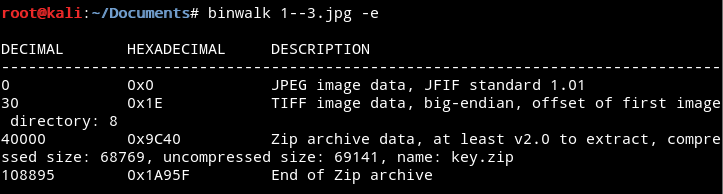
## 1. Tips:答案是与一部动漫名字有关的小写英文字母。

**flag格式：NSFOCUS{xxx}**

先用binwalk看下，顺便把里面的压缩包分离出来：



得到key.zip。发现压缩包里面有密码。

办法一：直接爆破压缩包。

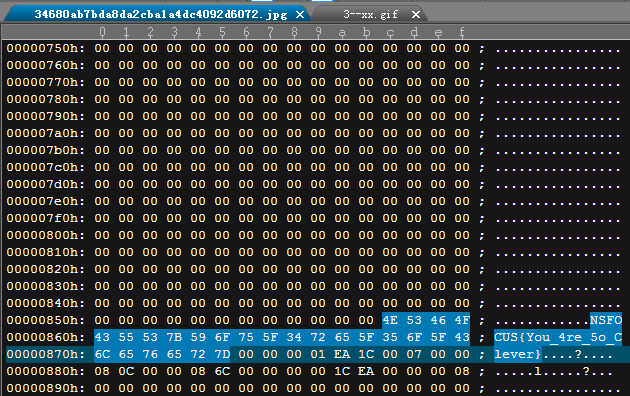
办法二：用UE或者Winhex打开，可以看到开头是FFD8，是个jpg来的，将后缀修改为.jpg，打开之后发现是张龙珠图片倒过来，所以flag为龙珠英文反过来写。

Flag：NSFOCUS{llabnogard}

## 2. Tips:听说到处都是提示。

**flag格式：NSFOCUS{xxx}**

压缩包有密码，文件名提示是生日。生成一个生日的字典进行爆破，可以获得密码是19990908。解压，里面是张图片。用UE打开图片，可以看到flag：NSFOCUS{You\_4re\_5o\_Clever}



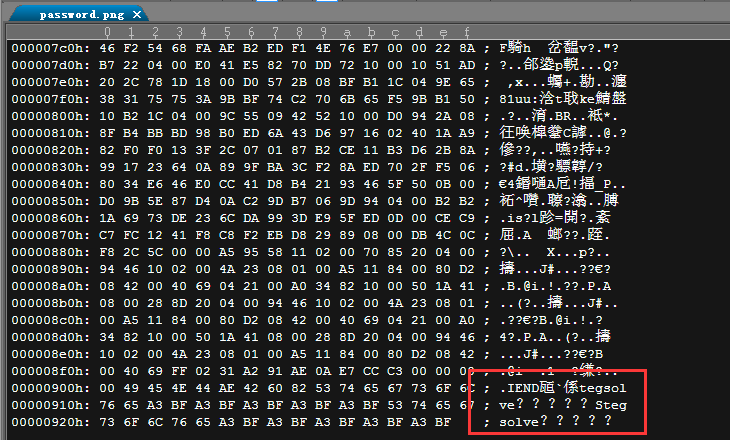
## 3 这个动图为啥打不开？？？？？

**flag格式：NSFOCUS{xxx}**

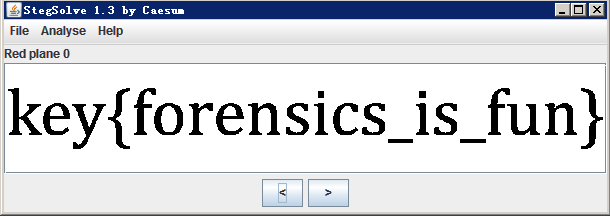
UE打开文件，发现缺少了GIF头，补上头部合成GIF89a之后可以打开gif图片。然后用Stegsolve查看每一帧，拼起来得到：key is：dGhpcyBpcyBhIGdpZg==，将这串字符进行Base64解码得到：this is a gif，所以flag为：NSFOCUS{ this is a gif }

