




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](#)

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/afanzcf/article/details/119750872>

版权



[CTF杂项MISC新手 专栏收录该内容](#)

5 篇文章 1 订阅

订阅专栏

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



<https://blog.csdn.net/afanzcf>

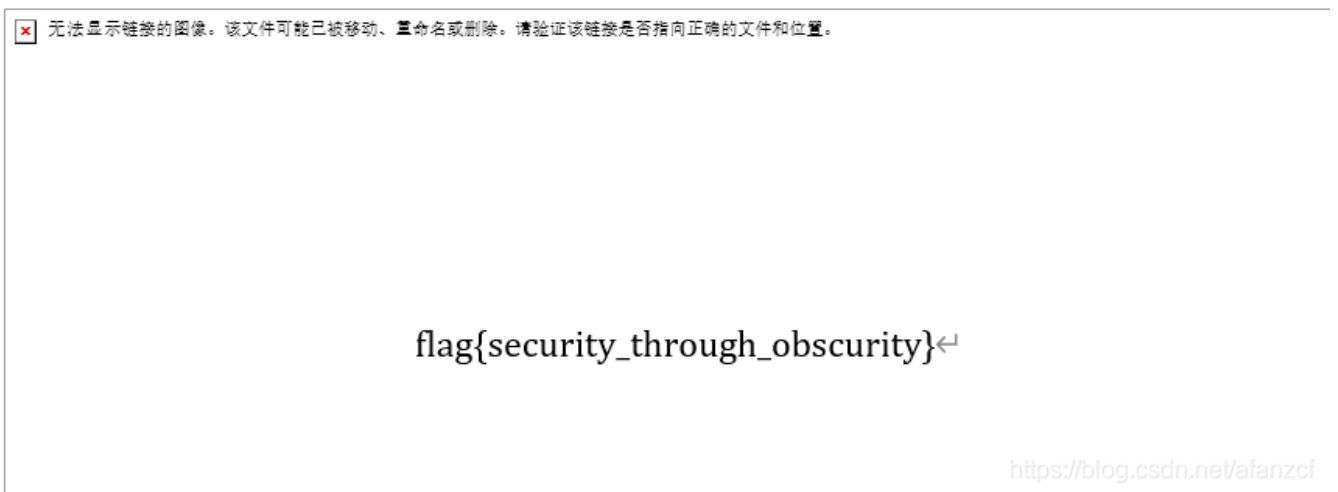
给的是一个pdf，打开之后，在图片中间能用鼠标选中字符，直接全选复制，粘贴就出来了。

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。



<https://blog.csdn.net/afanzcf>

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幡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苦奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆
多鉢以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得
槃漫夢盧幡亦醯呐娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇
輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

<https://blog.csdn.net/aifanzcf>

夜哆悉諳多苦奢陀奢諦冥神哆盧穆幡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苦奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得槃漫夢盧幡亦醯呐娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡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：

与佛论禅

MzkuM3gvMUawnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

心不变，万物皆不变

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆幡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苦奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得槃漫夢盧幡亦醯呐娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡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

<https://blog.csdn.net/aifanzcf>

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)

rot13

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

然后，再base64解密。

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

请输入要进行 Base64 编码或解码的字符

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

编码 (Encode)

解码 (Decode)

↑ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

flag{bdscjhbkmnfrdhbvckijndskvbkjdsab}

<https://blog.csdn.net/afanzcf>

得到flag。

flag{bdscjhbkmnfrdhbvckijndskvbkjdsab}

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 $26=2 \times 13$ ，ROT13函数是它自己的逆反。

base64:

