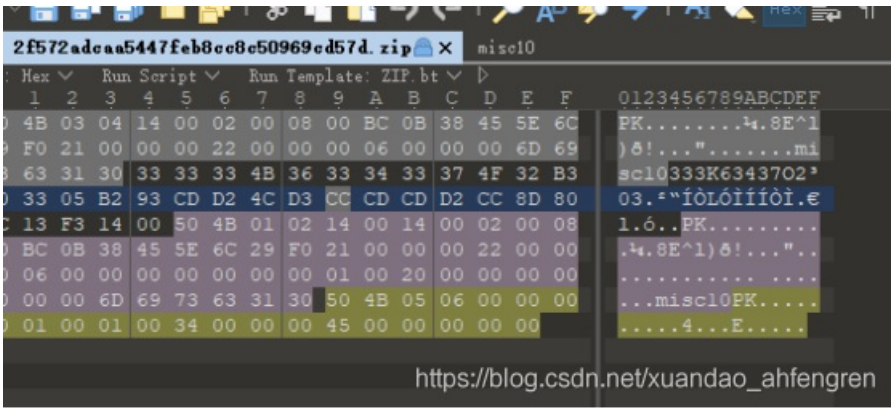
密码为fish

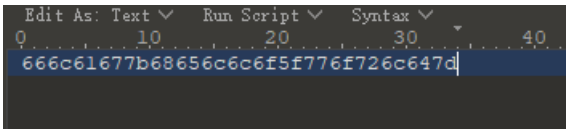
打开既有flag



Test-flag-please-ignore

用winhex打开里面有misc10文件，打开misc10发现疑似十六进制的文本



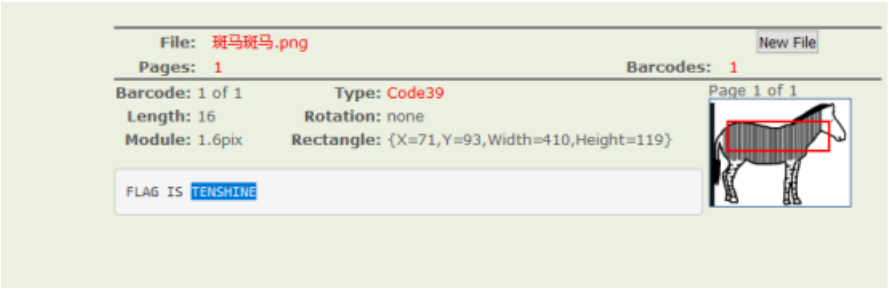


转换即可

Banmabanma

https://online-barcode-reader.inliteresearch.com/

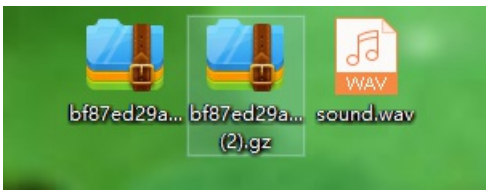
用在线工具进行扫描即可获取flag，加上flag格式直接提交



flag{TENSHINE}

Hear-with-your-Eyes

下载完附件之后，进行解压，然后把后缀名修改成gz再解压，还是修改成gz后缀解压之后就是音频文件了

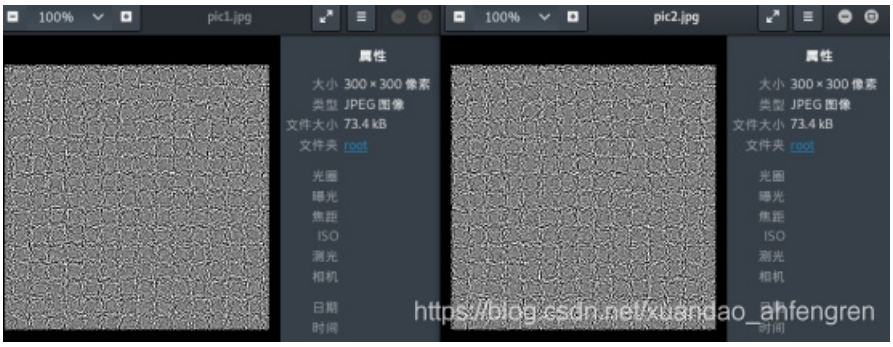


用打开Audacity

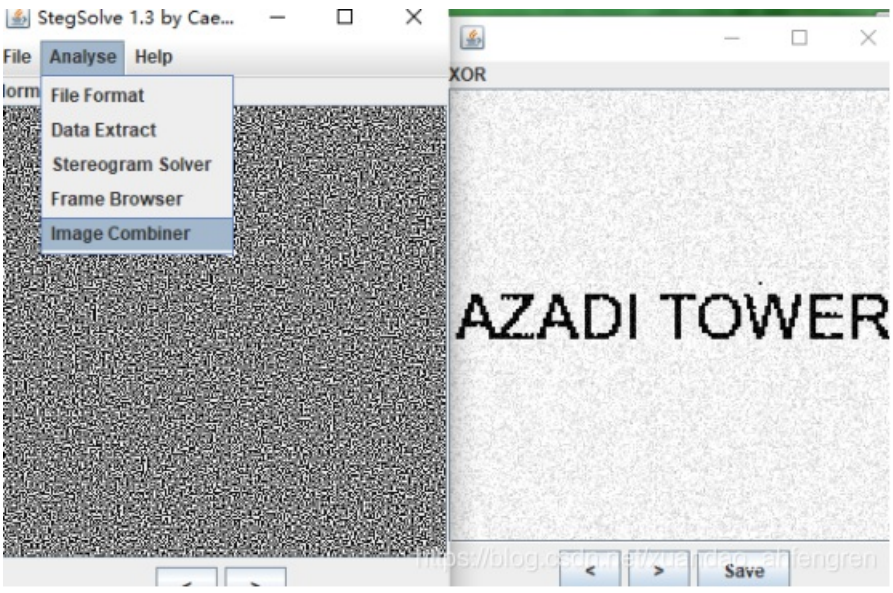
