目录

[Reverse 2](#_Toc20330)

[一. IDA 2](#_Toc23420)

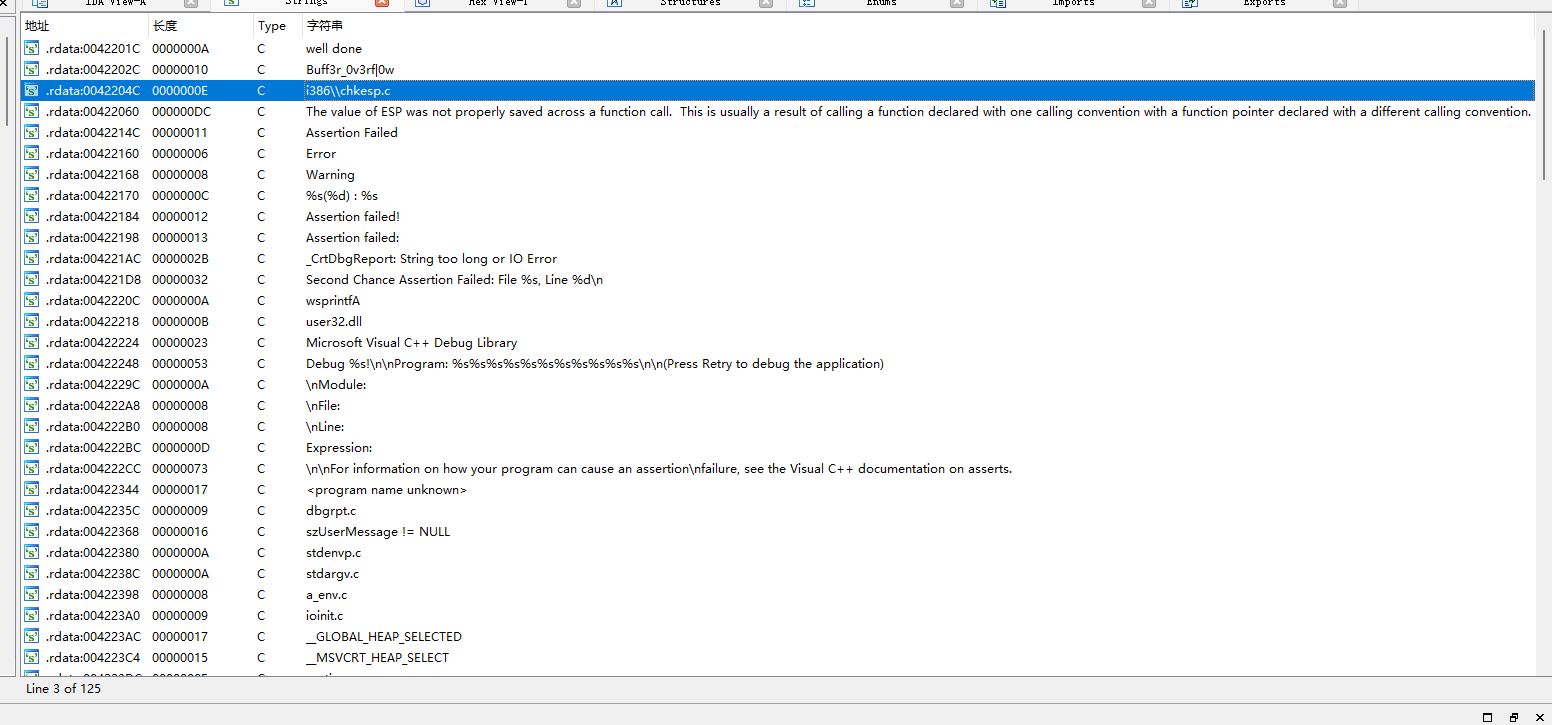
[二. C语言语法 4](#_Toc7222)

[三. 脱壳 6](#_Toc8740)