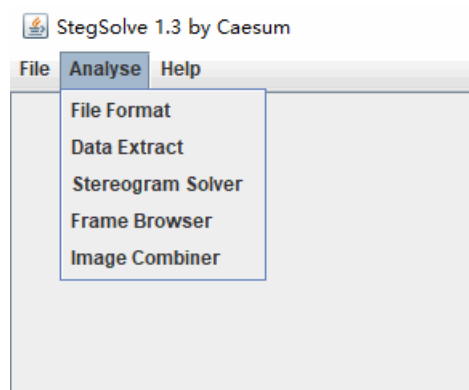
1. 标准base64只有64个字符（英文大小写、数字和+、/）以及用作后缀等号；
2. base64是把3个字节变成4个可打印字符，所以base64编码后的字符串一定能被4整除（不算用作后缀的等号）；
3. 等号一定用作后缀，且数目一定是0个、1个或2个。这是因为如果原文长度不能被3整除，base64要在后面添加\0凑齐3n位。为了正确还原，添加了几个\0就加上几个等号。显然添加等号的数目只能是0、1或2；
4. 严格来说base64不能算是一种加密，只能说是编码转换。使用base64的初衷。是为了方便把含有不可见字符串的信息用可见字符串表示出来，以便复制粘贴；

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

直接全选复制，到文本下粘贴。

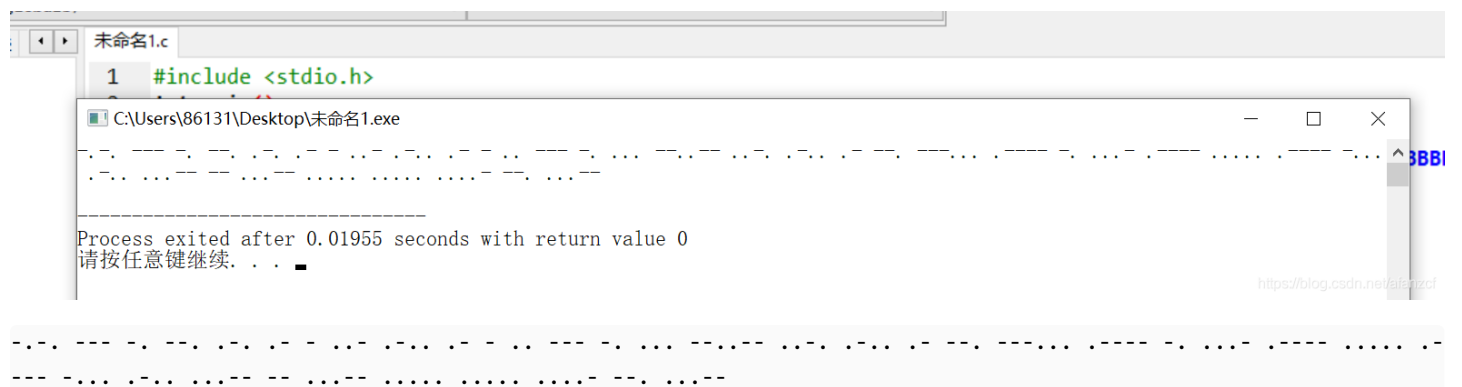
```
NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA 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。

```
1 #include <stdio.h>
2 int main()
3 {
4     char str[] = "BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA AB BBB BA AAAB AB
5     int i = 0;
6     for(i = 0; i<200; i++)
7     {
8         if(str[i] == 'A')
9         {
10            str[i] = '.';
11        }
12        else if(str[i] == 'b')
13        {
14            str[i] = '-';
15        }
16    }
17    printf("%s\n", str);
18    return 0;
19 }
```

<https://blog.csdn.net/alan201>

```
#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 AB BBB BA AAAB
ABBBB AAAAA AB BBB 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;
}
```



<https://blog.csdn.net/alan201>

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 \(all-tool.cn\)](http://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。

