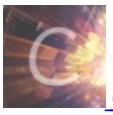
攻防世界 MISC新手练习区 刷12道题题所得的思路和方法

原创

别害怕我在 于 2021-08-17 10:41:53 发布 285 收藏 2

分类专栏： CTF杂项MISC新手

本文链接：https://blog.csdn.net/afanzcf/article/details/119750872



---

title: 攻防世界 MISC新手练习区
date: 22021年8月17日 10点31分
tags: MISC
categories: MISC

1、攻防世界 this_is_flag（签到题）

直接告诉了flag，签到题。

2、攻防世界 pdf（pdf转word、直接复制）

（1）方法一

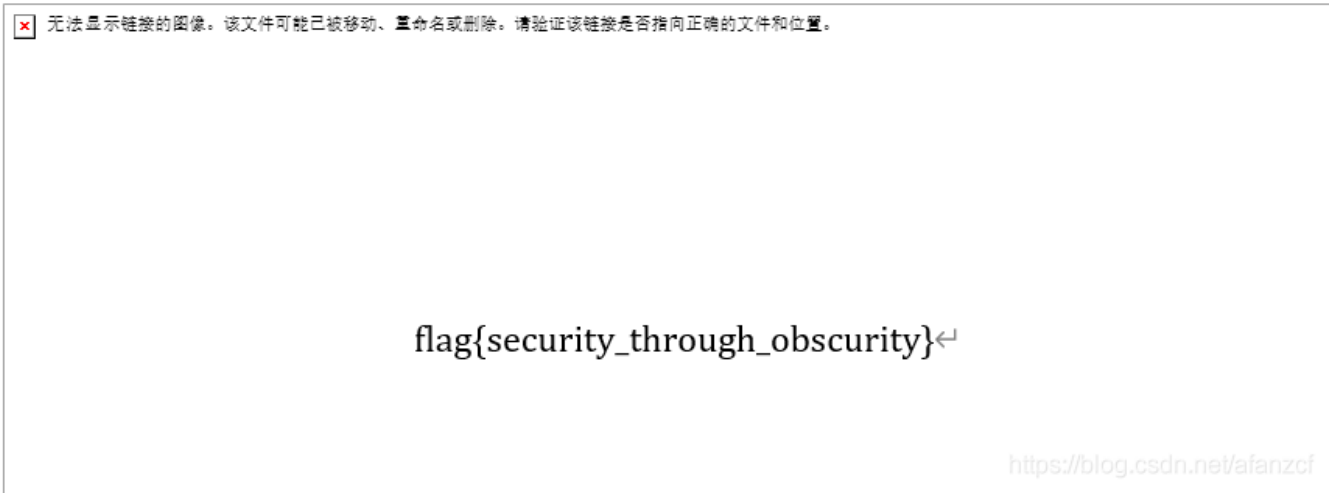
给的是一个pdf，打开之后，在图片中间能用鼠标选中字符，直接全选复制，粘贴就出来了。

flag{security_through_obscurity}

（2）方法二

PDF转Word——免费在线pdf转换成word文档 (pdfdo.com)

利用在线网站，在线pdf转为word，然后打开word。



3、攻防世界 如来十三掌（与佛论禅、rot13、base64）

给的是一个word，打开。

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鉢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鉢三死怯摩大蘇者數一遮↵

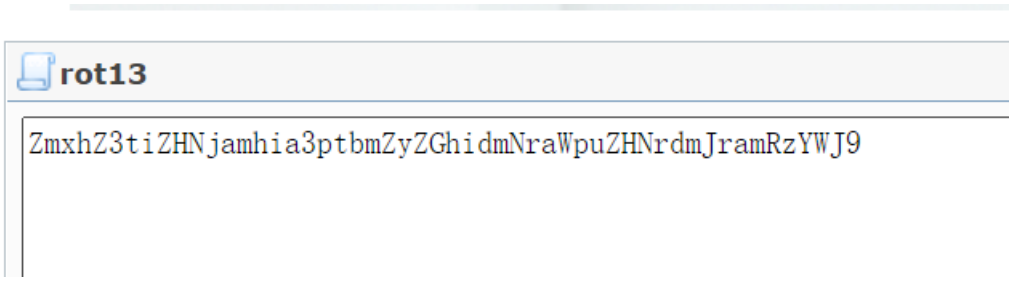
夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多鉢以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

之前知道类似的佛语。于是去与佛论禅的网站解密。
与佛论禅

记得在佛语前面加上佛曰：

然后得到的这一串字符，将之rot13解密，得到

网络管理员在线工具 - Rot13 (mxcz.net)




```
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9
```