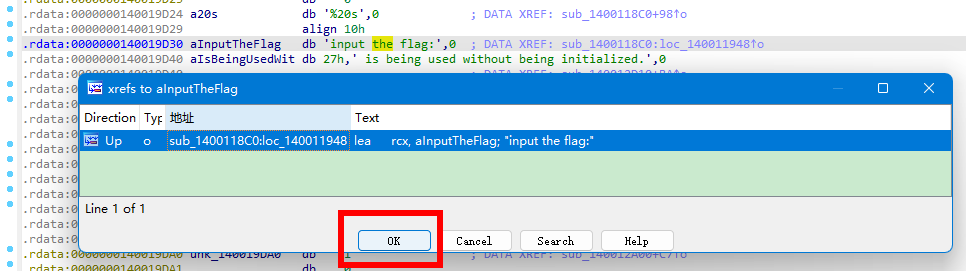
# Reverse

## IDA

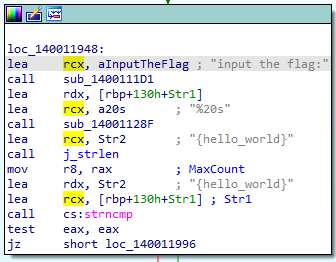
SHIFT+F12查看所有IDA程序中字符串，双击字符串进入内部查看



Ctrl+X查看当前引用位置

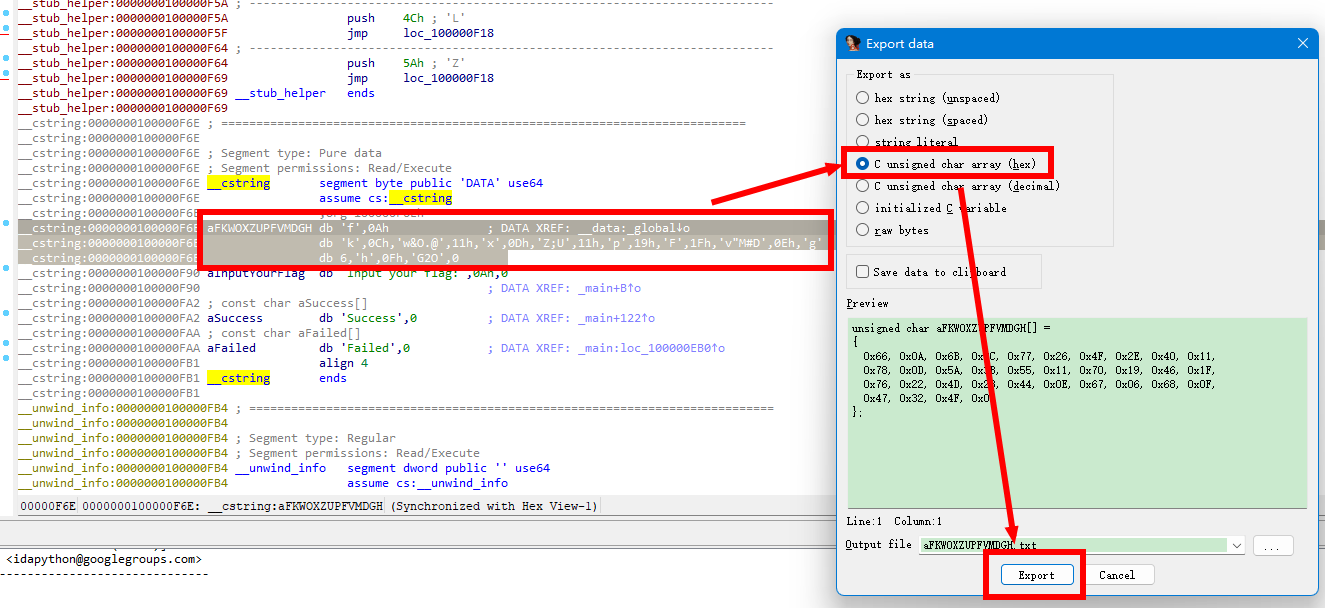


点击OK查看

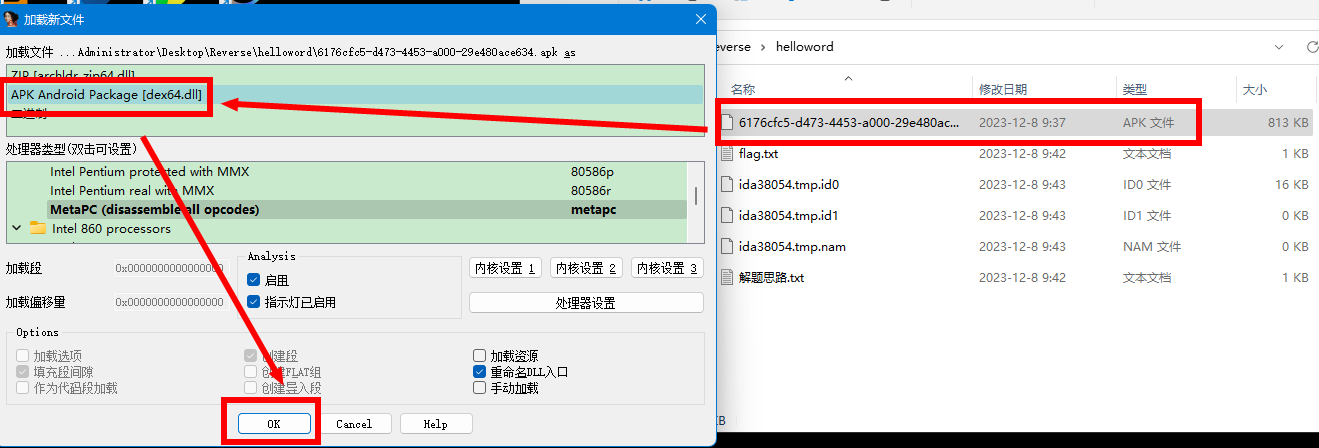


Esc回退

选中数据Shift+E可以将数据导出为任意格式

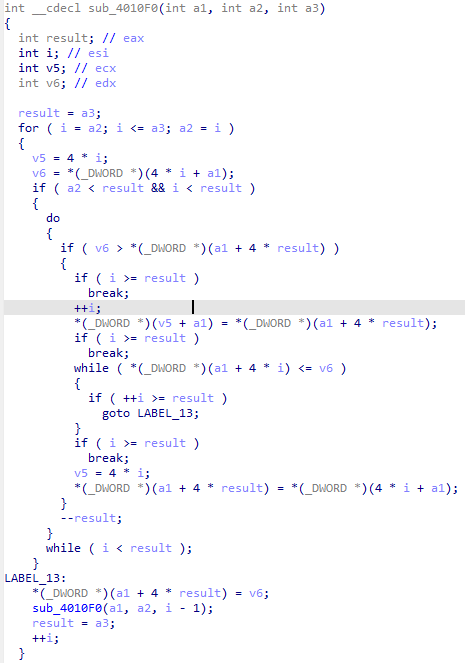


IDA查看APK文件



IDA字符串格式转换：右键字符串选择格式即可

伪代码转换为C语言代码，按F5同时双击

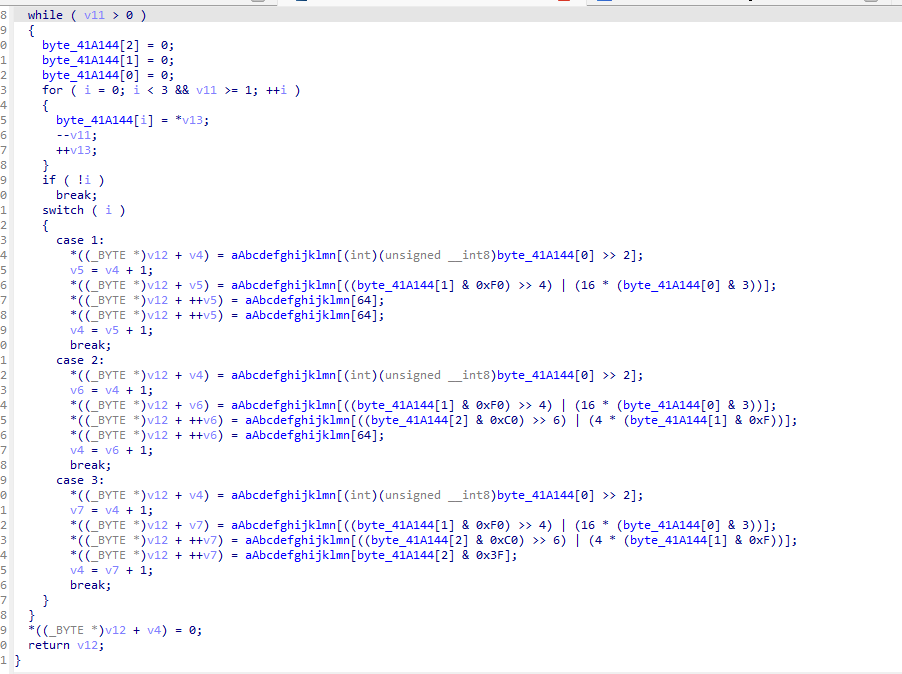


## C语言语法

atoi(x)：x为string，将字符串转为整数，注意”123xyz”会变成123，”-12.34”会变成-12，”123w45”会变成123，” 123w456”会变成123，”123 456”会变成123

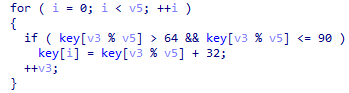
strncmp(a, b, 0x21uLL)代表：将字符串a和字符串b的前0x21个字符进行比较

BASE64方法代码



strcat(a, b)代表：得到字符串为a+b

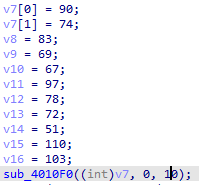
IDA的大小写转换方法代码



int占四个字节，所以需要\*4。如果是char类型或者系统作为下标，就不需要，例如a1 + result \* 4的值就是a1[result]，而v5+a1的值就是a1[v5]



IDA伪代码中，例如v开头接数字的，表示为一个字符串，如果函数调用(int)v7，则代表从7开始后的字符串的int数组，例如下面的v实际上是：ZJSECaNH3ng



## 脱壳

工具脱壳，将文件拖入万能脱壳助手后点击脱壳得到脱壳后的文件