## 4. Tips:压缩包的密码就藏在这幅白色图片中，仔细找找看吧。

解压出来是一个password.png，一张白色的图片，还有一个zip.zip。UE打开图片，最后有提示使用Stegsolve：



于是用Stegsolve打开，查看每一个RGB层，发现：key{forensics\_is\_fun}



那么压缩包的密码显然为：forensics\_is\_fun，解压压缩包看到a.gif。无法预览但是有缩略图。使用Stegsolve打开gif，然后查看每一帧，可以看到CTF{AS3X}

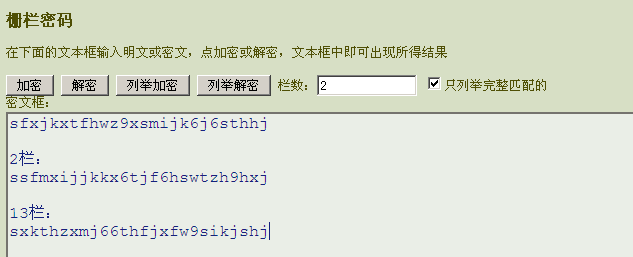
所以Flag为：CTF{AS3X}

## 5. 凯撒困在栅栏里了,需要你的帮助。

**sfxjkxtfhwz9xsmijk6j6sthhj**

**flag格式：NSFOCUS{xxx}，以及之前的格式**

先用密码机器进行栅栏解密：



然后使用脚本进行凯撒解密：

lstr="""sxkthzxmj66thfjxfw9sikjshj"""

for p in range(127):

str1 = ''

for i in lstr:

temp = chr((ord(i)+p)%127)

if 32<ord(temp)<127 :

str1 = str1 + temp

feel = 1

else:

feel = 0

break

if feel == 1:

print(str1)

