XCTF攻防世界_Misc练习区

原创

FAFU小宋 于 2020-10-29 23:28:34 发布 173 收藏

分类专栏： XCTF 文章标签： 安全

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/FAFUxiaosong/article/details/109367414

版权

XCTF 专栏收录该内容

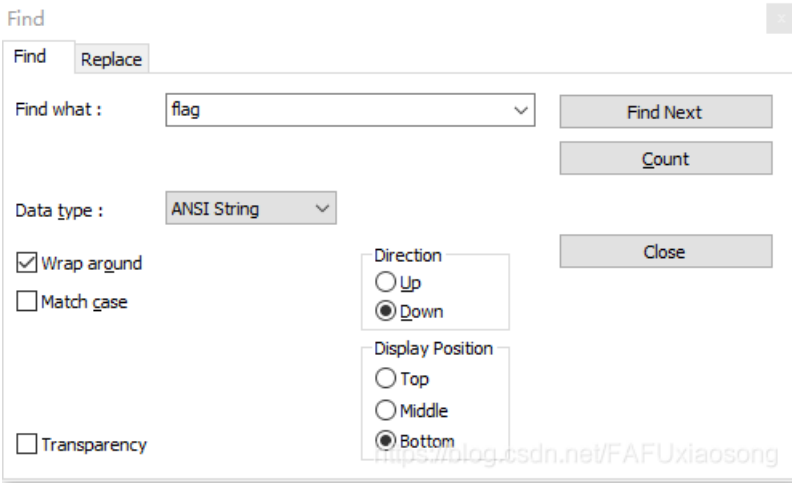
9 篇文章 0 订阅

订阅专栏

XCTF_Misc_新手练习区

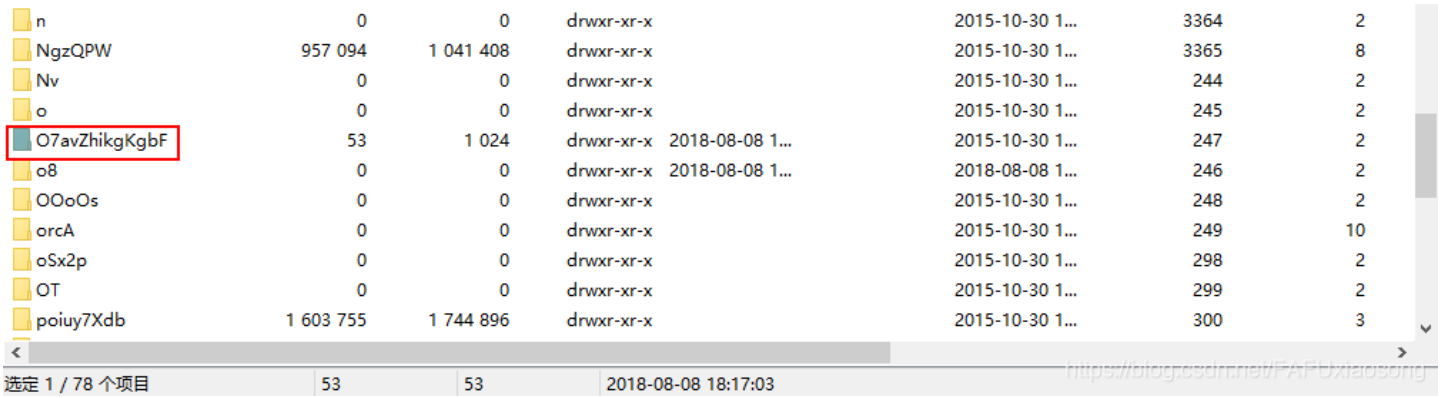
ext3

(1)附件是一个没有后缀的文件，使用notepad++打开，Ctrl+F出现搜索框，搜索flag




```
00680460  00 00 00 00 00 00 00 00 00 00 00 00 7e 72 6f 6f ............~roo
00680470  74 2f 44 65 73 6b 74 6f 70 2f 66 69 6c 65 2f 4f t/Desktop/file/O
00680480  37 61 76 5a 68 69 6b 67 4b 67 62 46 2f 66 6c 61 7avZhikgKgbF/fla
00680490  67 2e 74 78 74 00 00 00 00 00 00 00 00 00 00 00 g.txt.........
006804a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

（2）发现在O7avZhikgKgbF目录下有个flag文件，用7-ZIP工具打开附件，找到flag.txt文件。



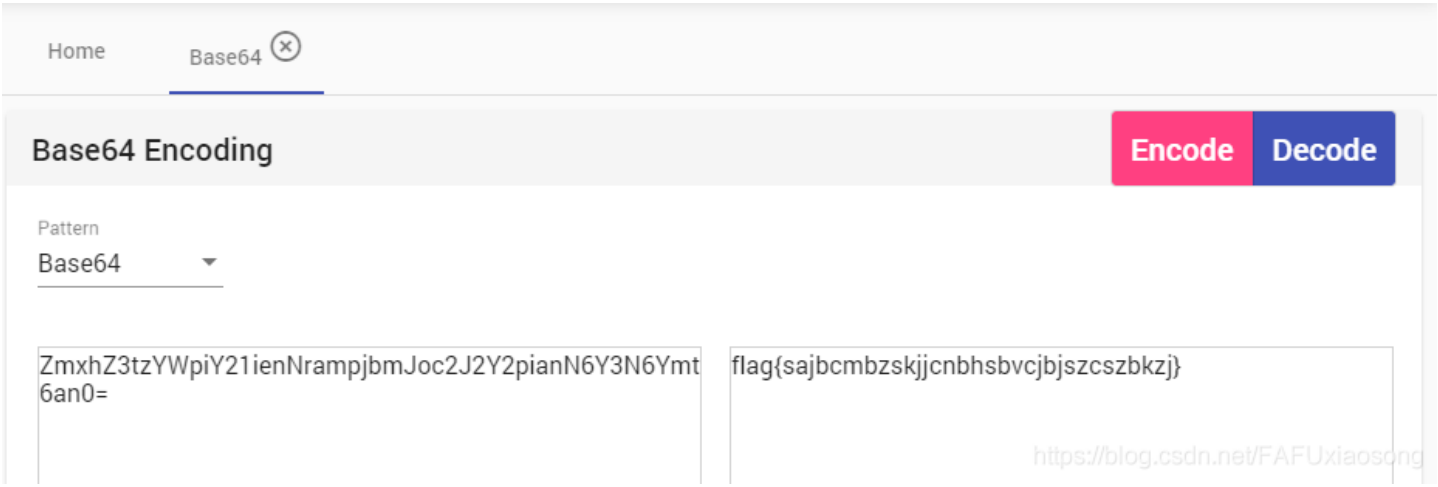
n	0	0	drwxr-xr-x	2015-10-30 1...	3364	2
