瓜大NPUCTF-Misc、Crypto Write Up

原创

F1shCyy 于 2020-04-29 08:35:37 发布 2121 收藏 4
分类专栏： Write Up CTF 文章标签： 经验分享

参考的wp链接

官方wp：https://github.com/sqxssss/NPUCTF_WriteUps

大佬们的wp：https://l1near.top/index.php/2020/04/20/33.html

Ga1@xy博客wp

Misc

Misc题目下载地址：自用蓝奏云 or BUUCTF

HappyCheckInVerification(黑人抬棺)

下载附件为一个zip无后缀名的文件，我直接扔到Kali里用binwalk -e提取，得到一个二维码和一段黑人抬棺的MP4文件。

（以上算是走了捷径哈哈哈,看大佬的wp得知应该这个样：这道题下载附件以后，用winhex打开压缩包会发现，压缩包的文件尾50 4B 05 06出现在文件头的位置，那么把他移到文件尾，然后又发现是伪加密，把09改成00但是发现用winrar打不开，当时我选择的是用bandizip，发现能打开，后来询问了出题人，得知正确解法是最开头一段PK移到结尾 伪加密可以不管 然后自己判断块长度去修复对应二进制位。）

二维码是一个缺少定位符的图片，用PS将二维码补全

扫描得到内容：flag{this_is_not_flag}三曳所諳陀怯耶南夜缽得醢怯勝數不知喝盧瑟侄盡遠故隸怯薩不娑羯涅冥伊盧耶諳提度奢道盧冥以朋罰所即栗諳蒙集皤夷夜集諳利顛吶寫無怯依奢竟#￥#%E68BBFE4BD9BE68B89E6A0BCE79A84E5A7BFE58ABFE59CA8E69C80E5908E32333333||254333fafusedasdasdafafa_$ba##se64$