在得到的结果中有一种情况与答案相近：nsfocushe11ocaesar4ndfence

所以flag为：NSFOCUS{he11ocaesar4ndfence}

## 6. 听说都是套路。

**. . -.-. ...- -. --- . .-.. ..-. ..**

**flag格式：NSFOCUS{xxx}**

摩斯密码，解密得到eecvnoelfi

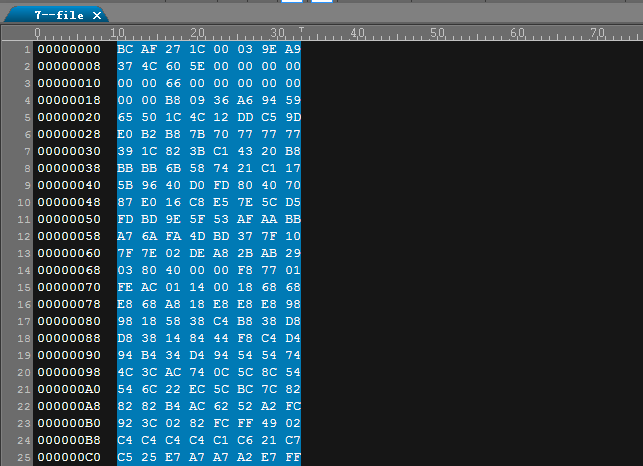
Flag：NSFOCUS{eecvnoelfi}

## 7. 文件坏了，你能帮我找回flag么？

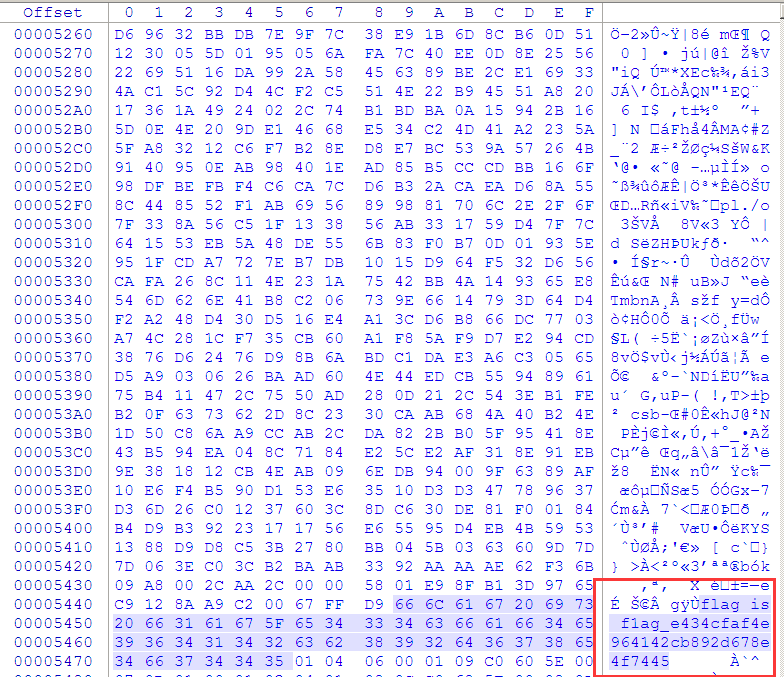
**Tips:听说都是套路。**

**flag格式：NSFOCUS{xxx}**

UE打开文件，然后列复制十六进制部分：



十六进制粘贴到Winhex中：



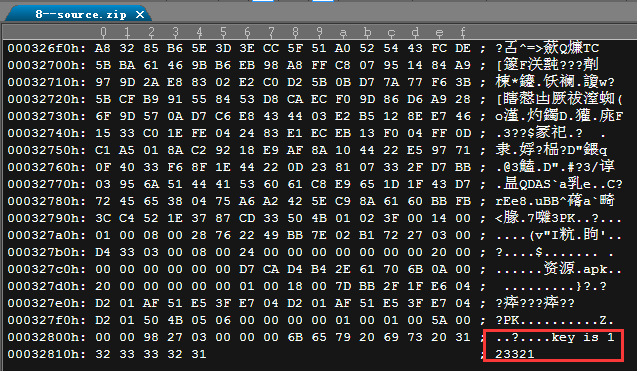
最后面可以看到flag：flag is f1ag\_e434cfaf4e964142cb892d678e4f7445

NSFOCUS{ f1ag\_e434cfaf4e964142cb892d678e4f7445}

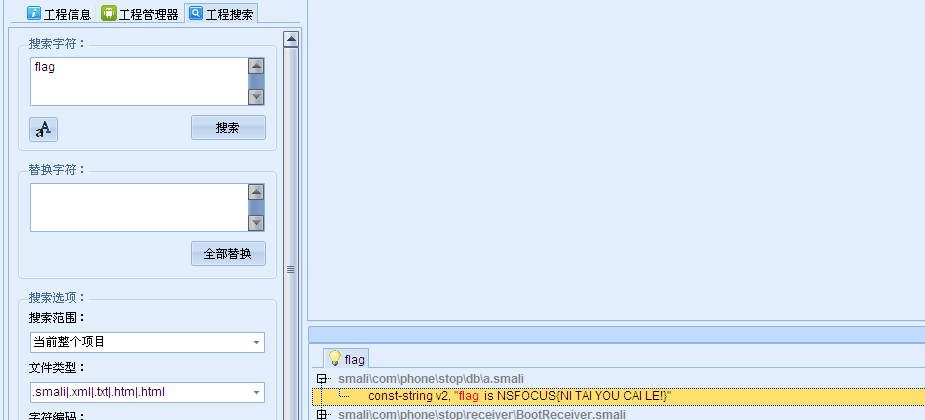
## 8. 最近收到了个资源app，分享给你，你懂的。

**解压密码你懂的！！！**

**flag格式：NSFOCUS{xxx}**

UE打开压缩包拉到最后就可以看到key：123321

解压之后用Android Killer打开，搜索字符串就可以了：



Flag：NSFOCUS{NI TAI YOU CAI LE!}

## 9. 猜猜这是多少次base加密.....

**flag格式：NSFOCUS{xxx}**

脚本：

import base64

a= base64.b64decode('...') #题目字符串

while True:

a = base64.b64decode(a)