NgzQPW	957 094	1 041 408	drwxr-xr-x	2015-10-30 1...	3365	8
Nv	0	0	drwxr-xr-x	2015-10-30 1...	244	2
o	0	0	drwxr-xr-x	2015-10-30 1...	245	2
O7avZhikgKgbF	53	1 024	drwxr-xr-x 2018-08-08 1...	2015-10-30 1...	247	2
o8	0	0	drwxr-xr-x 2018-08-08 1...	2018-08-08 1...	246	2
OOoOs	0	0	drwxr-xr-x	2015-10-30 1...	248	2
orcA	0	0	drwxr-xr-x	2015-10-30 1...	249	10
oSx2p	0	0	drwxr-xr-x	2015-10-30 1...	298	2
OT	0	0	drwxr-xr-x	2015-10-30 1...	299	2
poiuy7Xdb	1 603 755	1 744 896	drwxr-xr-x	2015-10-30 1...	300	3

选定 1 / 78 个项目 53 53 2018-08-08 18:17:03

https://blog.csdn.net/FAFUxiaosong

名称	大小	压缩后大小
flag.txt	53	1 024

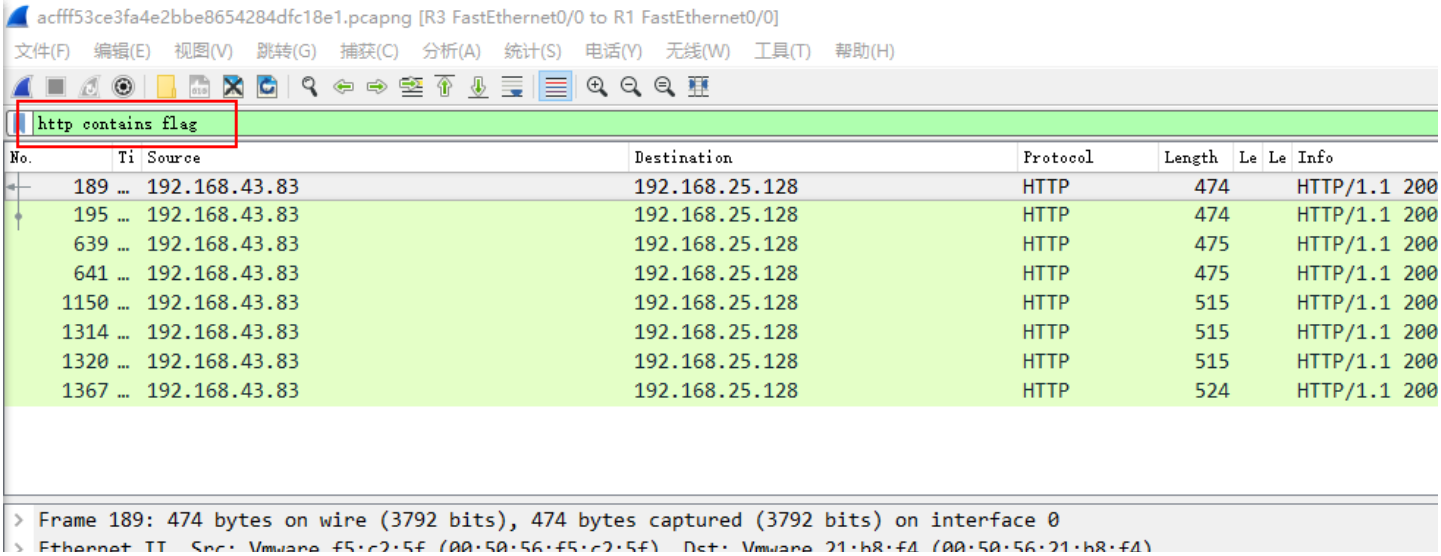
（3）出现了一串base64加密的字符串，这里我用的是CaptfEncoder工具，解码后得flag{sajbcmbzskjjcnbhsbvcjbjszcszbkzj}



https://blog.csdn.net/FAFUxiaosong

功夫再高也怕菜刀

（1）附件是一个.pcapng文件，使用Wireshark打开文件查看报文查找flag信息，输入表达式http contains flag查看http协议的报文是否包含flag 的信息