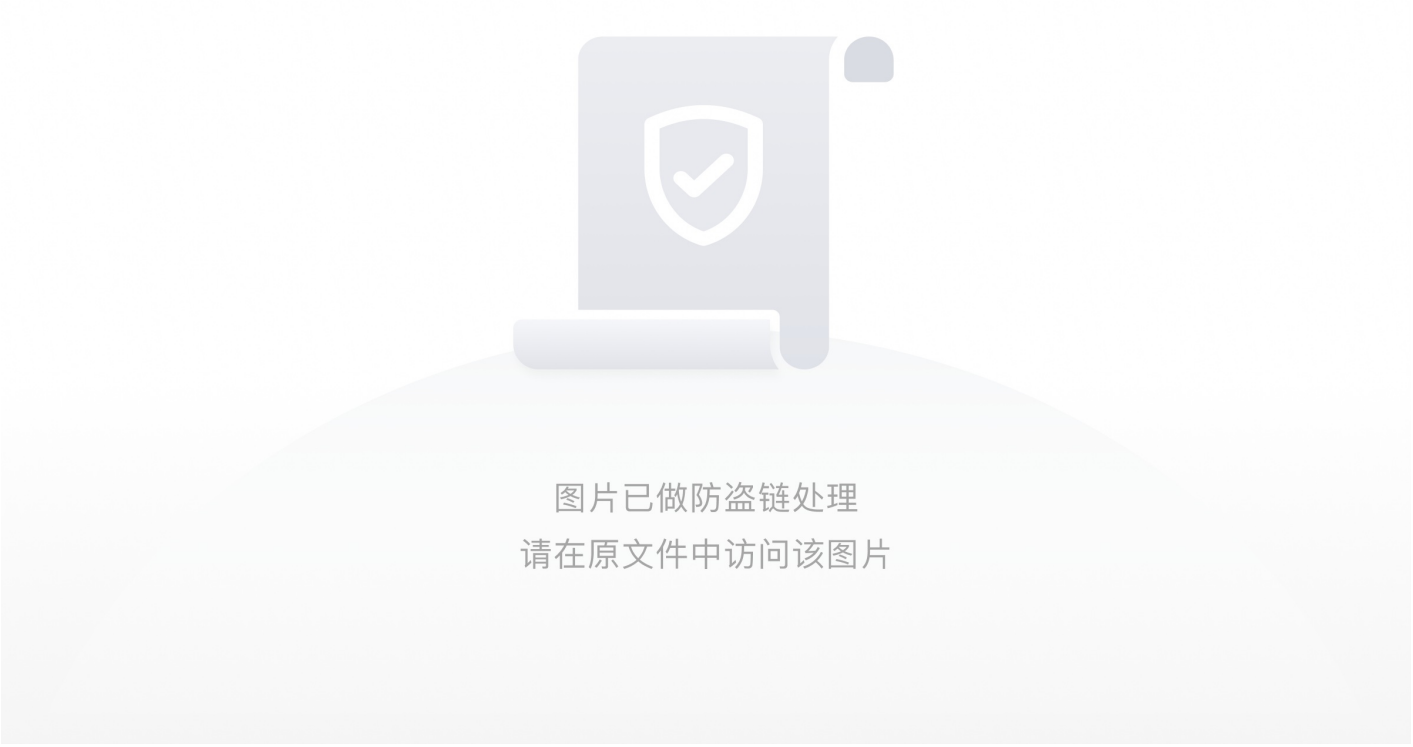
发现一堆乱乱的文字感觉像是与佛论禅于是解码一下得到（没啥用的提示QAQ）

注意与佛论禅解码需要在文本前加（佛曰:）否则解不出来。解码网址

其次是Base16，依次尝试解出来

然后就是先Base16解码

随后Url解码，注意需要将下面换成gb2312。得到一串汉字



最后我们在二维码扫除的这段文字末尾能看到use base64

好了这段文字没有给我们什么提示，我们去看MP4视频

在中间的位置会出现电话拨号的声音

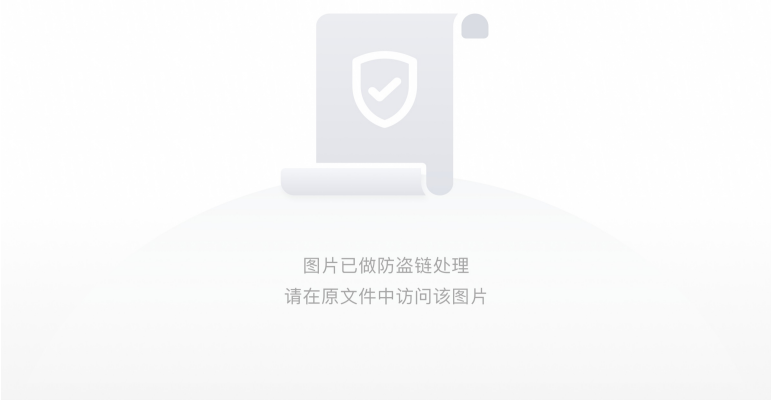
根据大佬wp提供的截取的拨号声我们使用**dtmf2num.exe**将其数字号码读取出来

截取的拨号声文件下载：**度娘网盘** **提取码：s27k**

使用方法：需要将两段音频分别放在dtmf2num所在文件夹下

使用cmd定位到此文件夹下

> 命令：dtmf2num.exe xxx.wav



然后开头几个数字去找了出题人得到了hint，最后得到手机号码xxx18070885

那么发短信过去会提示NWPUSEC

去微信公众号关注了以后，根据之前提示 **use base64** 发送了手机号码base64encode的结果，然后返回了一段音频

由于比赛已结束所以大佬的wp里提供了音频下载地址：**度娘网盘** **提取码：unm8**

打开音频播放了一段很刺耳的音频由此判定应该为**SSTV（慢扫描电视，它是无线电爱好者的一种主要图片传输方式）**

我们需要一个手机app：**Robot36** 将这段音频转化为图片

最后转化的图片为：

得到flag

老千层饼

下载附件解压压缩包后文件夹内有五个文件分别为：zde0、zde1、zel、zfr0、zfr1

其含义为：ZipDirEntry0/1,ZipFileRecord0/1,ZipEndLocator

安照顺序：**zfr0+zfr1+zde0+zde1+zel** 将其中的内容组合得到一个ZIP压缩包

解压出来有一个txt文件和一个图片文件。

组合方法：

1.分别将五个文件载入010按照顺序每个文件的内容**全部**复制黏贴在一个**新建的十六进制文件**中，然后另存为xxx.zip即可得到压缩包

2.另一种获取两个文件的方法（自己琢磨的）：简单粗暴的将zfr0和zfr1分别扔到kali里用binwalk分离即可得到

随后我们将图片载入010观察发现

应该到IEND这里就结束了但是下面又多了一行，所以应该是添加东西了。我们直接点一下IEND这一行定位到这里。

发现这里有一个**7z开头**，于是想到是**7z压缩包**，直接**新建十六进制文件**，然后将**从7z开始往后的所有部分**复制黏贴到十六进制文件下 **另存为1.7z**。