```
GameObject.class PlaneGameFrame.class
}
}
49 if (!this.p.isLive()) {
51     printInfo(g, "兄弟就死了的嘛", 50, 150, 200);
53     int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
54     printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
56     switch (period / 10) {
58         case 0:
59             printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
60             break;
61         case 1:
62             printInfo(g, "这东西你也要抢着带?", 50, 150, 300);
63             break;
64         case 2:
65             printInfo(g, "如果梦想有颜色, 那一定是原谅色", 40, 30, 300);
66             break;
67         case 3:
68             printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);
69             break;
70         case 4:
71             printInfo(g, "加油你就是下一个老王", 50, 150, 300);
72             break;
73         case 5:
74             printInfo(g, "如果撑过一分钟我岂不是没面子", 40, 30, 300);
75             break;
76         case 6:
77             printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
78             break;
79     }
80 }
81 }
82 }
83 }
84 }
85 }
86 }
87 }
88 }
89 }
90 public void printInfo(Graphics g, String str, int size, int x, int y) {
    Color c = g.getColor();
}
```

合集
470c.jar
ls

<https://blog.csdn.net/afanzcf>

看到有一个flag, 里面的字符串后面有一个=, 推测是base64加密,

请输入要进行 Base64 编码或解码的字符

RGFqaURhbGlfSmlud2FuQ2hpamk=

编码 (Encode) 解码 (Decode) **↕ 交换** (编码快)

Base64 编码或解码的结果:

DajiDali_JinwanChiji

<https://blog.csdn.net/afanzcf>

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 \(txttool.com\)](http://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
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2

复制到其中。全选之后，**ctrl + T**修改数据。



flag{hjzcydjzbdjckzkcugisdchjyjsbdf}

(2) 法二 (java脚本)

```

1 package 攻防世界_掀桌子;
2
3 public class xianzhuozi {
4     public static void main(String[] args) {
5         String
6         hex="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4
7         String temp="";
8         String flag="";
9         for (int i = 0; i < hex.length(); i+=2) {
10            temp=hex.substring(i, i+2);//获取相邻的字符
11            long dec=Long.parseLong(temp,16);//将两两字符转换为十进制
12            flag=Long.toString(dec-128);//将 long 型的十进制值减去 128, 再转换为 String
13            System.out.print((char)Integer.parseInt(flag));//解析 flag 为十进制整数, 并强
14        }
15    }
16 }

```

<https://blog.csdn.net/aianzcf>

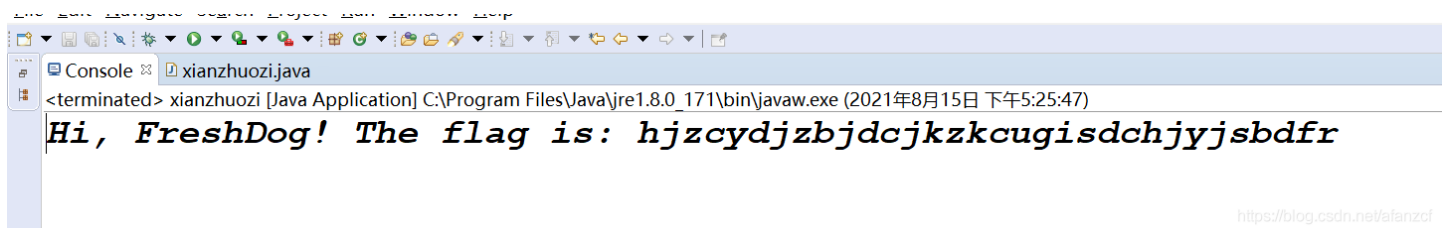
```

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。



<https://blog.csdn.net/aianzcf>

flag{hjzcydjzbdckzkcugisdchjysbdf}

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
006813A0 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
006813C0 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
006813E0 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
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
006814B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

<https://blog.csdn.net/afanzcf>

拖到base64解密。

[Base64 在线编码解码](#) | [Base64 加密解密 - Base64.us](#)