```
Internet Protocol Version 4, Src: 192.168.43.83, Dst: 192.168.25.128
Transmission Control Protocol, Src Port: 80, Dst Port: 47844, Seq: 346, Ack: 1873, Len: 420
Hypertext Transfer Protocol
Line-based text data: text/html
```

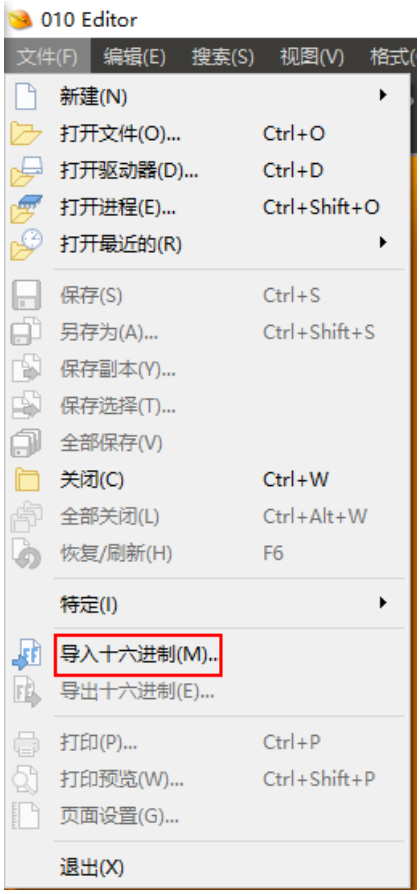
https://blog.csdn.net/FAFUxiaosong

（2）根据筛选出的报文，追踪tcp流，在第1150个报文中发现一串十六进制的流信息，其中，FFD8是jpg文件头标志，FFD9是结束标志，说明这里有一张jpg格式的图片。

```
k%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDp
cd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE00010
4A4649460001010100780078000FFDB00430001010101010101010
1010101010101010101010101010101010101010101010101010101
0101010101010101010101010101010101010101010101010101010
1FFDB00430101010101010101010101010101010101010101010101
```

