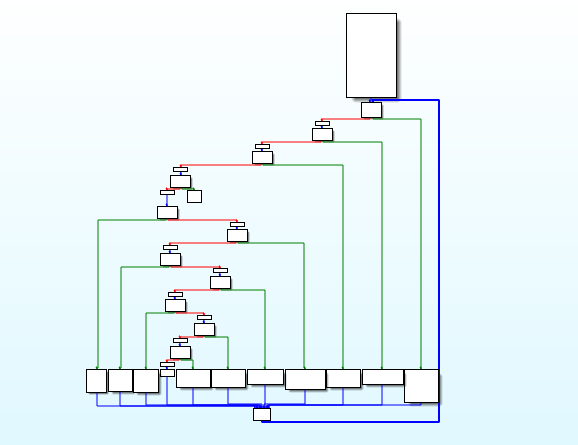
# 题目分析

拖进IDA可以判断使用ollvm指令流平坦化。



然后我们看到有5个fun\_check，来分析一下。

Fun\_check1



Fun\_check2



Fun\_check3



Fun\_check4



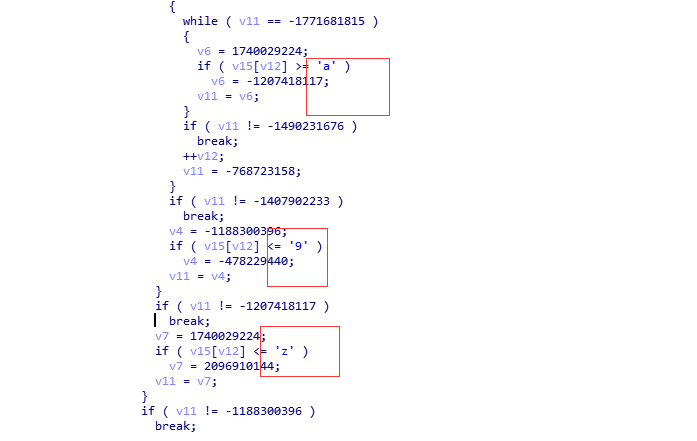
Fun\_check5

通过前四个check我们大致判断出flag格式为

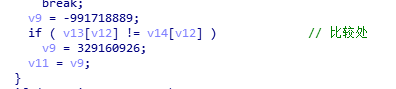
flag{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

进入check5我们通过看代码和IDA远程动态调试elf文件，输入一些数字和大小写字母，可以判断，check5只处理’0’-‘9’和’a’ – ‘z’的字符，以及如果是’ - ‘ 就不变。

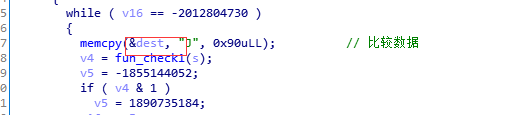
处理’0’-‘9’是ascii值+17，处理’a’ – ‘z’是ascii值-48。



然后我们可以找到check5处理后的数据比较的地方。



比较数据在这里，我们通过动态调试设断点可以得到” J2261C63-3I2I-EGE4-IBCC-IE41A5I5F4HB”。



# 脚本

data = "J2261C63-3I2I-EGE4-IBCC-IE41A5I5F4HB"  
flag = "flag{"  
for i in range(len(data)):  
 if(ord(data[i]) >= ord("A") and ord(data[i]) <= ord("J")):  
 flag += chr(ord(data[i]) - 17)  
 continue  
 if(ord(data[i]) >= ord("1") and ord(data[i]) < ord("A")):  
 flag += chr(ord(data[i]) + 48)  
 continue  
 else:  
 flag += "-"  
flag += '}'  
print flag

# flag{9bbfa2fc-c8b8-464d-8122-84da0e8e5d71}