请输入要进行 Base64 编码或解码的字符

ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

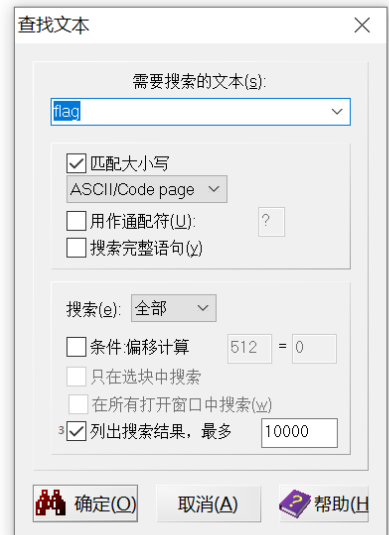
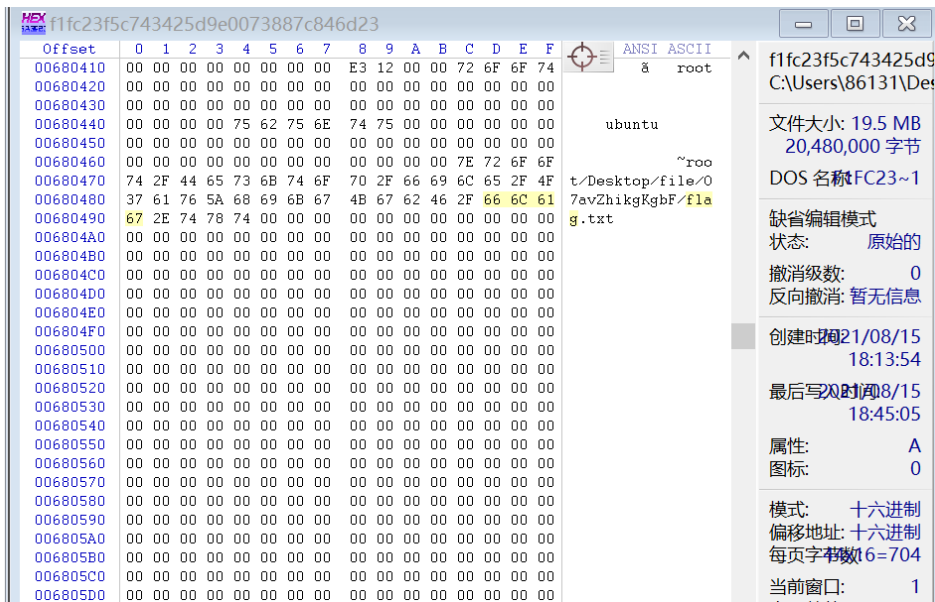
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

<https://blog.csdn.net/afanzcf>

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](#)

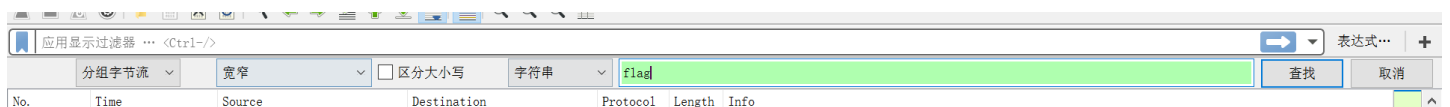
11、攻防世界 base64stego (base64隐写、zip伪加密)

[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

```

1147 50.13893287 192.168.43.83 192.168.25.128 TCP 60 80 → 47856 [ACK] Seq=247 Ack=206198 Win=64240 Len=0
1148 50.138903657 192.168.25.128 192.168.43.83 HTTP 777 POST /upload/1.php HTTP/1.1 (application/x-www-form-urlencoded)
1149 50.140816842 192.168.43.83 192.168.25.128 TCP 60 80 → 47856 [ACK] Seq=247 Ack=206198 Win=64240 Len=0
1150 50.147576455 192.168.43.83 192.168.25.128 HTTP 515 HTTP/1.1 200 OK (text/html)
1151 50.189982026 192.168.25.128 192.168.43.83 TCP 54 47856 → 80 [ACK] Seq=206198 Ack=708 Win=31088 Len=0

```

Line-based text data: text/html (7 lines)

```

->|./\t2017-12-08 11:42:11\t0\t0777\n
..\t2017-12-08 11:39:10\t4096\t0777\n
1.php\t2017-12-08 11:33:16\t33\t0666\n
6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n
flag.txt\t2017-12-08 11:35:29\t17\t0666\n
hello.zip\t2017-12-08 09:32:36\t224\t0666\n
|<-