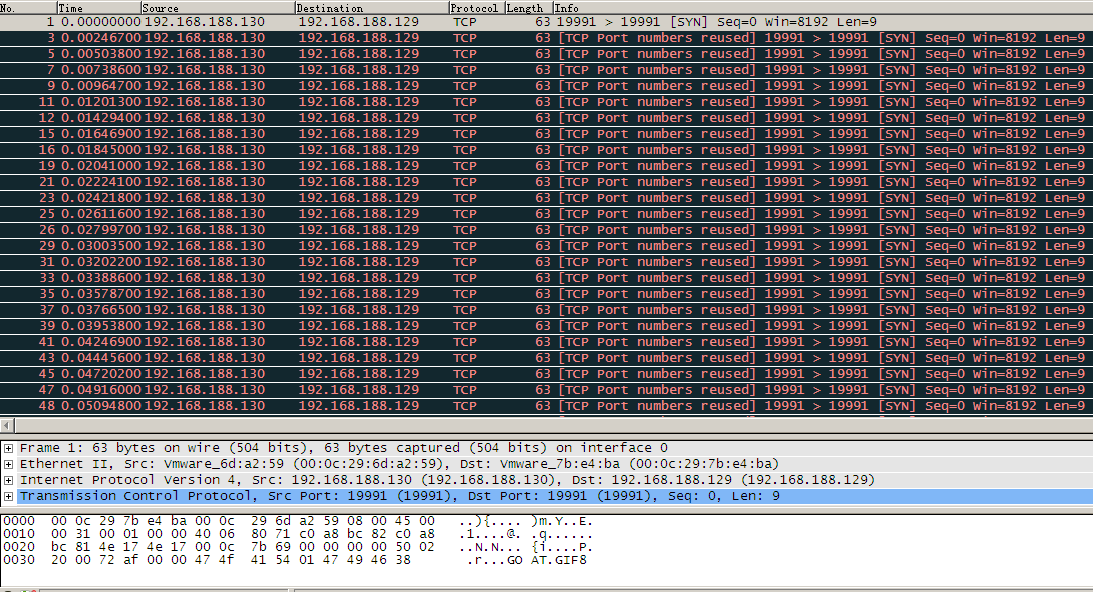
print a

print a

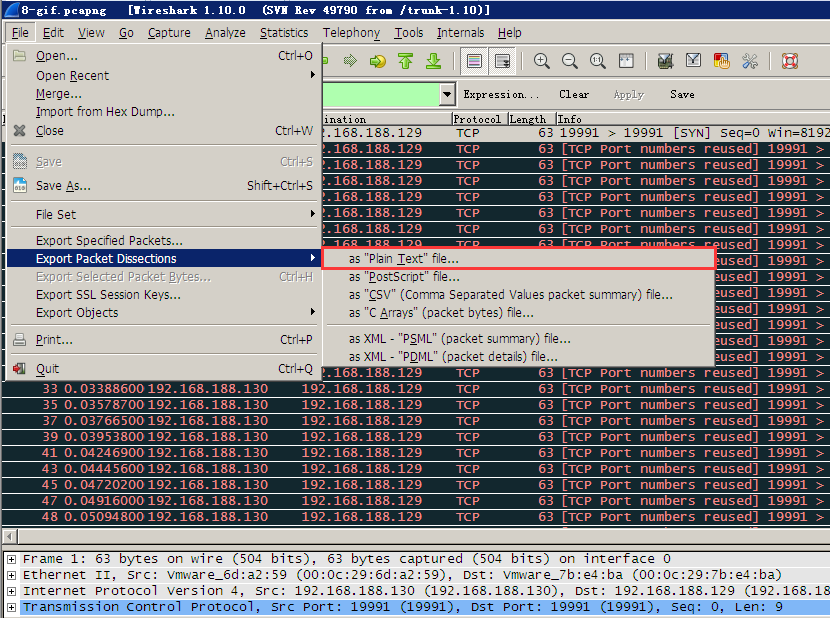
Flag：NSFOCUS{flag\_f67c2bcbfcfa30fccb36f72dca22a817}