就得到了一个压缩包解压得到一个含有base64的txt文件。

利用**在线网址**解一下得到：

```
//epicer_fehcrebyc

AES_Decrypt({'option':'Hex','string':'Remove'},{'option':'Hex','string':'this'},'CBC','Hex','Raw',{'option':'Hex','string':''})

Vigenère_Decode('keepthis')

PGP_Verify('Remove_this'/disabled)

From_Base64('A-Za-z0-9+/=',true)

XOR({'option':'Hex','string':'Remove_this_too'},'Standard',false)

DES_Decrypt({'option':'Hex','string':'av?'},{'option':'UTF8','string':'keepthis'},'CBC','Hex','Hex')
```

然后我们用工具StegSolve查看一下图片发现在Alpha这个通道里最上方好像有一串小字，这就证明有隐藏的内容是LSB隐写

根据**Ga1@xy大佬的博客Wp**里的脚本提取出其中的内容是个二维码，脚本由**FzWjScJ师傅**提供

```
from PIL import Image


p = Image.open('1.png')
a,b = p.size
i = ''
count = 0
for y in range(b):
    for x in range(a):
        data = p.getpixel((x,y))[3]
        if data == 255:
            i+='1'
        else:
            i+='0'
a = open('all.txt','w')
a.write(i)
a.close()


data = open('all.txt','r').read()
block1 = Image.new('L',(10,10),0)
block2 = Image.new('L',(10,10),255)
res = Image.new('L',(330,330),0)
for i in range(33):
    for j in range(33):
        if data[j+33*i] == '1':
            res.paste(block1,(i*10,j*10))
        else:
            res.paste(block2, (i * 10, j * 10))
res.show()
```

然后我们补全这个二维码

得到一串base64编码

> GvgQE86nZKJdFzN2Z9x2Y3OnZyvnYNQEbG282GRtSL0=

然后我们根据刚才7z压缩包解出来的txt文本名反过来得到提示：cyberchef_recipe

打开这个Cyberchef网址

> Operations,选择需要进行的操作，是编码还是加解密，或者其他操作
>
> Recipe，是相关操作需要的参数
>
> Input，输入数据
>
> Output，输出结果

首先点击**Recipe**旁边的**文件夹按钮**打开一个界面

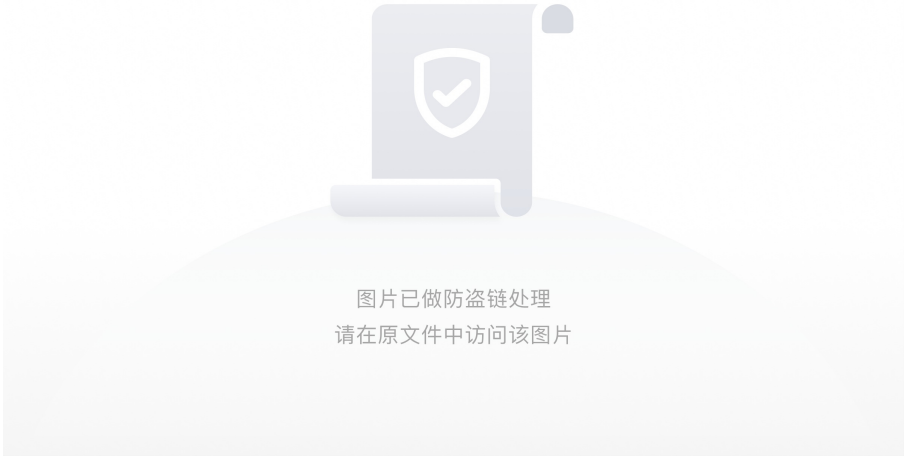
在下面将刚才Base64得到代码黏贴进去，注意要**删除**第一行的**//epicer_fehcrebyc**

