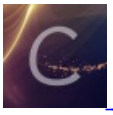
【reversing.kr逆向之旅】ImagePrc的writeup

原创

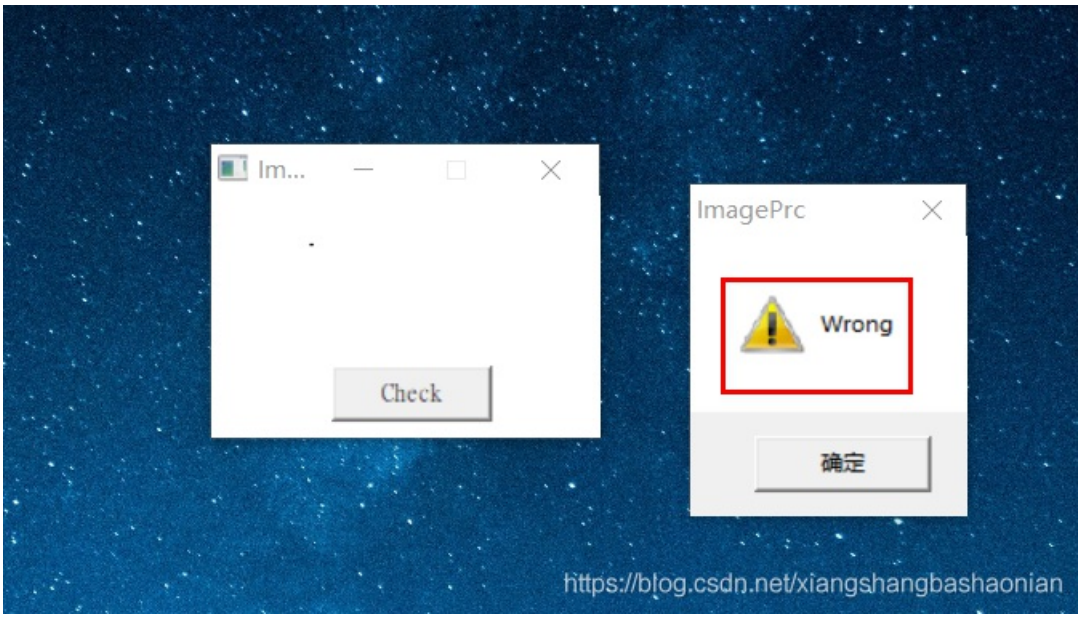
iqiqiya 于 2018-11-10 12:20:36 发布 355 收藏
分类专栏： 我的逆向之路 ------reversing.kr 我的CTF之路 文章标签： 【reversing.kr逆向之旅】ImagePrc的wri ImagePrc reversing.kr 逆向writeup reversing.kr


我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏

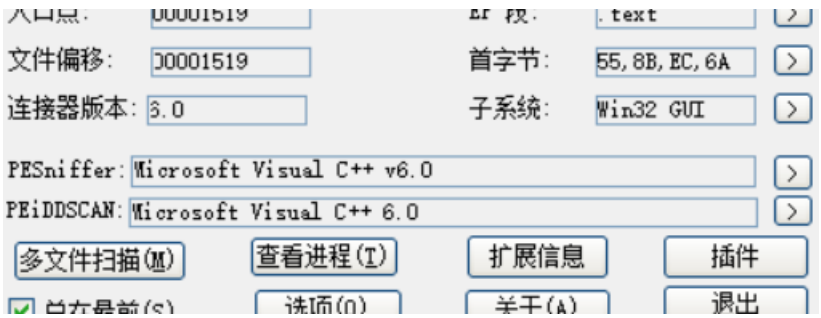

------reversing.kr
11 篇文章 0 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏

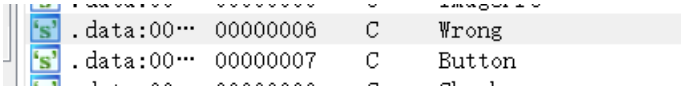
看到这道题有点懵 运行后只有一个Check按钮 中间是空白的 不知道什么鬼(最后才知道是个绘图板)