## 10. 小明弄丢了文件，他找到下载的数据包，你能帮帮他么？

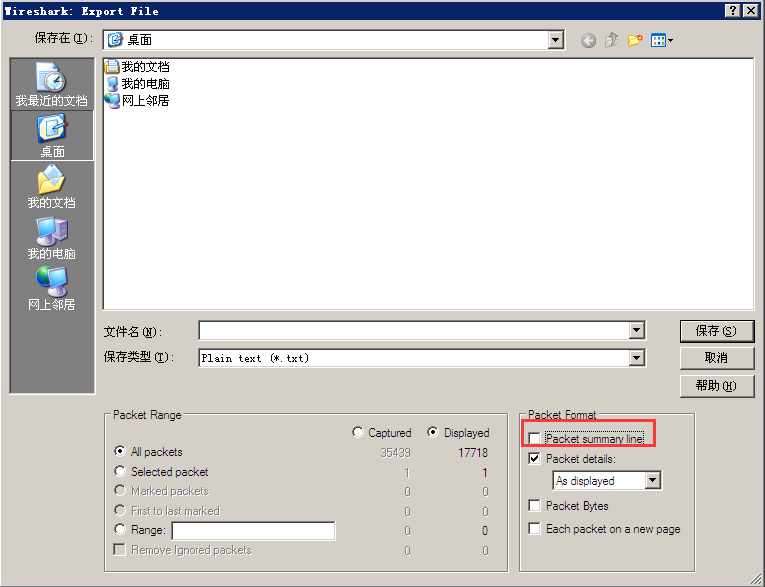
打开gif.pcapng，分析数据包，发现是通过syn为1的包进行数据传输，传输数据是一个gif。Wireshark的过滤器设置为tcp.flags.syn==1：