然后点击**LOAD**

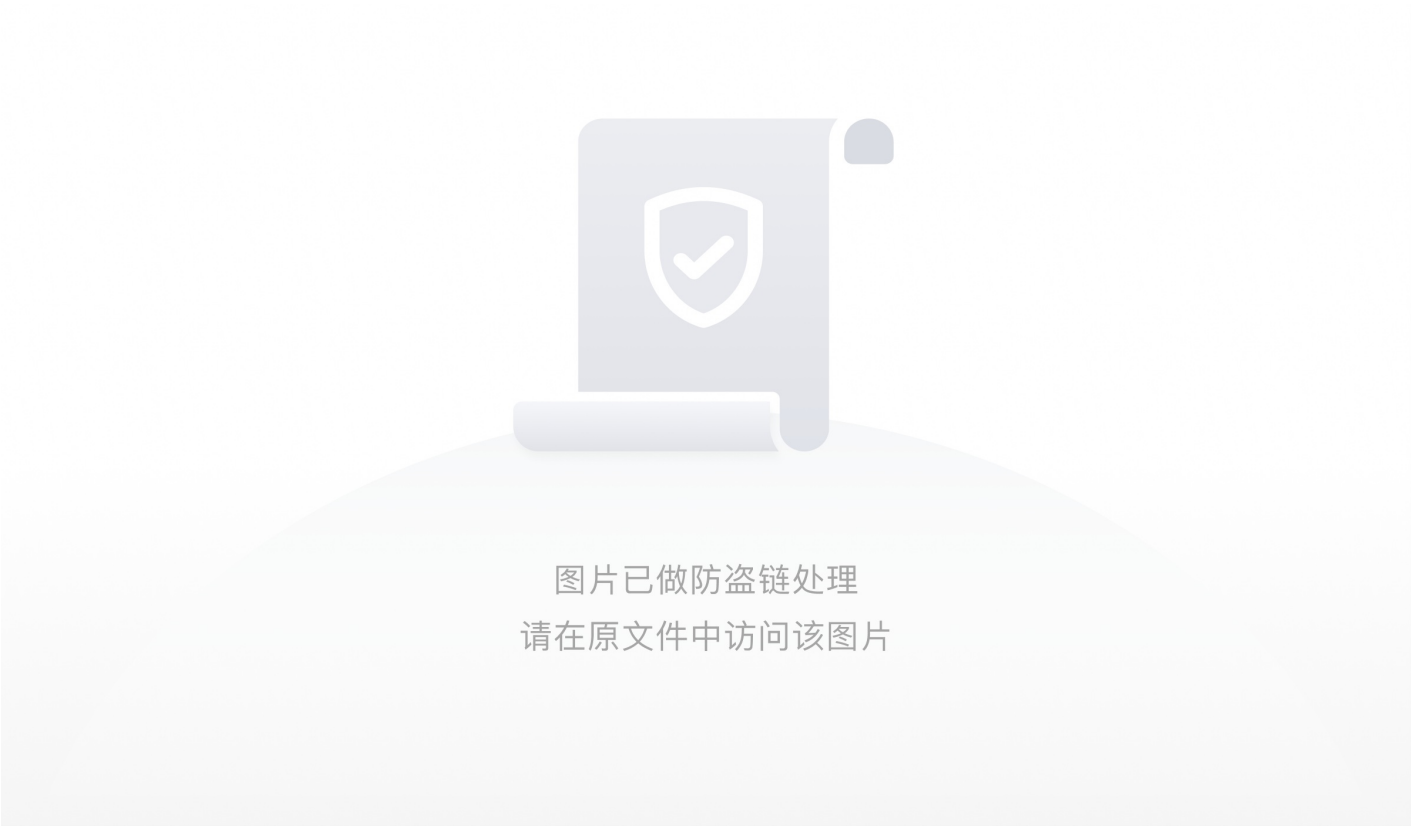
根据提示 **Remove this** 移除这个几个框（如何移除？双击框或者将框拖到别处即可）

