1.想蹭网先解开密码

提示WIFI密码为手机号。下载下来是一个cap包，用wireshark打开。网上查了一下，WIFI连接认证的重点在WPA的四次握手包，也就是eapol协议的包，过滤一下，恰好有四个匹配的包。根据题目提示的密码前七位，使用crunch生成11位的密码字典

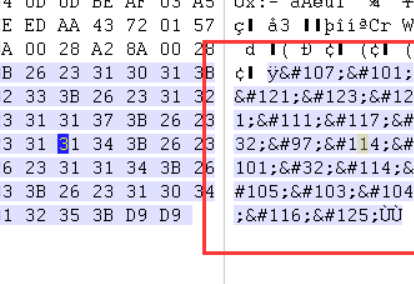
crunch 11 11 -t 1391040%%%% >>wifipass.txt //生成密码字典  
aircrack-ng -w wifipass.txt wifi.cap 进行密码爆破



密码即为flag

**2.这是一张单纯的图片**

格式改为zip，文件损坏。用winhex，再最后发现不正常的编码



然后用在线解码工具进行unicode解码，成功得到flag

**3.隐写**

解压后是一张图片，然后用winhex打开，在第二行第2,3列是宽，6,7列是高，把第六列的01改为11，那张图片就恢复原来的样子，flag就在那图片上。



**4.又一张图片，还单纯吗**

用binwalk跑一下，发现里面还有包含的jpg文件，用dd进行分离

dd if=2.jpg of=3.jpg skip=158792 bs=1

分离完后即可得到flag

**5.隐写2**

放到binwalk里发现有zip包含在里面，用dd分离出来

有密码，暴力破解直接就出来了（三位数的数字）

解压得到jpg，用winhex打开即可看到flag

**6.linux**

直接解压，flag文件丢进 notepad 搜key关键字  
key{feb81d3834e2423c9903f4755464060b}

**7.中国菜刀**

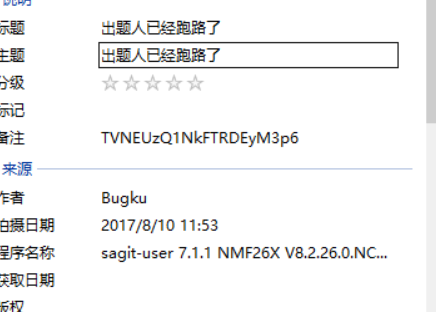
压缩文件里面有一个pcapng文件，用wireshark打开，

分离出包含的http对象，有一个zip文件  
解压--得到flag

**8.** **BugkuCTF\_杂项\_细心的大象 WriteUp**

下载下来一个压缩文件，解压出来后是一个图片，binwalk分析了一下，里面还包含其他文件，于是继续分离。  
又搞出来个一个压缩 文件，里面是一个PNG文件，压缩包有密码

查看图片属性，发现了BASE64码



进行BASE64解密后，得到一张png，然后老方法，但不太正常，修改高度

保存后再打开图片即可看到flag

**9.** **BugkuCTF\_杂项\_流量分析(cnss) WriteUp**

题目给了一个流量包 用wireshark 打开  
随便追踪一下TCP流



访问该网址即可在网页上找到flag的base64密码

WTI1emMzdGlNV3hwWW1sc01WOUJYMmRoZVY5M1JXSnphWFJsZlE9PQ==

base64二次解密即可得到flag