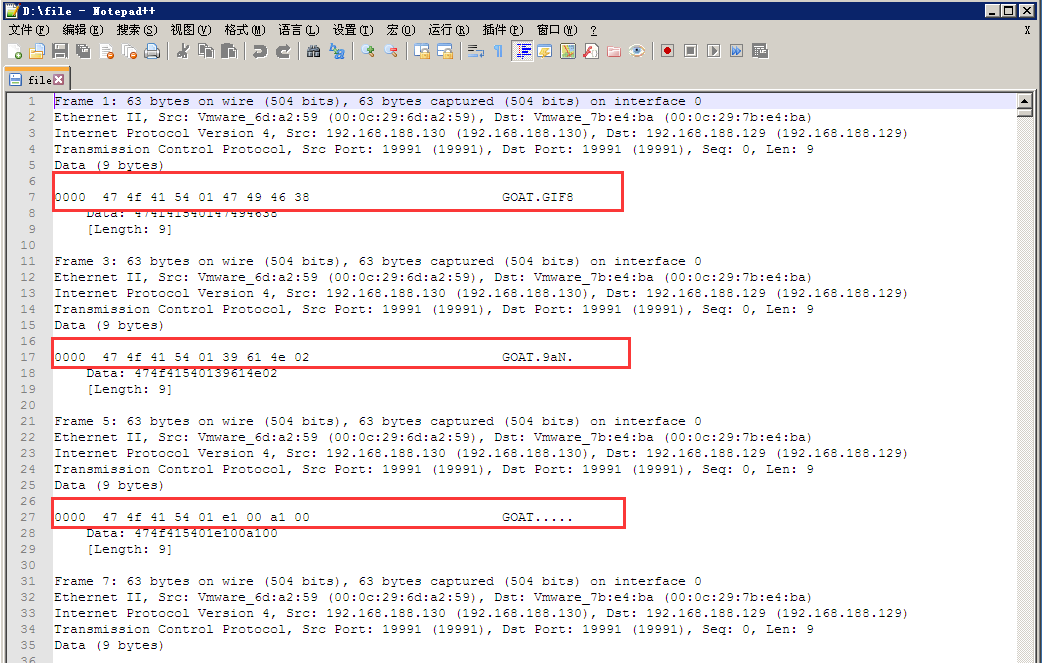
接着将分组解析结果导出：



这里Packet summary line可以不勾选：



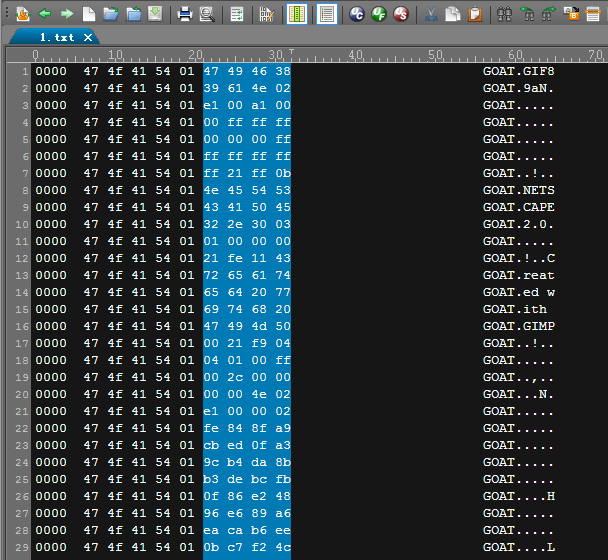
保存成file。打开：



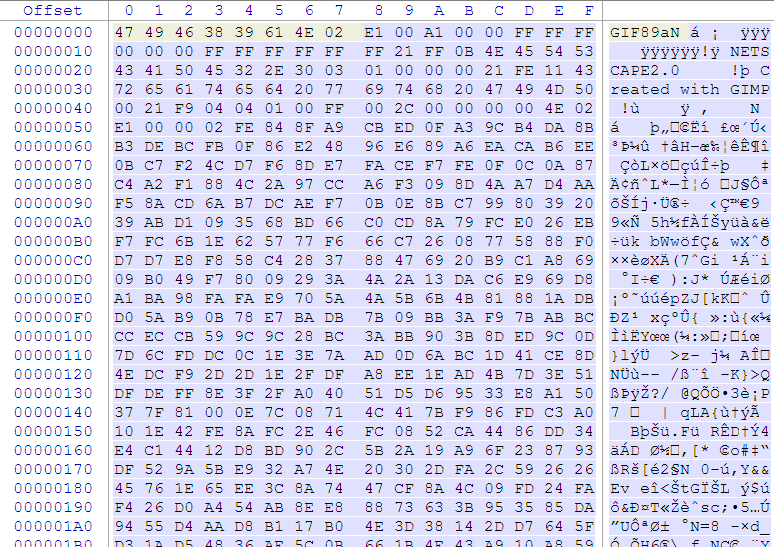
红框的部分的一部分数据就是我们想要的。用linux处理一下文件：

root@kali:~/Documents# cat file | grep "47 4f 41 54" > 1.txt

然后用UE打开1.txt，用列模式抠出数据部分的Hex：

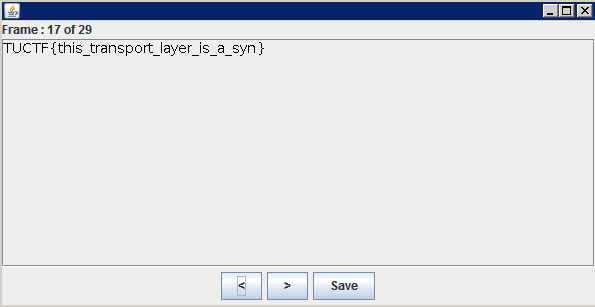


复制到winhex中：



然后保存就是一个gif了。

用Stegsolve打开gif，然后查看帧，可以看到flag：



Flag:TUCTF{this\_transport\_layer\_is\_a\_syn}

## 11. 小明喜欢X站，找到站长的加密密码了(269330a3a6ad86f0d7574b78a9a637e6)，但是他不知道原密码，你能帮帮她么？

**tips：站长喜欢用键盘记密码，比如以前用过asdf13573348998fdsa，不过他换号了，小明需要你....**

**tips2:小明说他找到新手机号是133\*\*54\*\*33**

**flag{站长的密码}**

脚本：

import hashlib

s1 = 'asdf133'

s2 = '33fdsa'

s3 = '54'

for i in range(0,100):

for j in range(0,100):

str1 = s1 + str(i) + s3 + str(j) + s2

m = hashlib.md5()

m.update(str1)

res = m.hexdigest()

if res == '269330a3a6ad86f0d7574b78a9a637e6':