在最后留下的几个框中看到一个**av**？我们联想到刚才图片的名字是BV开头的

有可能是bilibili的AV BV号，于是我们**在线网站**转换一下得到**av415411**



将得到的**av415411替换到key里**，然后在右边**Input**处将刚才扫码得到的**base64**黏贴进去下方会显示出flag



flag{An_Old_Th0usanqs_Of_Layer_P1e}

回收站

首先拿到题目解压看到文件后缀为E01，那么好了基本确定为取证的题目

我们需要用到一个软件**FTK Imager**

安装软件然后我们启动，点击File选择第三个选项卡载入**.E01**

注意：Mount Method 一定要选Writable

这里一定记得仿真的时候选择的挂载方式是可写

随后启动VM虚拟机，新建虚拟机，选择**自定义**

随后一直默认即可到选择**操作系统**时选择**win7 64**

然后一直默认即可，到选择**创建磁盘**，选择**SATA**

使用物理磁盘

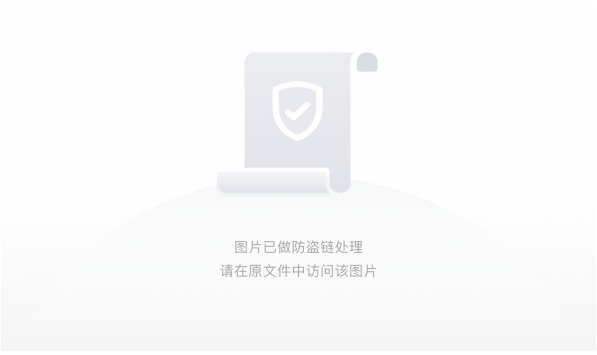
选择设备的时候一定要选跟FTK一样的才行

进去之后我们可以发现这里要密码，对于这里我们可以采用弱密码猜一猜，彩虹表，或者是你可以直接将注册表用户文件那一张改成你自己电脑的，然后登进去，或者可以用u盘清除windows的密码，这里密码很简单就是**admin123**

桌面是一个反转的：你知道我在哪儿嘛？由于题目是回收站所以我们打开回收站发现是空的

> 官方wp：这里就有一个知识点就是在取证的过程中，因为取证的镜像都是犯罪嫌疑人的，所以他们会把他们的东西放的很隐蔽，回收站在windows里面本来就是个隐藏文件夹，有些人就会将他们的重要的东西伪装成回收站目录或者注册表目录或者windows目录等然后隐藏，所以我们这里就要显示下隐藏文件夹，看看有没有被伪装成回收站的文件夹

设置显示隐藏的步骤，顺带将扩展名也显示出来



然后我们进入到C盘发现了一个隐藏的文件夹RECYCLER

进去以后有个flag的文件夹我们进到最里面，发现好多文件夹，然后有好多图片，拼起来是一个打了马赛克的flag

> 官方WP:我们可以看到他有点坑flag里面有好多的flag然后最后发现这些123456748…对应的是图片，还是可以拼起来的
>
> 拼起来之后我们可以发现这些图是打了马赛克的，恢复是恢复不出来的，所以这就告诉我们，当我们遇到一个很坑的题目的时候，我们一定要注意细节，拓宽思维，一个路子走不通那么肯定还有其他的路可以走得通（小声bb：我之前就被这么坑过）然后我们就注意下桌面了，你要相信，一个题目里面不可能有地方是随意给你的东西，只要在题目中出现就有他出现的作用，他可能是用来混淆视线也可能是用来给你最细微的提示

我们看到这个壁纸内容是“你知道我在哪吗？”，说这话的应该就是flag了，这里我们就要知道桌面壁纸在哪里，要注意两个地方就是win7默认壁纸目录还有win7当前壁纸目录

补充小知识：win7

在注册表中，HKEY_USERS/用户/Control Panel/Desktop

系统默认的桌面图片都放在C:\WINDOWS\Web\Wallpaper 里面。

当前桌面的图片的目录在

C:\Users\test\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg

flag隐藏在默认目录里

但是打不开，于是我们修改他的后缀名为txt得到flag

flag{e10adc3949ba59abbe56e057f20f883e}

碰上彩虹，吃定彩虹！

首先下载附件解压以后发现有三个文件：lookatme.txt、may be hint.txt和secret

打开lookatme.txt发现文件是一串数字，全选以后发现最下方有几个空格和TAB换行组成的空。联想到是摩斯密码，**空格 = "."，TAB = "-"**

翻译出来的摩斯密码是：**.- ..- - --- -.- . -.--**

在线网址解密一下得到密文：**autokey**

根据解出来的密文可以判断上面的字符串经过了autokey加密

然后我满打开hint文本提示的翻译一下是

在文本里的那里面隐藏了一些东西，但是我找不到他

我们将这个文本放到Kali里用vim查看一下

发现了一堆由**<200b>、<200c>、<200d>**组成的字符串

经了解这是**零宽度字符隐写**

需要用的**在线网址**解一下。如图操作

注意现在网站下方将200B、200C、200D进行勾选

得到密文

> do u know NTFS?