用频谱图打开即可

What-is-this

先打开压缩文件然后再tar -xvf解出两个文件



用StegSolve合成两文件即可获取flag

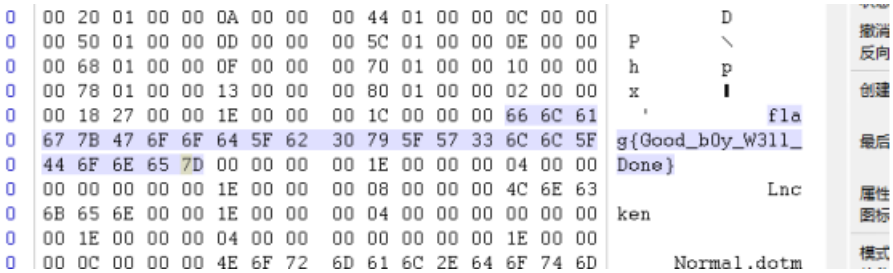


base64÷4

这就是告诉你，是base16嘛，直接拿去base16解密即可

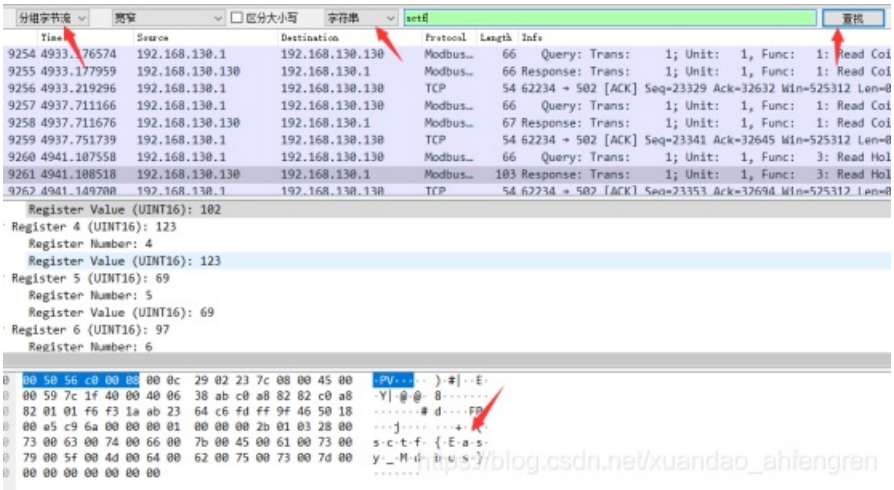
Embarrass

直接用winhex搜索flag{即可



神奇的Modbus

用wireshark打开然后搜索，字符串和字节流类型搜索sctf即可



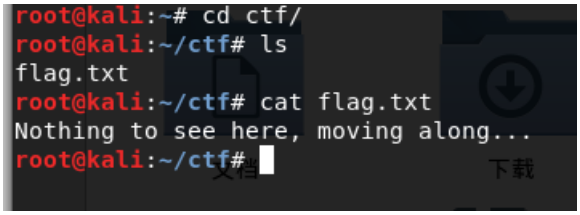
sctf{Easy_Modbus}

MISCall

先用file查看这是什么文件，然后进行压缩

```
root@kali:~# file d02f31b893164d56b7a8e5edb47d9be5
d02f31b893164d56b7a8e5edb47d9be5: bzip2 compressed data, block size = 900k
root@kali:~#
```