print i

print j

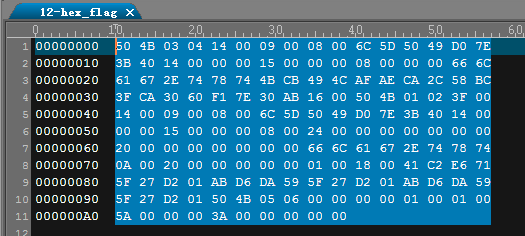
运行得到i=33，j=33

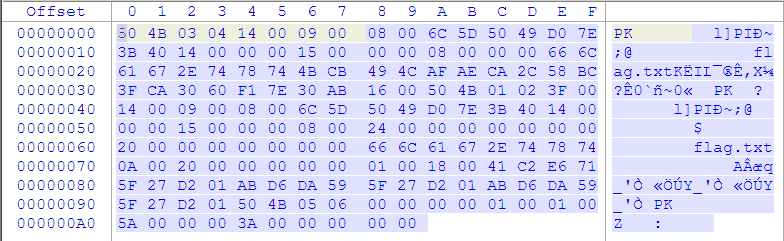
所以手机号为13333543333，密码为asdf13333543333fdsa。

Flag：flag{asdf13333543333fdsa}

## 12. hex-flag

UE打开，列复制十六进制部分到winhex：





可以看出这是一个zip文件。重命名为1.zip。发现压缩包有密码，尝试是否为伪加密，使用工具去掉伪加密：



之后发现里面文件可以打开：flag{zip？Z1P？zip？}

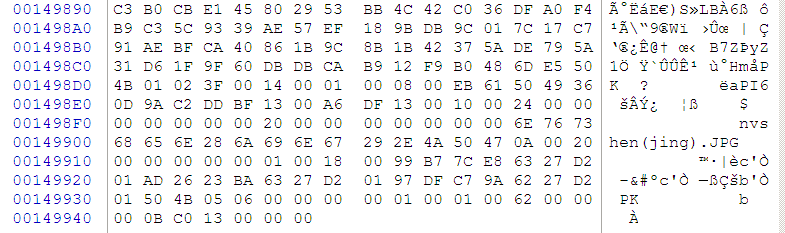
## 13. 女神走丢了。你能帮我找到她么？

**flag{女神的坐标}**

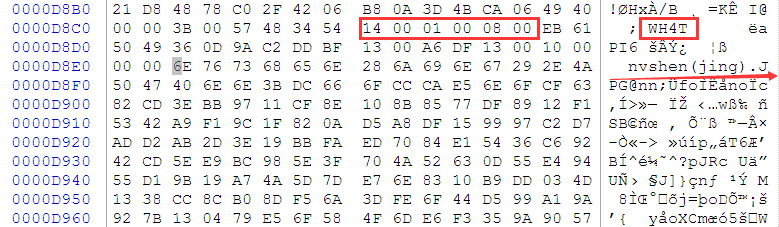
**like:flag{12;11;11.11---111;11;0.11}**

**精确小数后两位即可，如存在，需四舍五入**

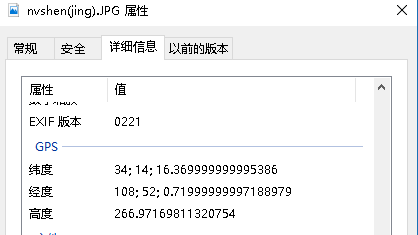
用Winhex打开gif，发现文件的最后有个nvshen(jing).jpg，还有zip文件的末尾504B0506等。猜想有个zip文件。



于是往前查找nvshen



果然前面又出现了一次，这里应该就是压缩文件的头了。观察140001000800应该是zip头在504B0304之后。WH4T应该是压缩包的密码。于是从1400之后到末尾抠出来到新文件，补上开头504B0304，然后将将14000100改成14000000（去掉zip的伪加密），重命名为zip后缀。打开之后，解压密码为上面看到的WH4T。解压出图片之后，根据题目的要求，找坐标。查看图片详情：