注：有关零宽度字符隐写可见浅谈基于零宽度字符的隐写方式这篇博客

即NTFS隐写，在附件所在文件夹打开**cmd**输入**dir /r**，可以发现在maybehint这个文件后隐藏有一个txt文件

注：有关NTFS隐写可见NTFS文件隐写_运维这篇博客

用notepad命令查看，可以看到文档中的内容，稍加观察可以发现其中只有几种字符，而且都为重复的，据此可以尝试词频分析，python脚本即可实现

Python脚本（Ga1@xy大佬博客转）

```
from collections import Counter


f=open('maybehint.txt:out.txt','r')
f_read=f.read()
print Counter(f_read)
```

得到结果为这几种字符

> Counter({'Z': 126, 'W': 123, '5': 120, 'j': 119, 'c': 118, 'n': 117, 'l': 115, 'w': 112, 'd': 104, 'G': 101, '8': 100, '=': 90})

我们将其从多到少的排列顺序，组合在一起得到**ZW5jcnlwdG8=**，明显base加密，尝试base64解密成功，得到**encryp**

下载后尝试用其加密一个文件，可以得知经过其加密的文件后缀名为**crypto**，将文件后缀名改为crypto即可打开文件

因为介绍网址打不开可能需要科学上网的缘故以下(绿字)内容搬运大佬的wp：

可以看到文件被加密，想到autokey，但是由于没有给出加密密钥，所以需要对其进行爆破

关于如何对autokey加密进行爆破，在该网址有详细介绍

用脚本对密文进行爆破

可以看到当key长度为14时，得到key可读为youhavefoundme，看一下后面的明文，在最后写到

> NOWIWILLGIVEYOUTHEPASSWORDITISIAMTHEPASSWD

翻译一下这段文字

再结合hint小写，得到password：iamthepasswd

可是用此密码解这个加密文件时却一直解不开，再结合题目描述中加粗的**括号删掉**，推测是不是在文件中隐藏了什么信息，用strings命令查看一下文件可以发现这样一条信息

或者有可能是：(Oh! You caught me! But...)

然后我们需要将其删除利用**WinHex**或者**010**载入这个文件Ctrl+f进行搜索然后删除保存即可

再输入刚才的密码成功解出文件得到一张图**(注：这张图并不是原图切勿拿来直接用)**

我们将这个图放入kali用foremost进行分离得到一个压缩包

里面有一个word文件 经测试不是伪加密所以我们需要密码

仔细观察图片可以发现，由五种不同颜色的横条分隔开的六块黄色有略微深浅的差异

我们用**gimp或者使用PhotoShop 用滴管工具**提取一下颜色

gimp

PhotoShop

可以发现他们颜色的HTML标记只有最后两位不同，从上到下依次为**70**、**40**、**73**、**73**、**57**、**64**，将这几个数组合在一起，用Converter的Hex to Text，或者python的decode('hex')，就可以得到解压密码，这里用的Converte

得到密码：p@ssWd

解压出来word文件打开解压后得到docx文件，想到word隐写，显示隐藏文字可以看到提示

仔细观察上面的一长串字母，可以在众多的小写字母中发现几个大写字母

按照顺序组合起来得到ALPHUCK，

百度可知其为一种Programming Language，与Brainfuck类似，只由a,c,e,i,j,o,p,s这8个小写字母组成，删去上面的几个大写字母，

在线网站解码一下即可得到flag

flag：flag{1t's_v3ry_De1iCi0us~!}

串味撒硕（转载wp，看不懂脑子疼）

得到题目中的c(=16)和题面后，发现这是一个计数类题目，有一定的子结构，可能需要dp，本质上是求c个不同点有多少种不同的连通图构造.

Eg.c=3时有四种:

下面想计数的思路，其实正向是不好计数的，因为它的子结构不太好，c=3的左下图就破坏了c=2的情形（假定c=2时的唯一情况就是12相连，其余图都是满足的），于是**反着思考**。

c个点的无向图总数（连通+不连通）共个，这是因为c个点的图中最多可连c(c-1)/2条不重边，而每条边可连可不连，所以总数如上。

如果能统计出**c个点的无向不连通图数量**，就可以计算出所求。

这时取一个特殊位置来计数：让节点**1所在的连通块**，和剩余部分不连通，这样就保证了整个图绝对是不连通的，同时存在子结构：1所在的块是连通的，所以它的情况数可以用之前的结果表示。接下来再按1所在连通块的节点个数分类，加和，即得出c个节点的不连通图数量。