tar -xvf d02f31b893164d56b7a8e5edb47d9be5



这是个假的flag文件

查看修改列表

git stash list

删除flag.txt文件

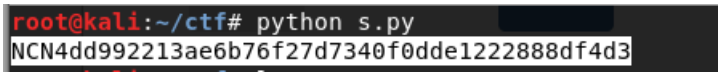
rm -rf flag.txt

使用git stash show校验列表中存储的文件

得到的flag.txt也是假的

运行s.py即可

得到flag直接提交即可



Reverse-it

用命令获取到反转的flag

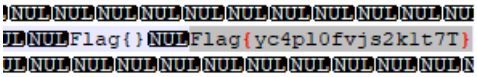
xxd -p 0da9641b7aad4efb8f7eb45f47eaebb2 | tr -d '\n' | rev | xxd -r -p > reversed

我们再用convert -flop reverse reversed

进而获取到flag是SECCON{6in_tex7}

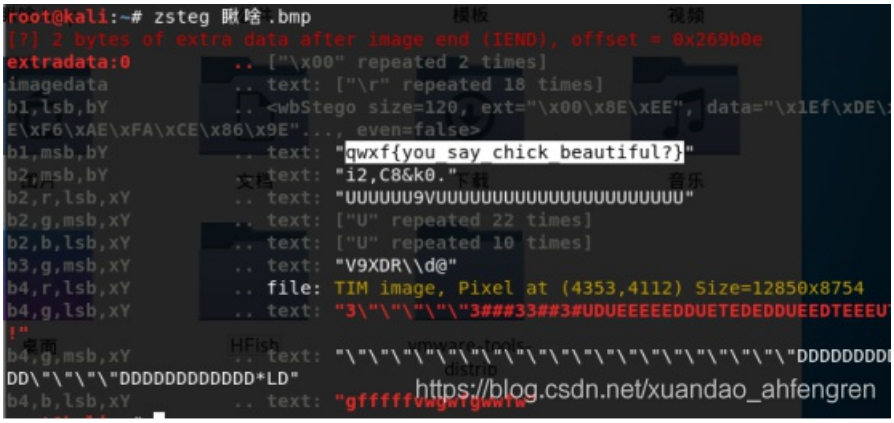
something_in_image

用编辑器直接打开然后搜索flag即可



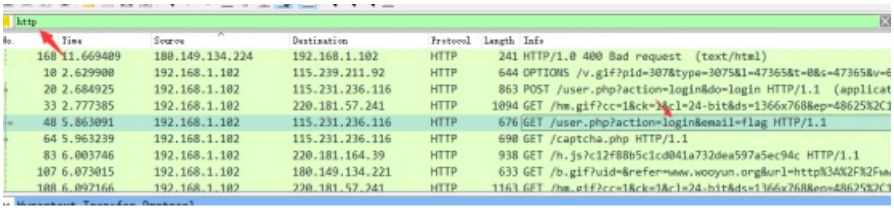
打野

下载附件用zsteg打开即可发现flag



wireshark-1

我们先过滤http，然后看到了个login登录的包，我们追踪tcp流看看



根据题目要求密码就是flag

```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.wooyun.org/user.php?action=login
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400;
Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,1435557576,1435590542;
bdshare_firstime=1433775454650; wy_uid=-1; PHPSESSID=h8i10mi6rdc819coc708otq661;
Hm_lpvt_c12f88b5c1cd041a732dea597a5ec94c=1435590574
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdffdb54e022f8facc&captcha=BYUGHTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Server: yunjiasu-nginx
CF-RAY: 1fe28d0a63e91c3b-JXG
Content-Encoding: gzip

236
..........l.Ok.A....~...zZ....qS..ZH.P,i..ut......*.`....J....6...6.L...|.......c`!
9....<...I.I=M..W.....X}.`.Q...Bk.$B.t
.x.~..b.9.&.Iu.[.b .....1f.C.X,F...Er(.....X.....JF3,..n.JL7...I..zb..."..X..o.3....
0i...,.....U(.2\b(H/.US..L..ld...[...L.PA|...!...$jk.}E
.e....].WtC..JN.2..x          .Y.z........&....>...M..G.R....Hs.....D...T.X.J.1.
```