然后，再base64解密。

Base64 在线编码解码 | Base64 加密解密 - Base64.us

得到flag。

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

rot13：
套用ROT13到一段文字上仅仅只需要检查字元字母顺序并取代它在13位之后的对应字母，有需要超过时则重新绕回26英文字母开头即可。A换成N、B换成O、依此类推到M换成Z，然后序列反转：N换成A、O换成B、最后Z换成M。只有这些出现在英文字母里头的字元受影响；数字、符号、空白字元以及所有其他字元都不变。因为只有在英文字母表里头只有26个，并且26=2×13，ROT13函数是它自己的逆反。

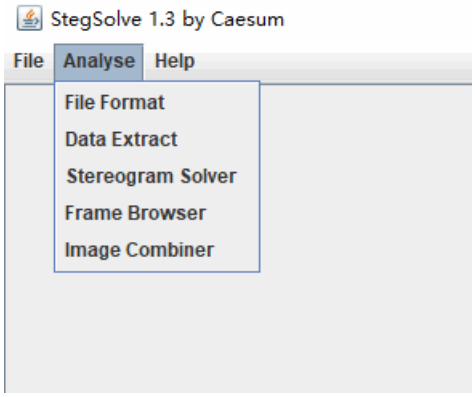
base64：
1.标准base64只有64个字符（英文大小写、数字和+、/）以及用作后缀等号；
2.base64是把3个字节变成4个可打印字符，所以base64编码后的字符串一定能被4整除（不算用作后缀的等号）；
3.等号一定用作后缀，且数目一定是0个、1个或2个。这是因为如果原文长度不能被3整除，base64要在后面添加\0凑齐3n位。为了正确还原，添加了几个\0就加上几个等号。显然添加等号的数目只能是0、1或2；
4.严格来说base64不能算是一种加密，只能说是编码转换。使用base64的初衷。是为了方便把含有不可见字符串的信息用可见字符串表示出来，以便复制粘贴；

4、攻防世界 give_you_flag（stegsolve工具、二维码）

给的是一个gif动图。

stegsolve下载地址：http://www.caesum.com/handbook/Stegsolve.jar

配置好java环境之后，在命令行输入java -jar Stegsolve.jar 打开stegsolve



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

使用Frame Browser之后，会得到一张二维码图片，但是缺少了三个角，补全三个角之后，扫出来就是flag。

5、攻防世界 stegano（摩斯密码）

给的是一个pdf，打开之后。

interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam[Your flag is not here]olestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet *magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc* diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum

直接全选复制，到文本下粘贴。

NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Close - but still not here !
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at

就能看到一串AB，一开始以为是培根密码，但是培根密码是五个一组，然后想到摩斯密码，将B换为-，A换为. 手换容易出错，自己写了一个脚本。

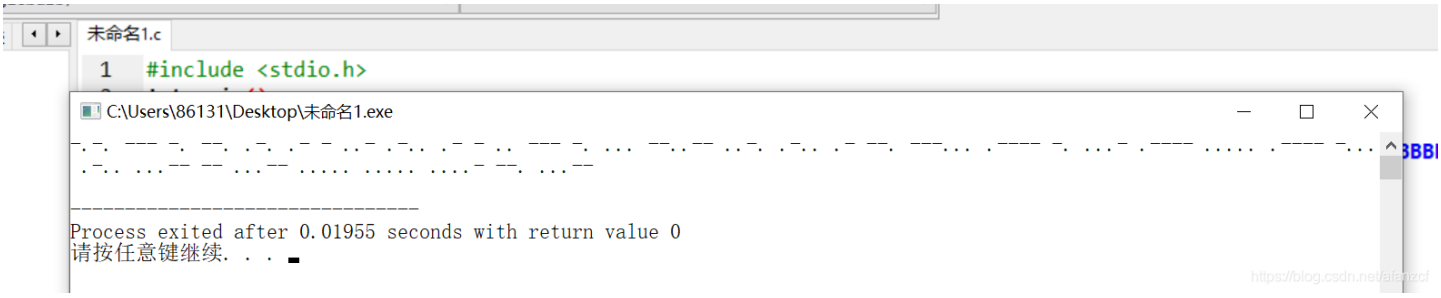
```c
#include <stdio.h>
int main()
{
    char str[] ="BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABB
    int i = 0;
    for(i = 0; i<200; i++)
    {
        if(str[i] == 'A')
        {
            str[i] = '.';
        }
        else if(str[i] == 'B')
        {
            str[i] = '-';
        }

    }
    printf("%s\n", str);
    return 0;
}
```



```c
#include <stdio.h>
int main()
{
 char str[] ="BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB
ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB" ;
 int i = 0;
 for(i = 0; i<200; i++)
 {
  if(str[i] == 'A')
  {
   str[i] = '.';
  }
  else if(str[i] == 'B')
  {
   str[i] = '-';
  }

 }
 printf("%s\n", str);
 return 0;
}
```




```
-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .-
--- -... .-.. ...-- -- ...-- ..... ..... ....- --. ...--
```