```

```

0160 30 39 36 09 30 37 37 0a 31 2e 70 68 70 09 32 096 0777 1.php 2
0170 30 31 37 2d 31 32 2d 30 38 20 31 31 3a 33 33 3a 017-12-0 8 11:33:
0180 31 36 09 33 33 09 30 36 36 36 0a 36 36 36 36 2e 16 33 06 66 6666.
0190 6a 70 67 09 32 30 31 37 2d 31 32 2d 30 38 20 31 jpg 2017 -12-08 1
01a0 31 3a 34 32 3a 31 31 09 31 30 32 32 32 36 09 30 1:42:11 102226 0
01b0 36 36 36 0a 66 6c 61 67 2e 74 78 74 09 32 30 31 666 flag .txt 201
01c0 37 2d 31 32 2d 30 38 20 31 31 3a 33 35 3a 32 39 7-12-08 11:35:29
01d0 09 31 37 09 30 36 36 0a 68 65 6c 6c 6f 2e 7a -17-0666 hello.z
01e0 69 70 09 32 30 31 37 2d 31 32 2d 30 38 20 30 39 ip 2017- 12-08 09
01f0 3a 33 32 3a 33 36 09 32 32 34 09 30 36 36 36 0a :32:36 2 24 0666
0200 7c 3c 2d |<-

```

一个是flag.txt，一个是hello.zip，一个是6666.jpg。

我们先找到6666.jpg，

应用显示过滤器 ... <Ctrl- />

分组字节流 宽窄

No.	Time	Source	Length	Info
1144	50.098716397	192.168.43.8	300	HTTP
1145	50.098792302	192.168.25.1	54	4785
1146	50.134447510	192.168.25.1	290	4785
1147	50.138633287	192.168.43.8	60	80 →
1148	50.138903657	192.168.25.1	777	POST
1149	50.140816842	192.168.43.8	60	80 →
1150	50.147576455	192.168.43.8	515	HTTP
1151	50.189982026	192.168.25.1	54	4785

Line-based text data: text/html (7 lines)

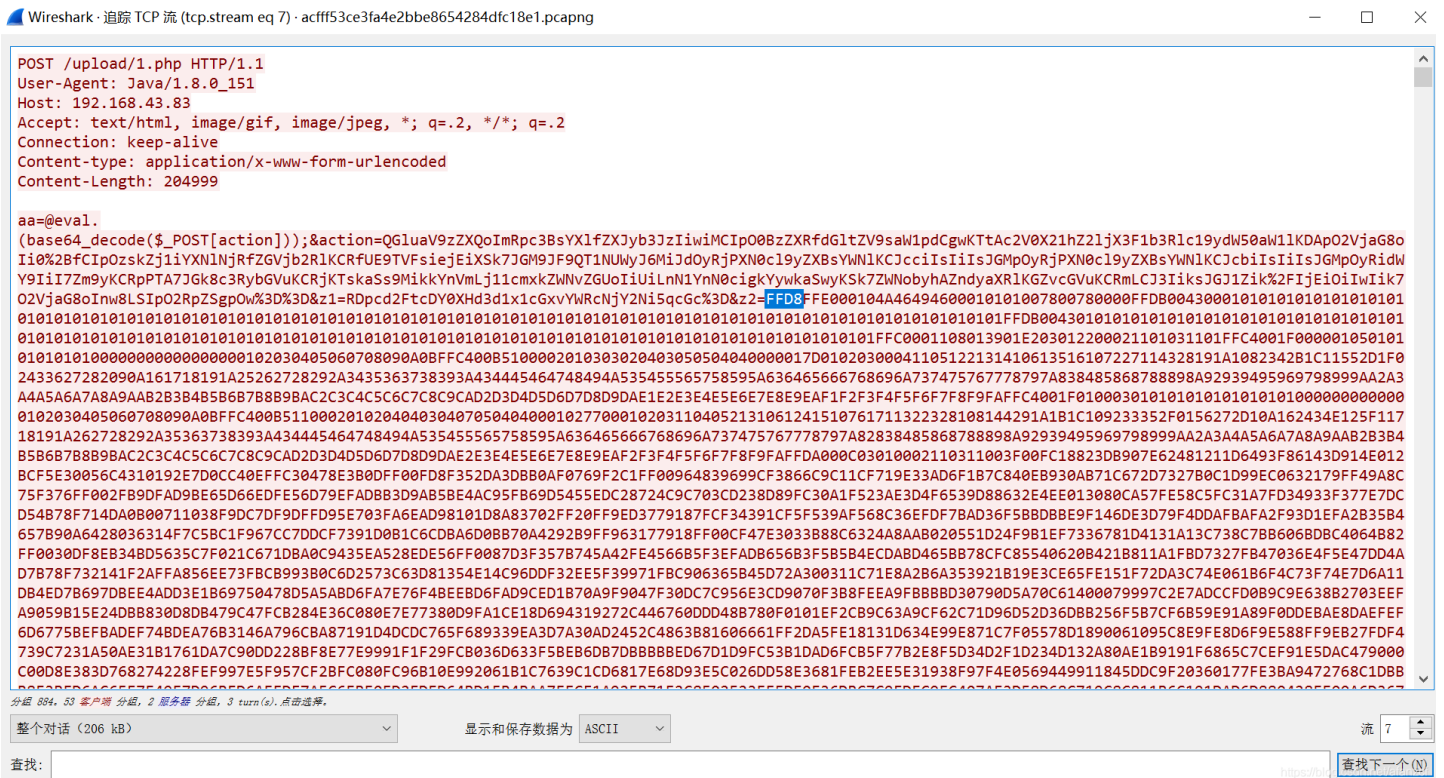
```

->|./\t2017-12-08 11:42:11\t0\t0777\n
..\t2017-12-08 11:39:10\t4096\t0777\n
1.php\t2017-12-08 11:33:16\t33\t0666\n
6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n
flag.txt\t2017-12-08 11:35:29\t17\t0666\n
hello.zip\t2017-12-08 09:32:36\t224\t0666\n
|<-