```
DE4F5F4EDBD97BBA2E9A7F2A3E830EB45E89F7DD41EBD5FC7AF7F7B
AC9B59E658327293B9CF2E1BEF7FB5FF02EBF8D15763FF571FF00B8
BFFA08A2B86DFE1FFC05797F93FBFEFE9E65DA5FF81BFF002F5FE96
FFD9HTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:07 GMT
```

（3）将这部分信息复制到一个文本文档.txt中保存，用010 editor工具以十六进制导入，并另存为jpg格式，得到一张图片



https://blog.csdn.net/FAFUxiaosong

（4）接着在kali中用foremost分离附件.pcapng文件，得到一个zip文件，里面有一个压缩包，包含flag文件。使用上面图片中的“Th1s_1s_p4sswd_!!!”作为密码，获取flag。

#foremost已在kali中预安装，使用如下命令安装

```
$sudo apt-get install foremost       //非管理员需要加上sudo
```

#分离文件

```
$foremost -t all ctf.pcapng
```

#执行完上面的语句后，会生成一个output目录，进入该目录即可查看分离的文件。

give_you_flag

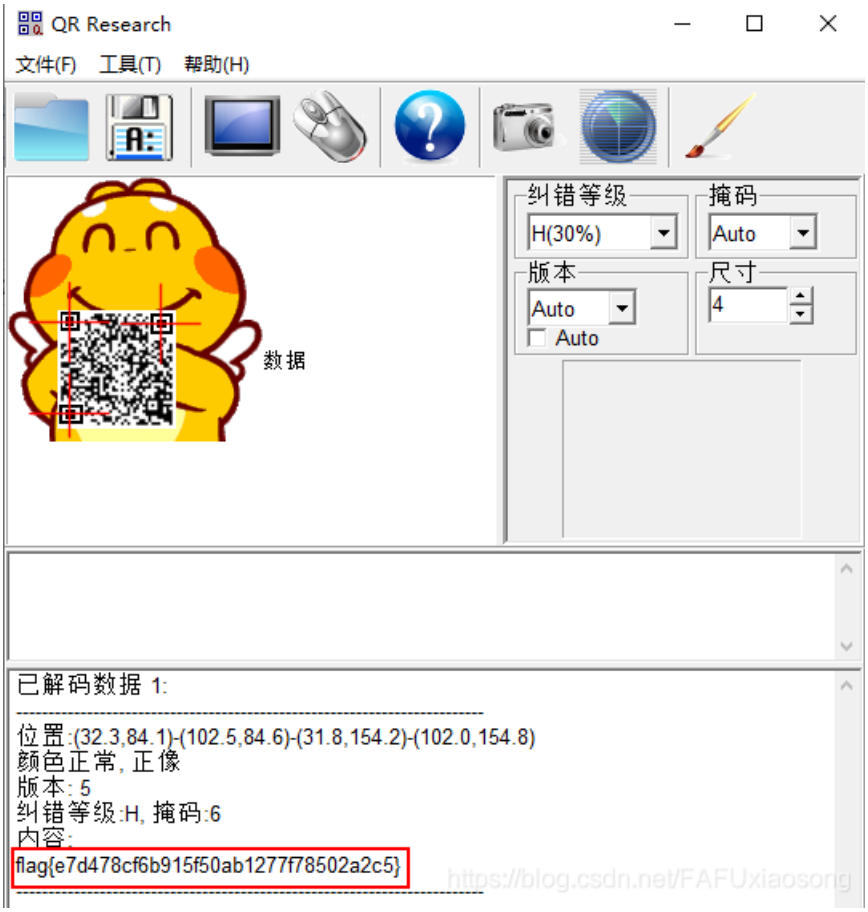
（1）附件是一张gif的动图，查看后可发现图片里存在一个二维码。于是这里用stegsolve工具将动图分解为一张张图片，以便查看。

（2）找到那张出现二维码的图片，发现定位点缺失。百度下载一张二维码定位点图片，接着打开Windows自带的画图工具，选择“新建”，然后依次把定位点图片和二维码图片通过“粘贴来源“导入，将定位点拖拽到缺失的地方，保存即可。（不会ps只能这样了，嘤嘤嘤~）

#下载的定位点图片可能会有一些白色边框，在合成图片时可能会覆盖掉二维码。同样可以在画图工具里，打开定位点图片，通过多次“旋转”的操作，然后不断调整白色画布的大小去掉边框，去掉边框后保存就可以了。

https://blog.csdn.net/FAFUxiaosong

（3）二维码图片补全后，用二维码扫描器扫描就可以得到flag了。



#stegsolve工具：

File Format:文件格式，这个主要是查看图片的具体信息

Data Extract:数据抽取，图片中隐藏数据的抽取

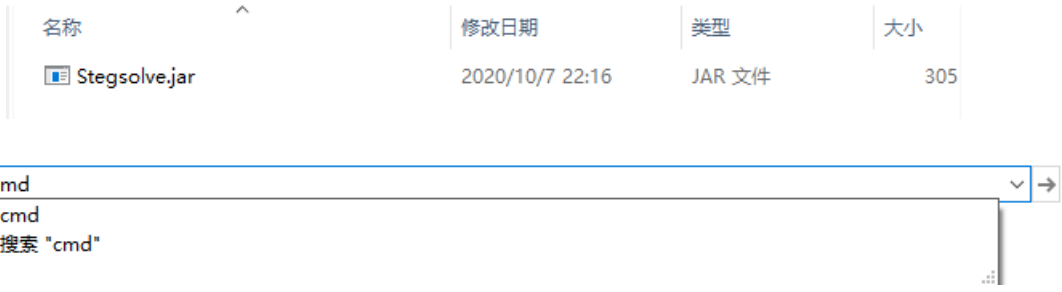
Frame Browser:帧浏览器，主要是对GIF之类的动图进行分解，动图变成一张张图片，便于查看

Image Combiner:拼图，图片拼接

#stegsolve打开方式：

（1）首先需要添加java环境，这里就不赘述了。

（2）打开stegsolve所在目录，在目录框输入cmd，打开运行窗口

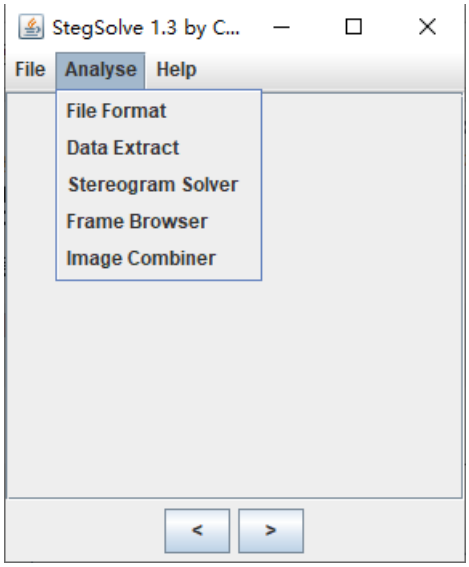


（3）在运行窗口输入以下命令即可打开：