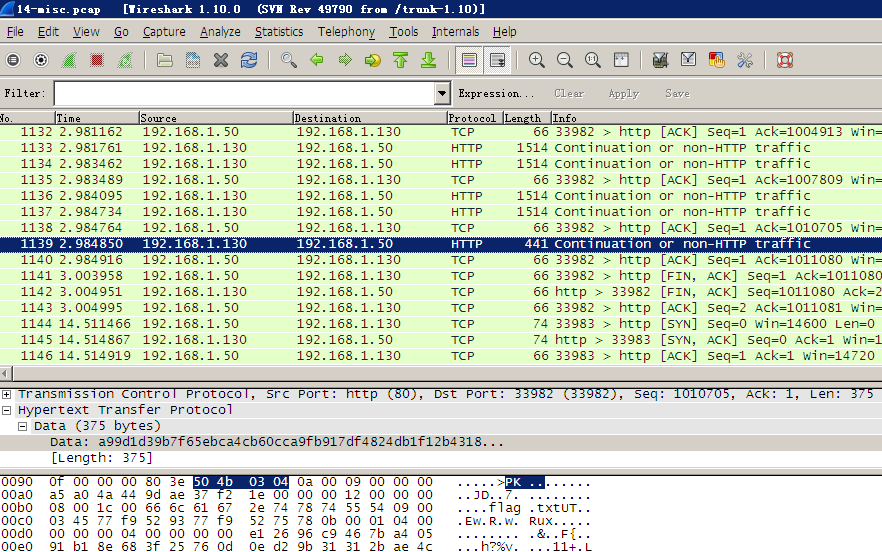
那么flag{34;14;16.37---108;52;0.72}

## 14. flag is flag{xxxx}

分析http流的时候很容易发现有个secret.txt，打开之后可以看到内容：the password for zip file is : ZipYourMouth

那么接下来就是找zip了。然后可以发现上面有个flag.zip，尝试提取出来。发现提取出来是坏的，用winrar无法修复。

在pcap文件中直接查找zip文件头Hex：504B0304，可以发现在1139行还有一个zip。里面有个flag.txt。



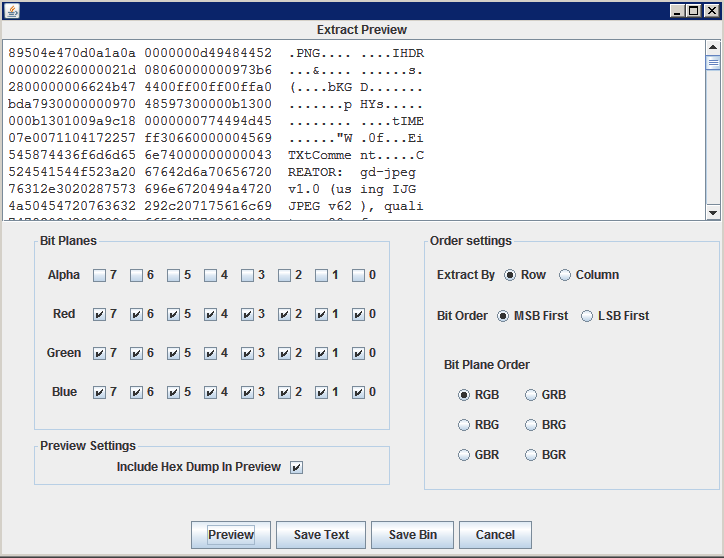
提取出来之后，用winrar修复，根据上面找到的压缩包密码就可以解压了。打开就是flag：Flag-qscet5234diQ。

Flag：flag{ qscet5234diQ}

## 15. ting shuo he xiang su you guan

**flag is flag{xxxx}**

使用Stegsolve打开图片，然后在RGB有数据的位都勾上：



可以看出这是一张PNG图片，保存成bin文件，然后重命名为1.png。Flag在图片里：



IceCTF{puT\_Th4t\_1n\_yoUr\_cOlOrng\_Book\_4nD\_5moKe\_1T}

## 16. 答案非标准格式，提交前加上flag{}

**yhnhjm ytfvbh wsxdrfvgy resxcfv tgvgy dfresxc yhnhu oijm,l uhbnmko**

键盘密码：h o w a r e y o u

Flag：flag{howareyou}