2021红明谷杯数据安全大赛技能场景赛 Input Monitor

原创

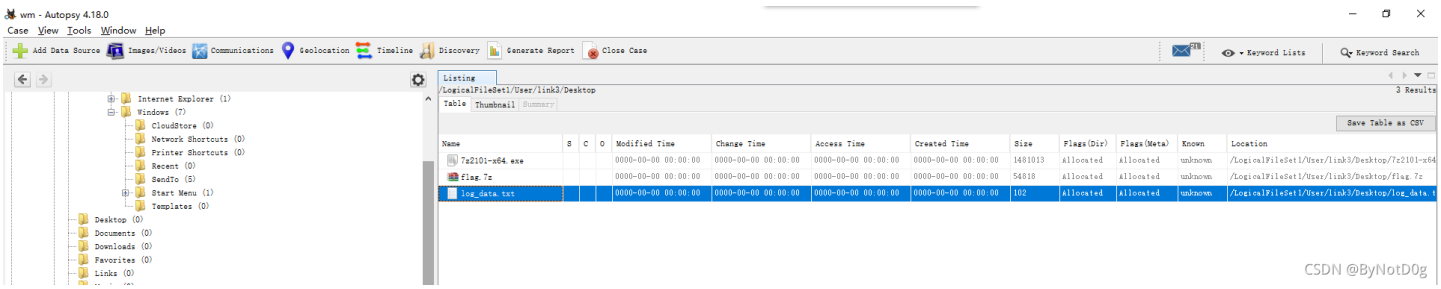
ByNotD0g 于 2021-09-25 15:33:36 发布 1180 收藏

分类专栏： 笔记 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_45805993/article/details/120472334

突然想起这个题…

先用autopsy挂载给的文件



桌面有压缩包和hint

> 没事，我都删掉了，之前的聊天记录都被我清干净了。除非他们在监控我输入

提示要得到输入记录

用到输入法取证https://mp.weixin.qq.com/s/0p3vbLub5vPKO5Pik9zmUQ

通过对Win10系统自带中文输入法程序运行进程的分析，发现与中文输入法相关的用户词库文件主要存储在

C:\Users\Administrator\AppData\Roaming\Microsoft\InputMethod\Chs

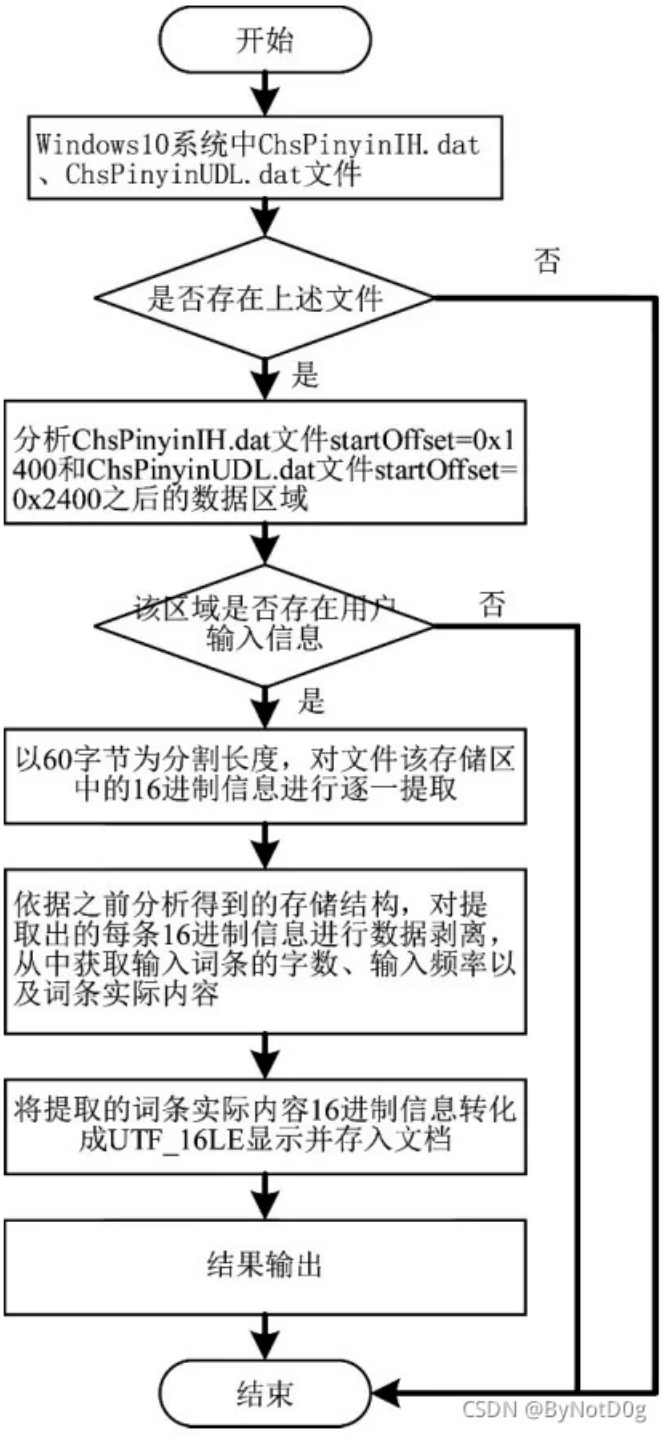
路径下，对所有文件的属性信息分析，发现其中文件名分别为**ChsPinyinIH**和**ChsPinyinUDL**的两个DAT文件，其属性信息会随着系统用户输入行为的发生而不断变化。但由于其是DAT类型文件，无法直接用常规方法获取记录信息。

因此，利用Winhex对这两个文件进行分析，如图1所示，发现存储的信息具有一定规律性，数据块之间存在明显分隔，并且在Unicode方式显示下，可以很明显发现文件名分别为ChsPinyinIH和ChsPinyinUDL的DAT文件中零散存储着系统用户之前输入的字词句信息，并且均以Unicode明码的方式保存在数据区中。

进一步分析ChsPinyinIH.dat和ChsPinyinUDL.dat两文件,发现ChsPinyinIH.dat文件记录着系统用户的中文字词输入信息，而ChsPinyinUDL.dat文件记录着系统用户的中文短句输入信息。

由此可知，Win10中文输入法用户词库信息采用独有格式进行存储，但没有采用复杂的加密算法对其进行保护处理

具体程序流程，如图所示。首先，分别检索ChsPinyinlH和ChsPinyinUDL两个DAT格式用户词库文件中偏移地址在0x1400和0x2400之后的数据区域；然后，对该区域数据信息按特定长度进行分割，并对分割出的每条信息进行格式解析，从中提取用户输入词条字数、输入频次、词条内容等关键信息；最后，将提取出的信息进行编码转换并输出。



注意该dat文件是UTF_16LE的格式，可以修改文件头两个字节（BOM）为FF FE然后在记事本直接打开

> BOM是用来判断文本文件是哪一种Unicode编码的标记，其本身是一个Unicode字符（"\uFEFF"），位于文本文件头部。

用六位汉字密码解开zip，flag就藏在pdf中