```
java -jar stegsolve.jar
```

C:\Windows\System32\cmd.exe - java -jar stegsolve.jar

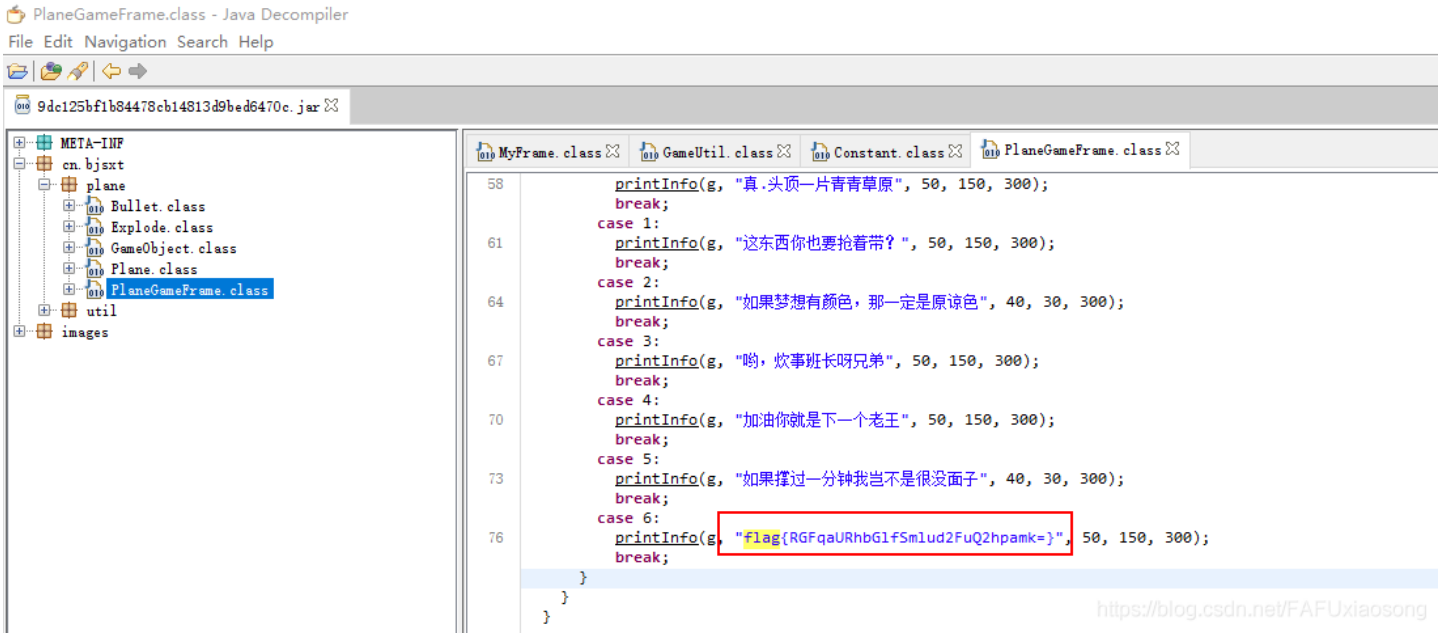
```
Microsoft Windows [版本 10.0.18362.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