在线摩斯密码解密。

摩斯电码转换_摩斯密码翻译器-在线工具 (all-tool.cn)

分割为空格，得到flag，再根据题目提示需要小写，得到flag{1nv151bl3m3554g3}

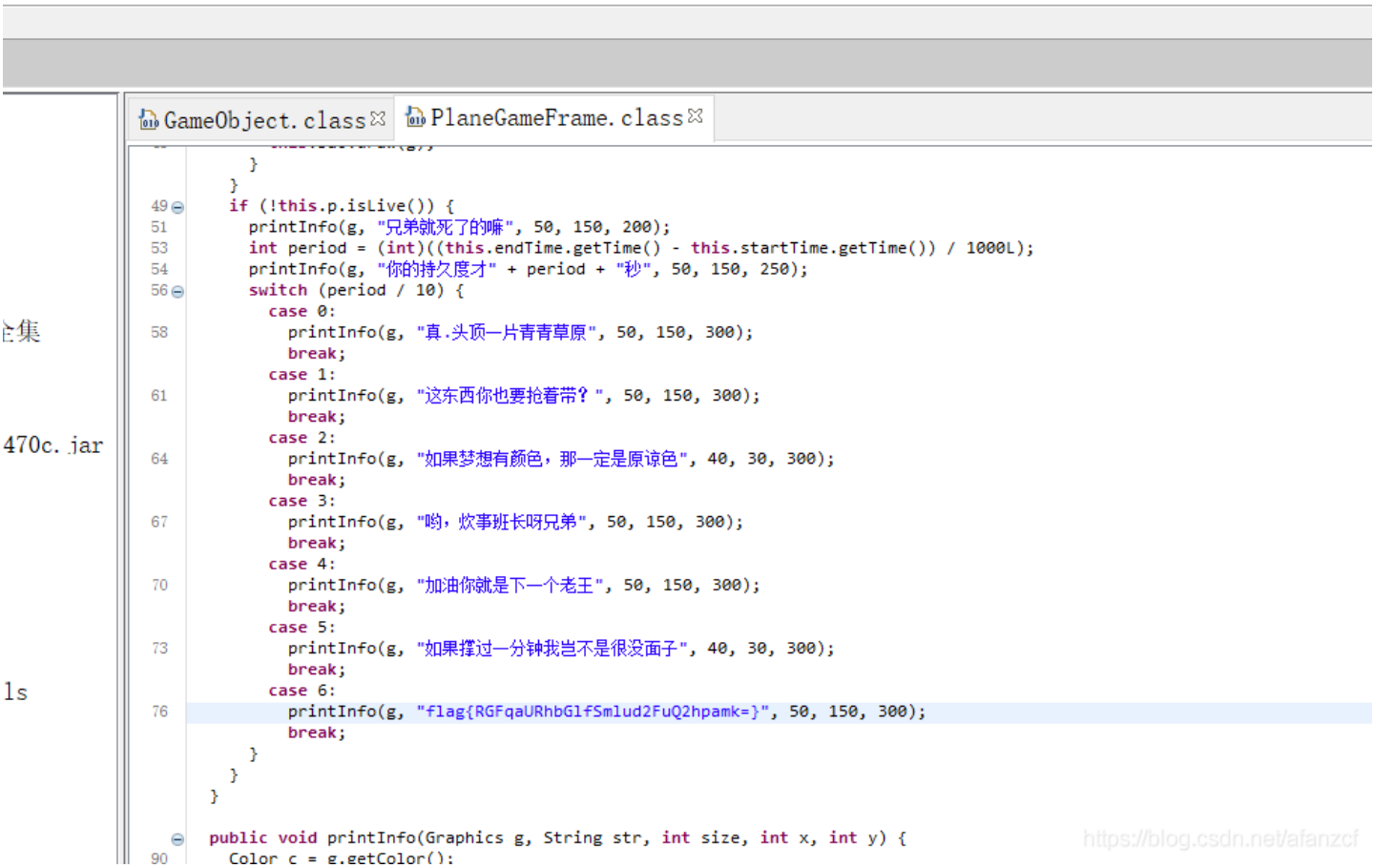
6、攻防世界 坚持60s（java小游戏、jd-gui反编译java工具）

下载题目之后，是一个jar包，解压之后得到很多class。查看别人的wp，发现是这是一个游戏。

打开小游戏方法：在命令行中，输入 java -jar 文件包的名字.jar ，便打开了。

应该是要玩60s，但是不知道怎么玩，直接jd-gui打开反编译。

JD-GUI Free Download (apponic.com)jd gui下载地址



看到有一个flag，里面的字符串后面有一个=，推测是base64加密，

得到flag{DajiDali_JinwanChiji}

7、攻防世界 gif（103张黑白图，看成是0和1，二进制转字符）

这个题，给的是一个压缩包。解压之后，得到了103张黑白的图片，

把白色看成0，黑色看成1，写出二进制。（一开始我将白为1，黑为0，没有得出结果）

```
01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101
```