```

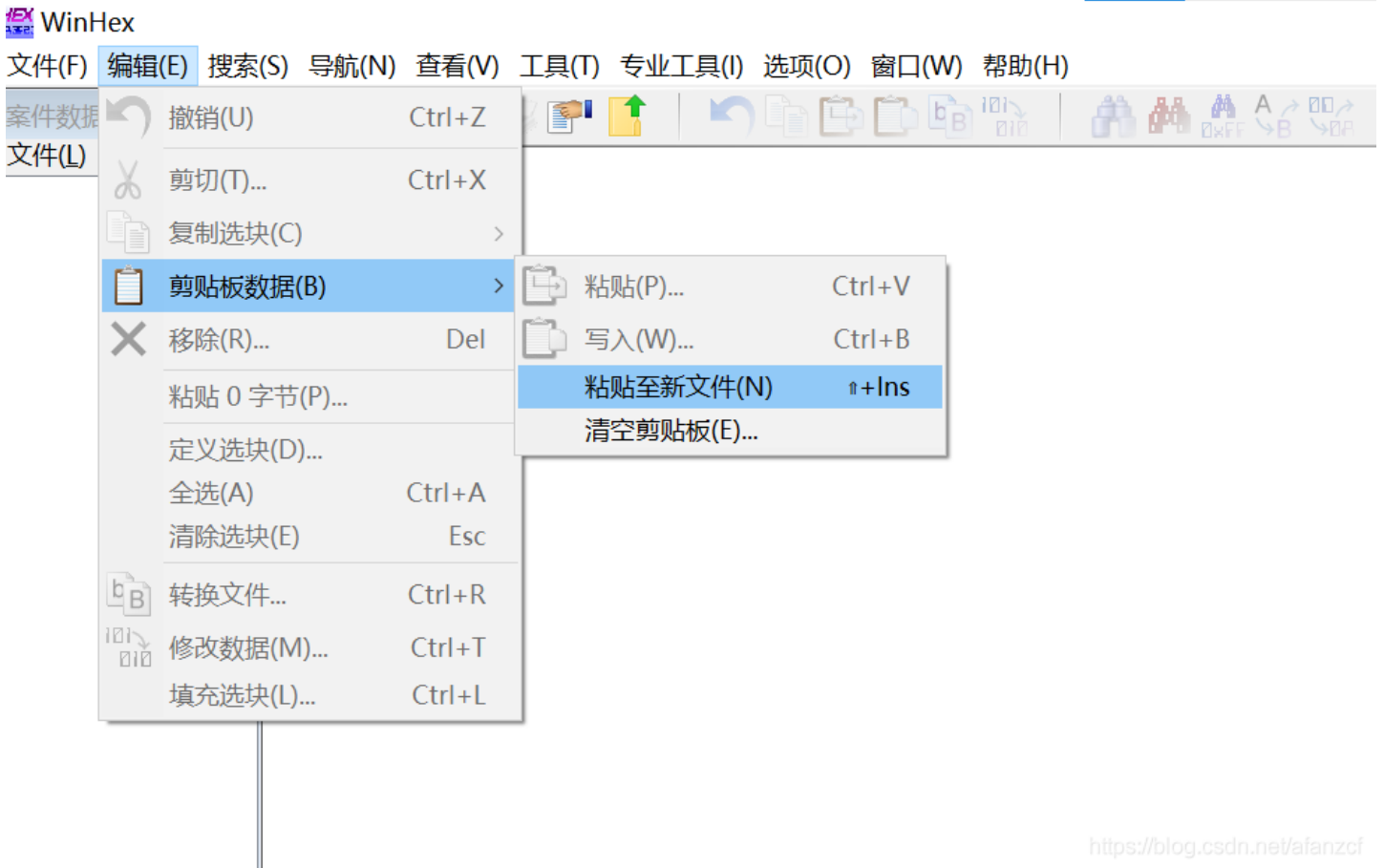
- 收起全部(A) Ctrl+Left
- 应用为列 Ctrl+Shift+I
- 作为过滤器应用
- 准备过滤器
- 对话过滤器
- 用过滤器着色
- 追踪流
- 复制
- 显示分组字节... Ctrl+Shift+O
- 导出分组字节流(B)... Ctrl+Shift+X
- Wiki 协议页面
- 过滤器字段参考
- 协议首选项
- 解码为(A)...
- 转到链接的分组(L)