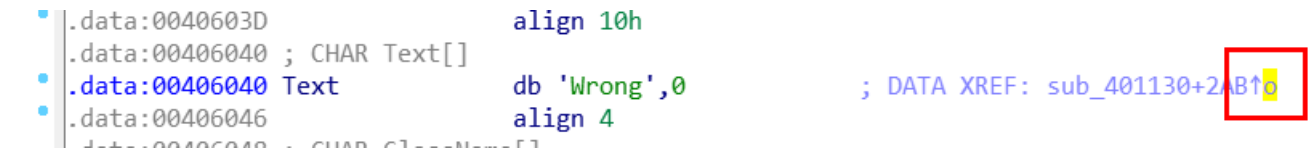
PEiD载入 发现还是没壳 Vc++6.0编写的程序



IDA载入进行分析　首先还是Shift+F12　查找关键字符串



双击



再双击　接着F5看伪代码　看不大懂　不过可以搜下bmiHeader

```
61    }
62    if ( wParam == 100 )
63    {
64      GetObjectA(hbm, 24, &pv);
65      memset(&bmi, 0, 0x28u);
66      bmi.bmiHeader.biHeight = cLines;
67      bmi.bmiHeader.biWidth = v16;
68      bmi.bmiHeader.biSize = 40;
69      bmi.bmiHeader.biPlanes = 1;
70      bmi.bmiHeader.biBitCount = 24;
71      bmi.bmiHeader.biCompression = 0;
72      GetDIBits(hdc, (HBITMAP)hbm, 0, cLines, 0, &bmi, 0);
73      v8 = operator new(bmi.bmiHeader.biSizeImage);
74      GetDIBits(hdc, (HBITMAP)hbm, 0, cLines, v8, &bmi, 0);
75      v9 = FindResourceA(0, (LPCSTR)0x65, (LPCSTR)0x18);
76      v10 = LoadResource(0, v9);
77      v11 = LockResource(v10);
78      v12 = 0;
79      v13 = v8;
```


可以知道是和bmp位图有关

FindResourceA与LoadResource是关于资源的

下面的while循环就是比较　结合后面那个MessageBox

猜测就是程序会加载资源与什么进行比较

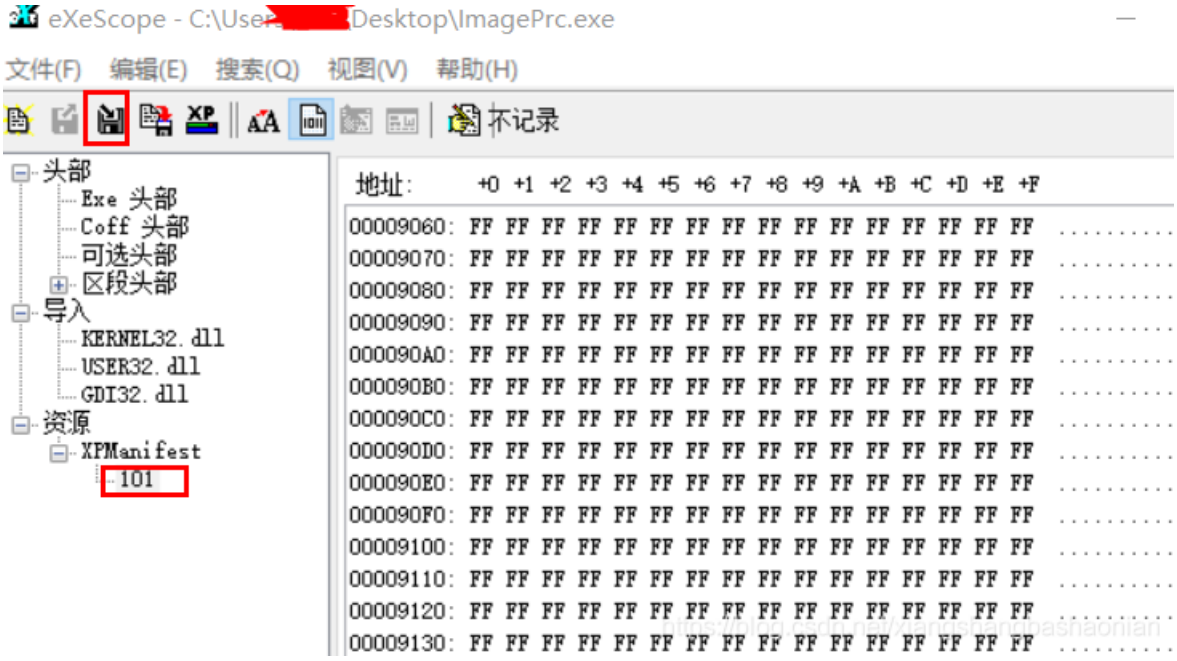
```
    v10 = LoadResource(0, v9);
    v11 = LockResource(v10);
    v12 = 0;
    v13 = v8;
    v14 = v11 - (_BYTE *)v8;
    while ( *v13 == v13[v14] )
    {
      ++v12;
      ++v13;
      if ( v12 >= 90000 )
      {
        sub_401500(v8);
        return 0;
      }
    }
    MessageBoxA(hWnd, Text, Caption, 0x30u);
    sub_401500(v8);
    return 0;
  }
  return 0;
}
```