pure_color

把文件放进StegSolve里面，左右换颜色即可

flag{true_steganographers_doesnt_need_any_tools}

Aesop_secret

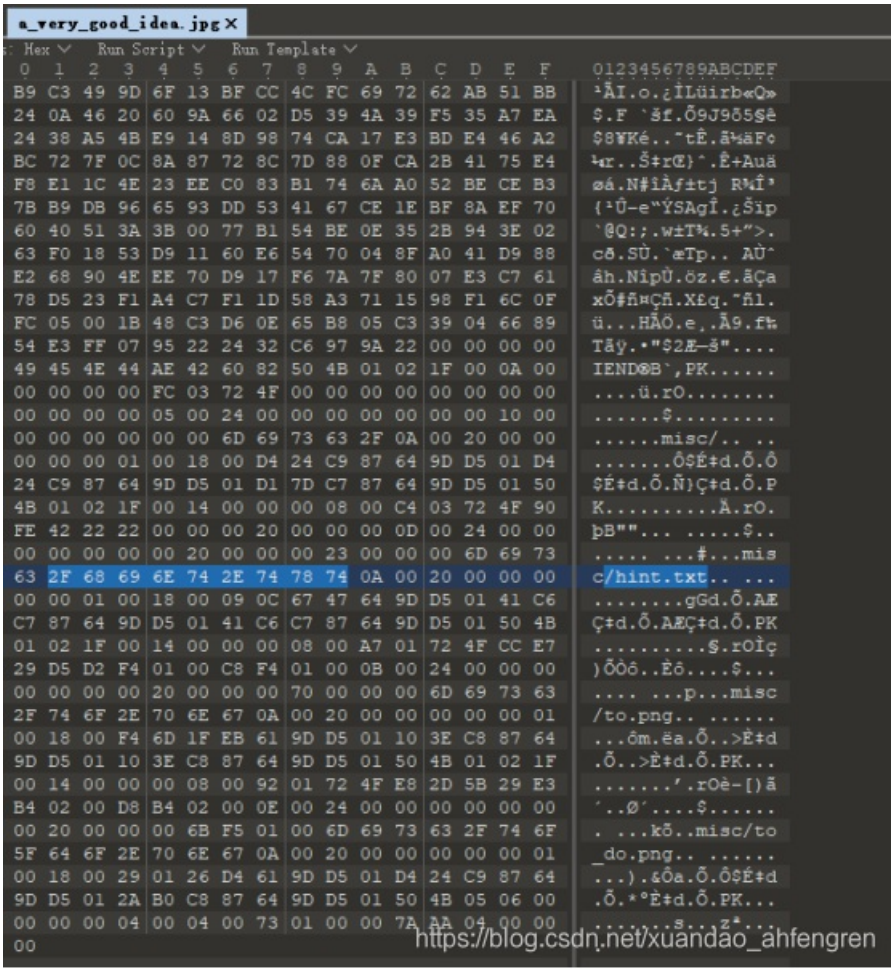
下载附件之后打开，发现一串字符串，这似乎是ase加密，但是我们没有密匙

这是动态图片，每一帧图片都不一样，我们把每一帧都放在一起发现了ISCC，就是密匙了

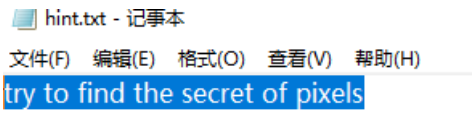
两次解密后出现flag

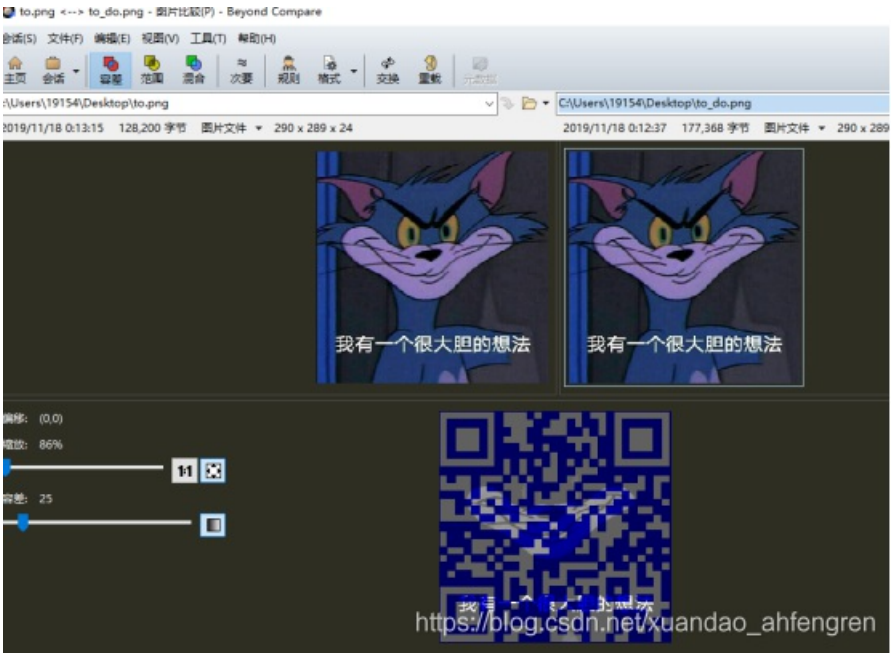