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。

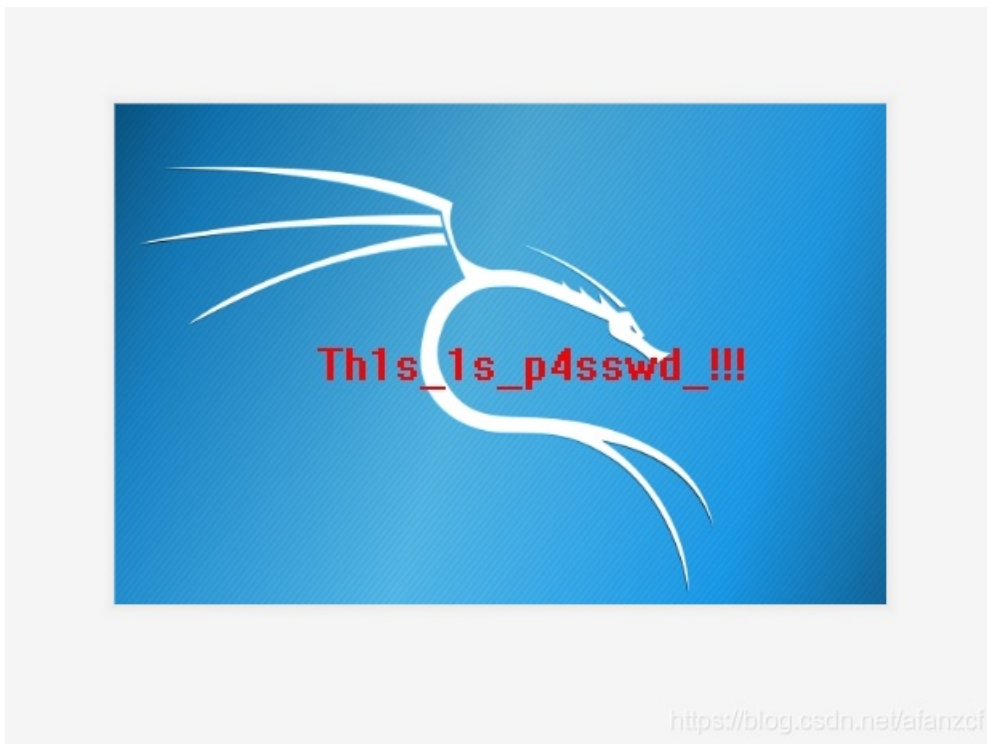
然后去winhex粘贴。



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。