在线二进制转字符串。

在线转换二进制到字符串 (txttool.com)

输入二进制文本:

```
01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101
```

转换后的文本:

```
flag{FuN_giF}
```

得到flag。

flag{FuN_giF}

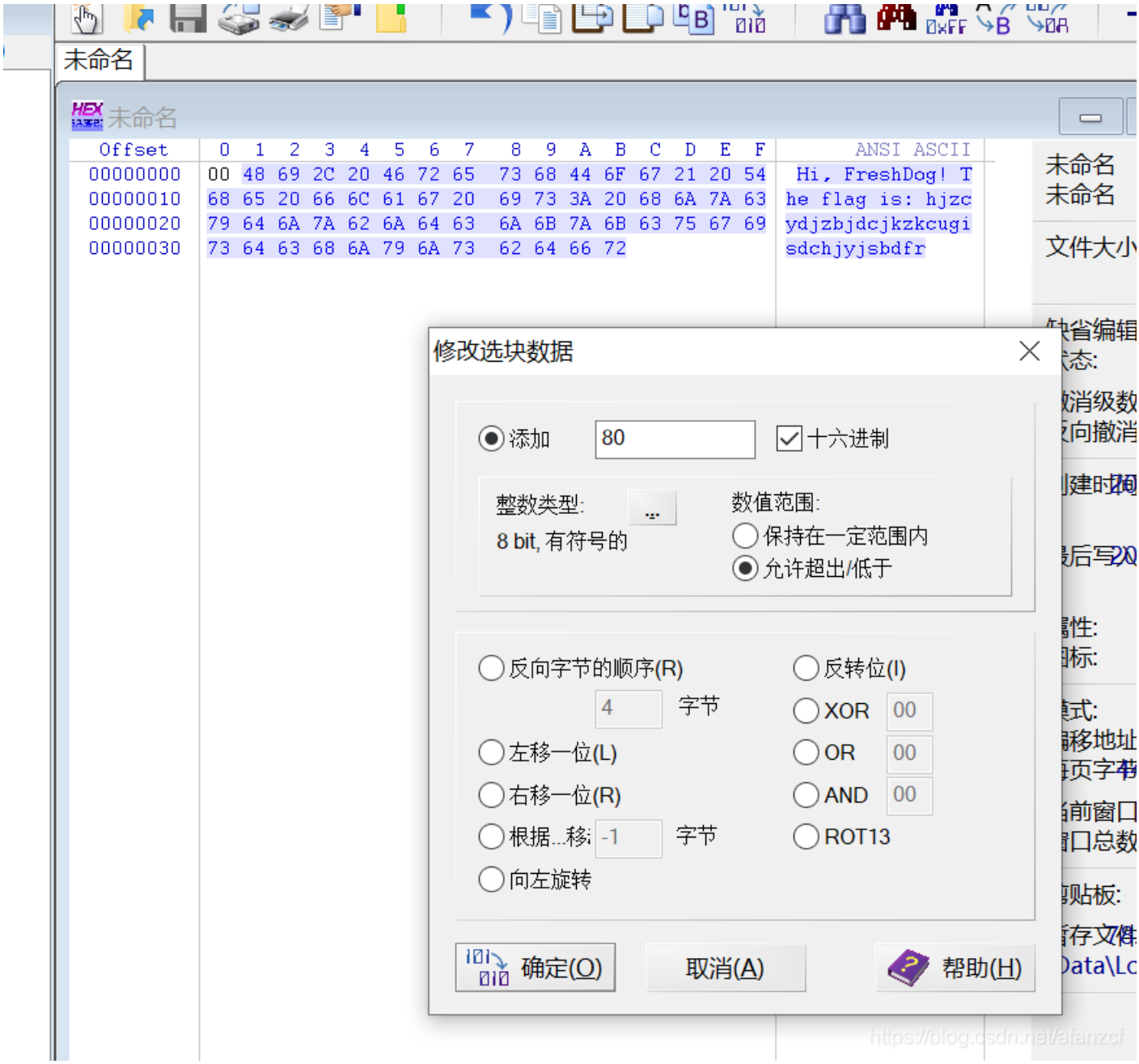
8、攻防世界 掀桌子

（1）法一（winhex）

在winhex中，新建一个1字节的文件。

然后将
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2

复制到其中。全选之后，**ctrl + T修改数据** 。



flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

（2）法二（java脚本）

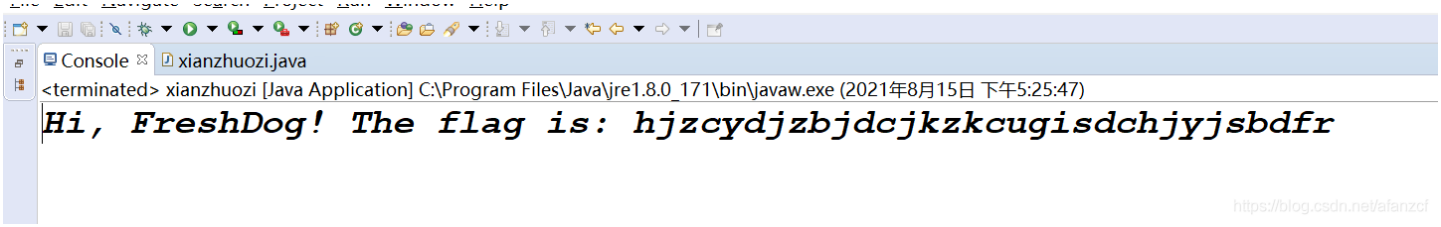
```java
package 攻防世界_掀桌子;

public class xianzhuozi {
        public static void main(String[] args) {
        String
        hex="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4
        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);//将两两字符转换为十进制
        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
        }
        }
        }
```

```
package 攻防世界_掀桌子;

public class xianzhuozi {
  public static void main(String[] args) {
  String
  hex="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf
9eaf3e2e4e6f2";
  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);//将两两字符转换为十进制
  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,获取字符
  }
  }
  }
```