a_good_idea

用010editor打开，发现有txt文件，果断改成zip文件把文件压缩出来



然后根据hint.txt的提示，我们用BeyondCompare将两张图片进行比较发现二维码，扫描得出flag





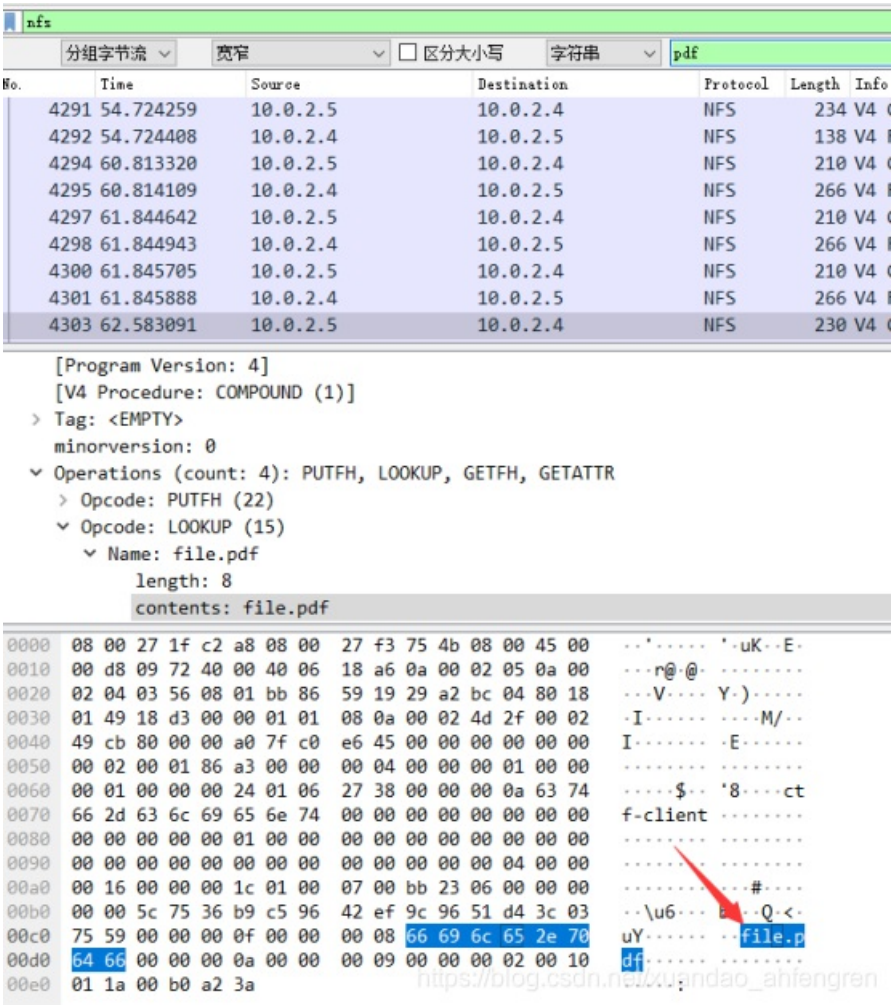
2017_Dating_in_Singapore

估计题目描述我们知道每两位数对应号数一共有十二组，我们将他们连接起来得到flag

HITB{CTFFUN}

simple_transfer

我们发现nfs包中看到了pdf文件，那我们就把文件分离出来



foremost -T 文件名即可分离

打开pdf文件即可获取flag