D:\安全工具\Misc工具配置\数据隐写类工具>java -jar stegsolve.jar
```



坚持60s

（1）附件是一个.jar文件，在cmd下用java -jar xxxx.jar查看

（2）用jd-gui工具反编译，在cn.bjsxt.plane.PlaneGameFrame.class文件下发现flag（Ctrl+F搜索）



gif

（1）解压附件，在gif文件夹下看到许多黑白的图片，联想到二进制

（2）将各个图片转化为对应的二进制，使用在线二进制转字符串工具http://www.txttool.com/WenBen_BinaryStr.asp即可得到flag。

掀桌子

题目描述： 菜狗截获了一份报文如下c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2，生气地掀翻了桌子(╯°□°)╯┻┻

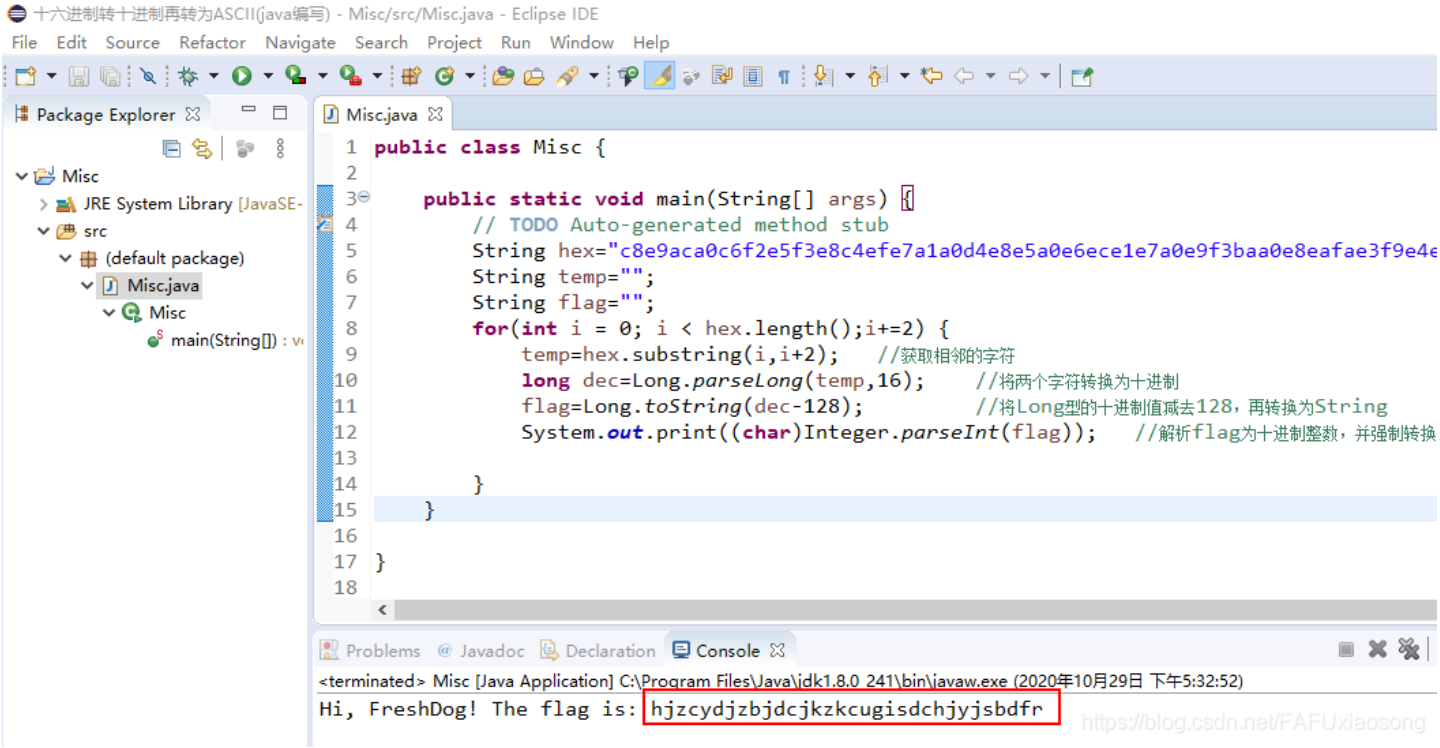
（1）获取的报文内容为0-9，a-f，考虑十六进制。但该串十六进制数无法直接转化为字符串（ASCII值）

（2）把十六进制两两一组转换为十进制；接着将十进制数减去128（因为ASCII码值为0~127），让其落到ASCII码表上，然后计算出对应ASCII码值的字符，获取flag。

（3）采用如下java编写的代码：