得到flag。



flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

9、ext3（winhex、360压缩）

（1）直接找到base64

直接winhex打开，找到一串类似base64的字符串

当然这个方法，没啥用，在茫茫字符中，一下找到base64加密，不太可能。

```
00681380  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681390  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006813A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006813B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006813C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006813D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006813E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006813F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681400  5A 6D 78 68 5A 33 74 7A  59 57 70 69 59 32 6C 69  ZmxhZ3tzYWpiY2li
00681410  65 6E 4E 72 61 6D 70 6A  62 6D 4A 6F 63 32 4A 32  enNrampjbmJoc2J2
00681420  59 32 70 69 61 6E 4E 36  59 33 4E 36 59 6D 74 36  Y2pianN6Y3N6Ymt6
00681430  61 6E 30 3D 0A 00 00 00  00 00 00 00 00 00 00 00  an0=
00681440  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681450  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681460  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681470  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00681490  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
006814A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

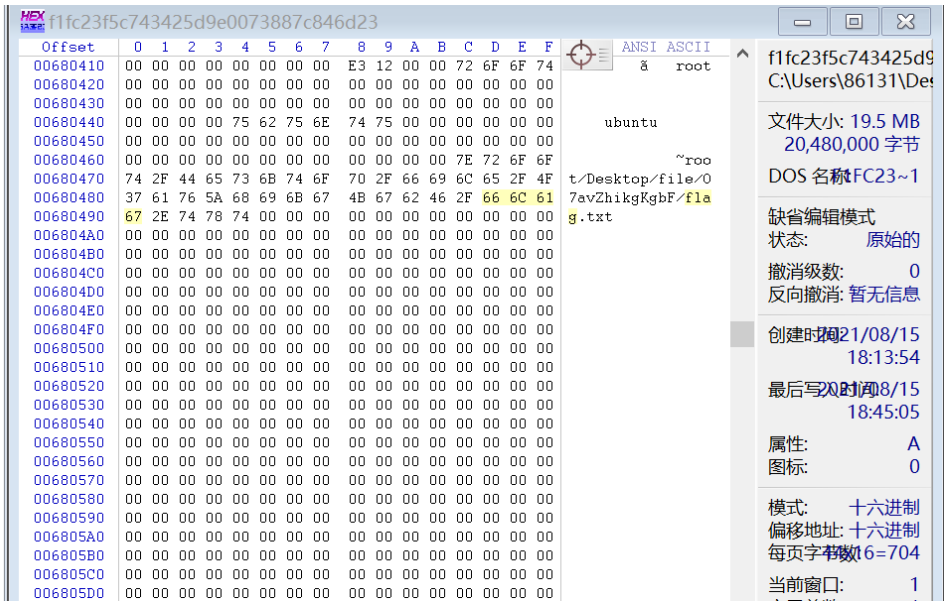

拖到base64解密。

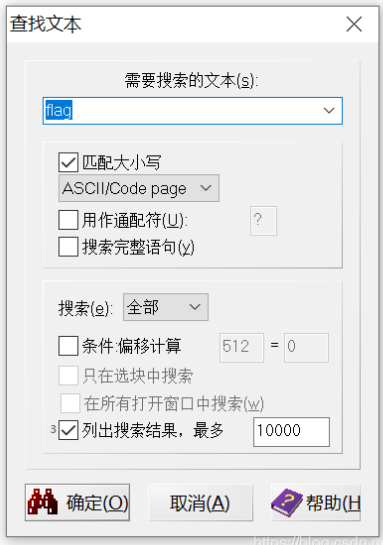
Base64 在线编码解码 | Base64 加密解密 - Base64.us