假设题目中的c个路口的连通图情况数为**f[c]**

那么当节点1所在的连通块内节点个数为j时，其自身有 **f[j]** 种情况。

因为点都不同，还可以被1的连通块选中或不选中，这需要从 [全部路口-1] (1节点已经在其中了)中选出j-1个路口，有种选法。

没在1连通块内的路口，它们之间可以任意组合（有多少个连通块都无所谓，他们的整体和1不连通）。根据上面的无向图总数公式，得到应该有种情况。

综合下来，在路口数为i时，

i其实就是单步的all。上面式子的意义即 (i点的连通图总数+i点不连通图总数=i点图总数)

所以F[i] 可以用F[1~i-1] 递推出，可以写出计算程序。

答案数比较大，没有要求取模，所以用python和java的BigInteger都是比较好的选择。

经过dp 计算F[16]得到一个大数：132857895833578320100833898686845427712

直接填入jar的窗口后，常见的应该都是卡住/崩溃。（当你人品够好的时候，也许答案会蹦出来）

用java的反编译打开jar (如jd-gui)。

发现有两个class，Gui主要处理窗体，其中实例化了Lib，打开Lib观察发现，它的功能是分解质因数，并且e函数返回了两个最大质因子的乘积显示在窗体中，只是分解方法采用了非常低效的随机数法+试除法。

于是不让程序来分解，自己分解，可以使用Pollard-Rho算法（约），或者自己的工具，或是网站（如http://www.factordb.com）。

最大的两个质因子为511756380671和1021144515583，根据两个大质数的乘积，e和(q-1)(p-1)互质这些特点，猜出这里是RSA加密，而两个质因子的乘积就是RSA加密里的n。

联系团长说的话，应该就是密文，所以现在已知密文C，密钥(n,e)，甚至连n的两个大因子都知道，不难进行解密。

得到原文：6879957879849583847980

长度22，有可能是2*11的分组，发现特点：六七十对应的是ascii的大写字母，出现两次的95对应ascii中的下划线。

所以原文进行ascii解密后得到DO_NOT_STOP，套上flag{}即结果。

不要停下来啊！

签到（我的世界纯转载wp）

进入游戏后，按照指引可以看到有一个开关和红石灯，打开开关后红石灯开始闪烁。

经过分析可知，红石灯有两种状态，常亮和短亮，故猜测其代表的是二进制值短亮为0，常亮为1，可得出序列

```
001110010110000100111001
```

根据题目字符串提示，将其转为字符串为

```
9a9
```

计算其MD5为8F108D05D23041B5866F9CB2FF109661，包裹Flag格式为

```
npuctf{8F108D05D23041B5866F9CB2FF109661}
```

如果不想等待红石灯闪烁可以去进行电路分析，按照开关线路，第一部分产生红石脉冲信号。

第二部分控制活塞推动方块。

第三部分异或门。异或门输出取反即为红石灯的信号输入。

游戏利用MC特性，龙蛋不能传递红石信号，而沙子可以传递红石信号。根据此可以判断活塞控制了三种状态：

1. 活塞处有两种不同方块，对应产生不同信号，异或门输出取反为灯灭
2. 活塞推出，对应产生相同信号，异或门输出取反为灯亮
3. 活塞处有两种相同方块，对应产生相同信号，异或门输出取反为灯亮

所以我们只需要判断两个不同方块间是否有相同方块就可以得出0和1，如

为0，

为1。

Crypto

这是什么觅马

将附件下载下来得到一个日历的图片

上网百度了一下根据这个将flag翻译了出来

依次查找，**F1 W1 S22 S21 T12 S11 W1 S13**对应着就是**3 1 12 5 14 4 1 18**(S22就代表是S2(Sunday)的第二个，同理可知S13 T12等)

其对应的字母为：calendar 即是flag

Classical Cipher

打开附件解压得到一个压缩包和一个txt文件

根据文本内容判断压缩包不是伪加密。

根据对应明文的提示想到的第一种可能是位移了是凯撒密码。

但是解出来的却不是，于是又想到的是quipquip但还是错误的。

最后感觉会不会是倒序排列，于是百度了一下是否有这种密码。

最后得到的结果是：埃特巴什码（Atbash） 即最后一个字母代表第一个字母Z = A

解密网址：点我~qvq

压缩包密码为：the_key_is_atbash

输入压缩包密码得到了一张图片

第一个是猪圈密码的变种（附密码表）

第二种根据狮身人面像感觉与埃及有关，于是得到了古埃及象形文字字母表

解出flag为flag{classicalcode}