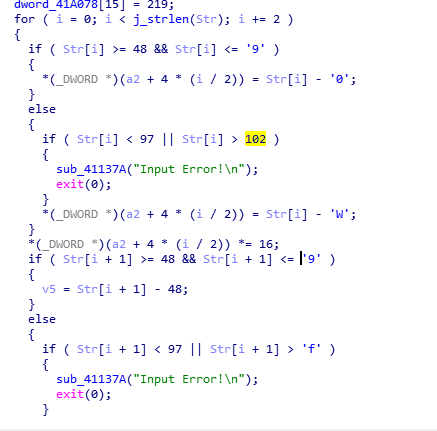
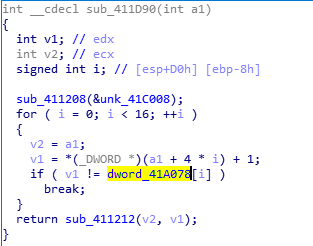
程序加了upx壳，脱壳后拖进ida进行分析。

然后有一堆操作，我们直接看处理flag的sub\_414E50，



很轻松可以看出来这是将输入的hex-string转换成内存中的bytse。

然后在sub\_411D90中进行+1操作后，和dword\_41A078地址的数据进行比较。



然后写出脚本即可。

arr = [0x50,0xc6,0xf1,0xe4,0xe3,0xe2,0x9a,0xa1,0xa7,0xde,0xda,0x46,0xab,0x2e,0xff,0xdb]  
flag = ""  
for i in range(len(arr)):  
 flag += "%x"%(arr[i] - 1)  
print flag

得到flag **4fc5f0e3e2e199a0a6ddd945aa2dfeda**