得到flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

（2）搜索flag

一开始使用搜索的时候，便不好使，后面发现是搜索的条件设置错了。





根据大佬的wp，发现是要解压这个文件，但是我的WinRAR不行，好像得360压缩，还别说，这360流氓软件的功能还挺强的。

然后，根据路劲找到这个flag.txt，打开。里面就是我们刚刚找到的base64了。

（3）linux下挂载操作

这个方法不太会，没kali的虚拟机。日后再去分析。

10、攻防世界 SimpleRAR（文件块、Stegsolve、ps操作）

这个题，是一个rar，解压之后里面有一个txt。但是这是表面。

在我解压的时候，解压软件提醒我，有一个png文件的头被损坏。

一开始以为是rar的文件头被损坏，但是用winhex查看之后，发现便不是，后面才知道这涉及到了rar文件块的知识。再加上后面的Stegsolve的使用和ps的使用。

于是单独写了一篇wp来记录一下。

攻防世界 SimpleRAR(文件块、Stegsolve工具的疑惑、ps详细操作)_啥也不会的大白555的博客-CSDN博客

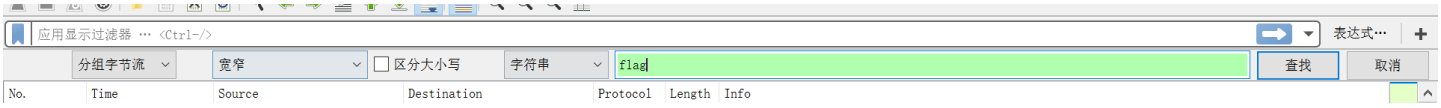
11、攻防世界 base64stego（base64隐写、zip伪加密）

攻防世界 base64stego_啥也不会的大白555的博客-CSDN博客

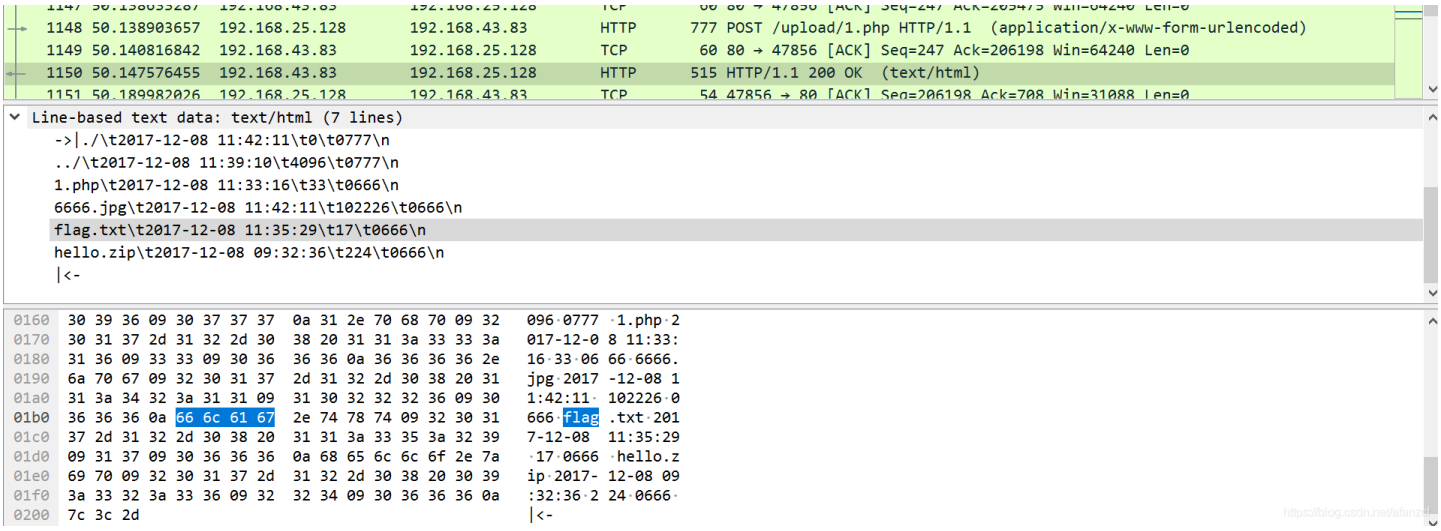
12、攻防世界 功夫再高也怕菜刀（wireshark、foremost、winhex）

这道题对于目前的我来说，很难。第一是wireshark的使用，第二是foremost的使用。