```
public class Misc {

 public static void main(String[] args) {
  // TODO Auto-generated method stub
  String hex="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2";
  String temp="";
  String flag="";
  for(int i = 0; i < hex.length();i+=2) {
   temp=hex.substring(i,i+2);    //获取相邻的字符
   long dec=Long.parseLong(temp,16);     //将两个字符转换为十进制
   flag=Long.toString(dec-128);          //将Long型的十进制值减去128，再转换为String
   System.out.print((char)Integer.parseInt(flag));    //解析flag为十进制整数，并强制转换为char，存取字符

  }
 }

}
```

（4）查看执行结果



如来十三掌

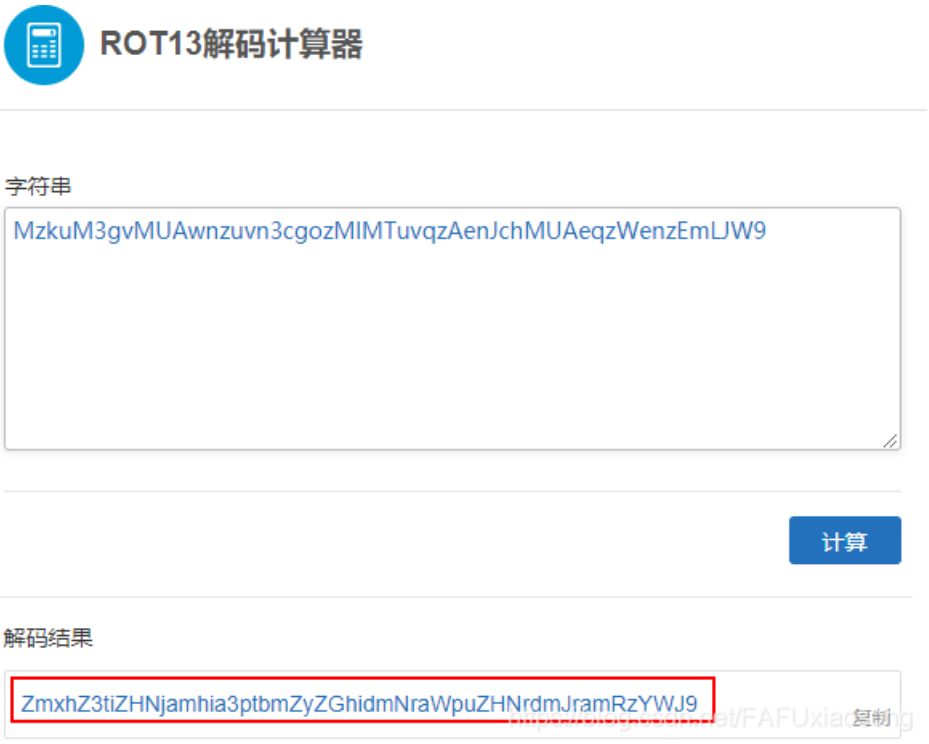
（1）附件是一串禅语

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

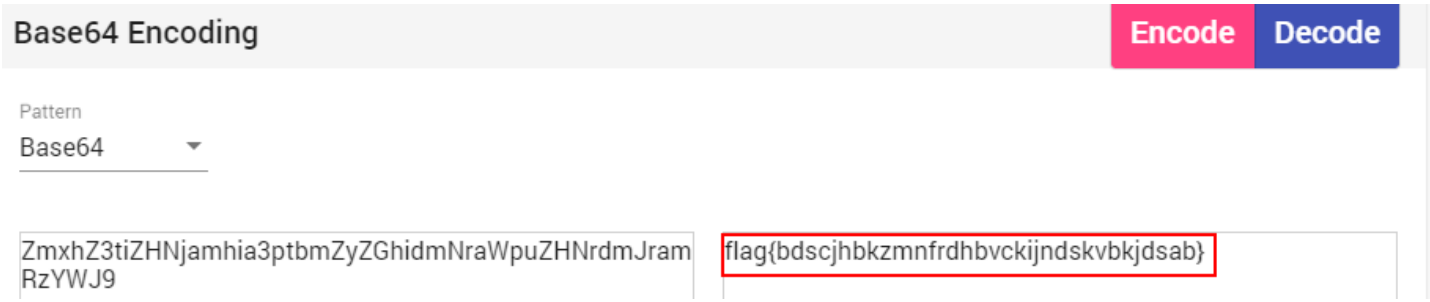
（2）使用在线工具使用“与佛论禅”来进行解码（解码时记得在原文字的开头加上“佛曰：”）在线工具：http://www.keyfc.net/bbs/tools/tudoucode.aspx

（3）根据题目提示的13掌，用rot-13解码

#rot13使用一个简单的替换加密算法，类似凯撒密码

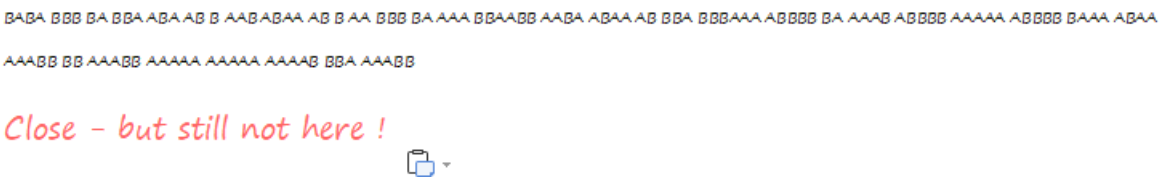