这是错误弹窗

看了一些师傅的writeup

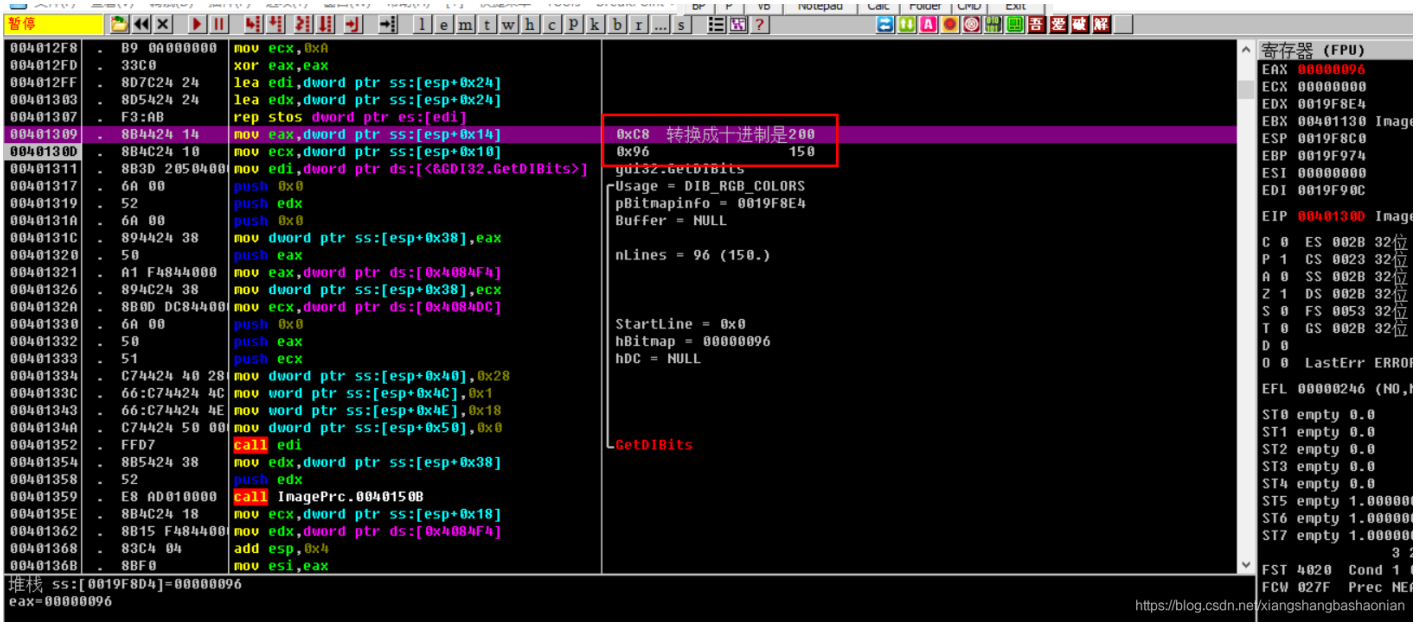
用exescope可以提取出这个资源文件 也就是bmp图片

打开 双击101　点击上方工具栏　命名为dump　导出



用python脚本还原成bmp图片

那么怎么确定图片的高度以及宽度呢　这里需要载入OD来确定



脚本来自:http://www.mottoin.com/article/reverse/88447.html

```
from PIL import Image

width = 200
height = 150

image_file = open('dump', 'rb')
data = image_file.read()
image = Image.frombuffer('RGB', (width, height), data, 'raw', 'RGB')
image = image.transpose(Image.FLIP_TOP_BOTTOM)
image.show()
image_file.close()
```

得到

答案就是GOT

这道题真的让我涨姿势了