下载附件之后，得到了一个pcapng文件，用wireshark打开，ctrl + F 搜索

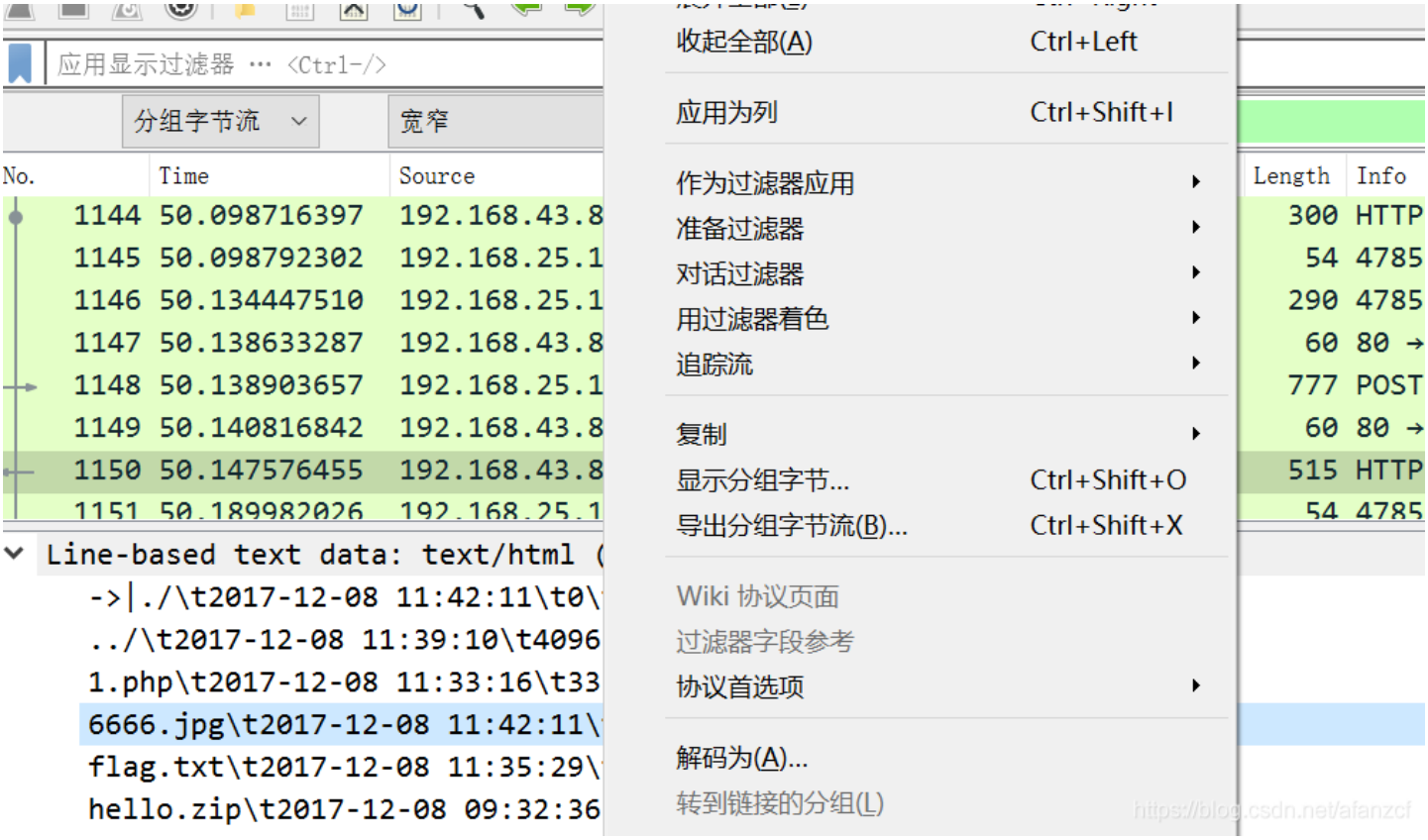


在1150处，可以观察到有好几个文件

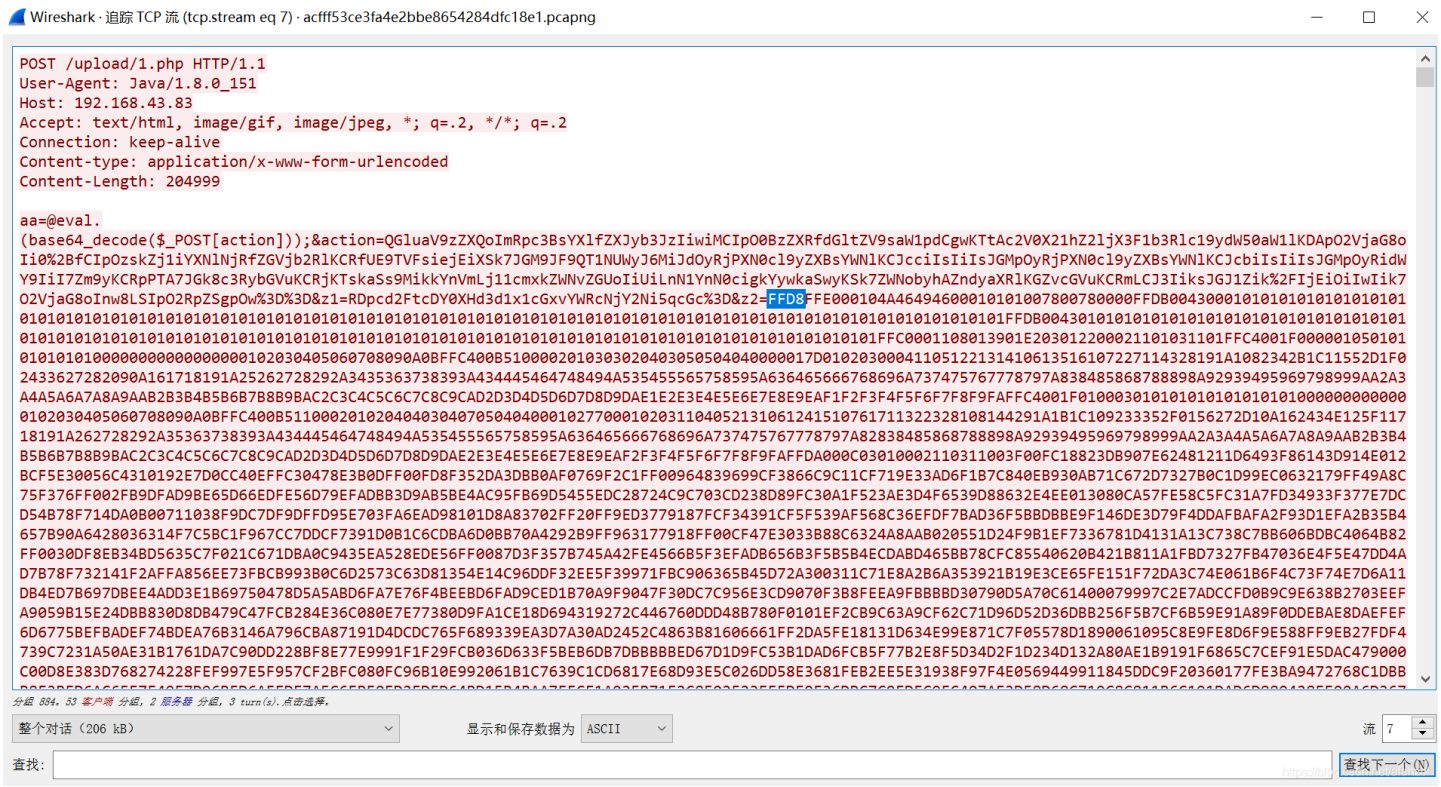


一个是flag.txt，一个是hello.zip，一个是6666.jpg.

我们先找到6666.jpg，



选择追踪流，然后TCP流



可以看到得到了一大串字符，在字符中，发现了jpg图片的文件头FFD8，和文件尾FFD9，我们复制。

然后去winhex粘贴。

这里要选择ASCII hex的格式。

然后另存为xxx.jpg。

最后打开图片就可以看到zip压缩包的密码。

刚刚在1150处看到有一个hello.zip，这个文件我们需要使用foremost工具，将它分离出来，这里我没有kali就不演示了（后面有时间再来复习重做）。

得到hello.zip之后，把图片上的密码输入就能打开了，然后得到flag.txt，打开就得到了flag。

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}

总结

做完了这12道misc新手题，感悟很多，也知道和认识了很多工具。比如Stegsolve、foremost、wireshark、winhex、等等，知道了很多密码，base64、rot13、还有一些方法zip伪加密啊，ps补全二维码啊，也学到了很多misc题的解法，从一开始拿到题目不知道怎么下手，不知道工具，到现在能懂了一点皮毛，也算是有所收获，继续加油。