（4）又是一串密文，用base64试试，看到flag。



stegano

（1）附件是一个pdf文件，全选后复制到一个word文档里，发现了一串特殊的字符



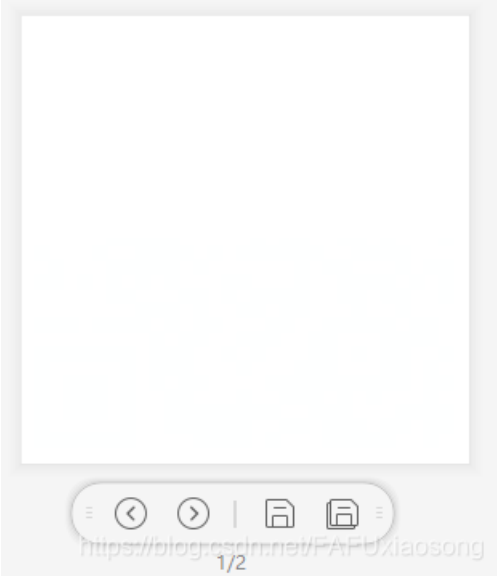
（2）看到AB，但不是培根密码，培根密码是5个一组，联想到摩斯密码将A替换为.，B替换为-，可以自己写个代码转换一下（这里我用的c语言）

```
int main(){
 char word[200];
 gets(word);
 int i=0;
 while(word[i] != 0){
  if(word[i] == 'A'){
   word[i]='.';
   printf("%c",word[i]);
  }
  if(word[i]  == ' '){
   printf(" ");
  }
  if(word[i] == 'B'){
   word[i]='-';
   printf("%c",word[i]);
  }
//  printf("%s",word[i]);
  i++;
 }

 system("pause");
 return 0;
```

（3）然后放到在线摩斯密码加解密上解密http://www.txttool.com/t/?id=Mzg1（注意分割的时候空格也要输入）

SimpleRAR

（1）解压附件得到一张两帧的图片



（2）现将这两帧图片分别保存，然后用stegsolve分别打开，发现是都是缺失一半的二维码图片

（3）利用画图工具，将两张图拼在一起，并将定位点补充完整，用二维码扫描器扫描即可

已解码数据 1:

位置:(4.2,4.9)-(258.5,0.2)-(-1.1,263.0)-(253.0,257.3)
颜色正常, 正像
版本: 3
纠错等级:H, 掩码:4
内容:
flag{yanji4n_bu_we1shi}

https://blog.csdn.net/FAFUxiaosong