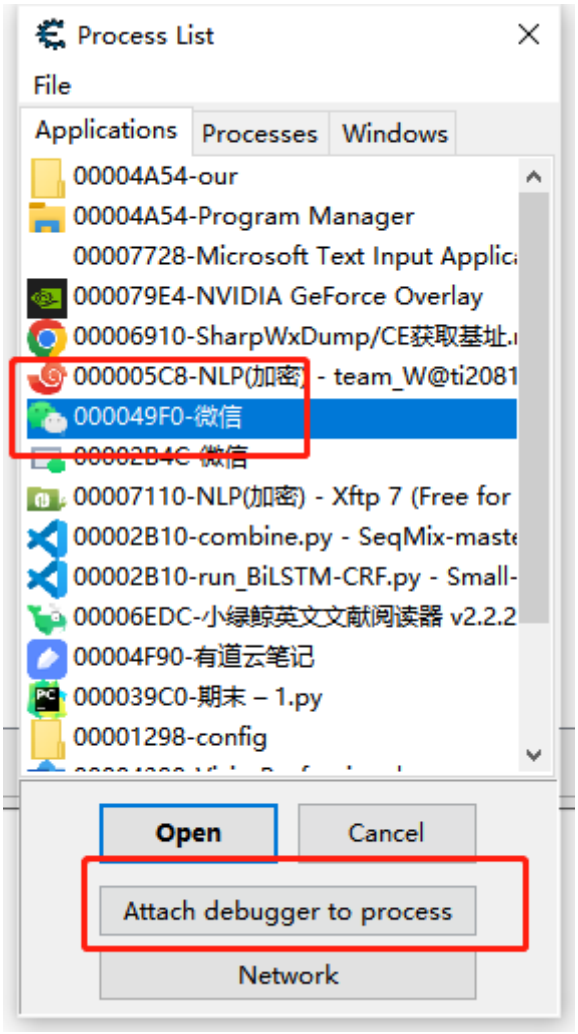
1. 安装 Cheat Engine

2. 使用（此处为3.9.2.26前的32位版本，64位同理）

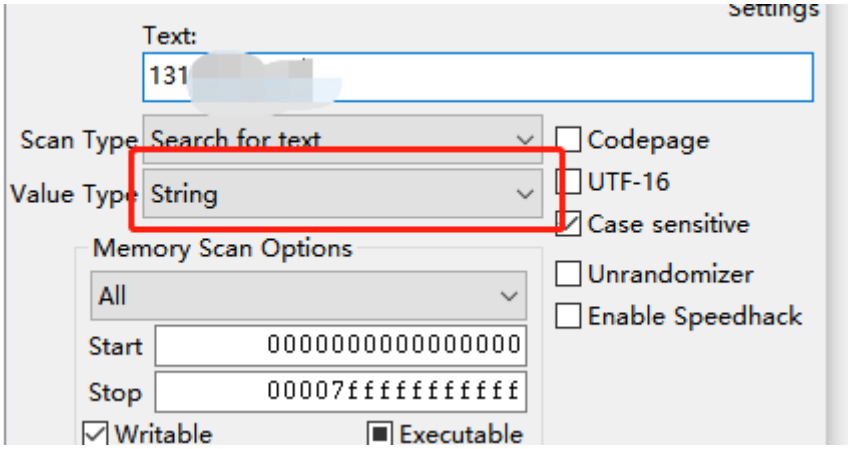
2.1 附加wx进程

保证微信的登录状态

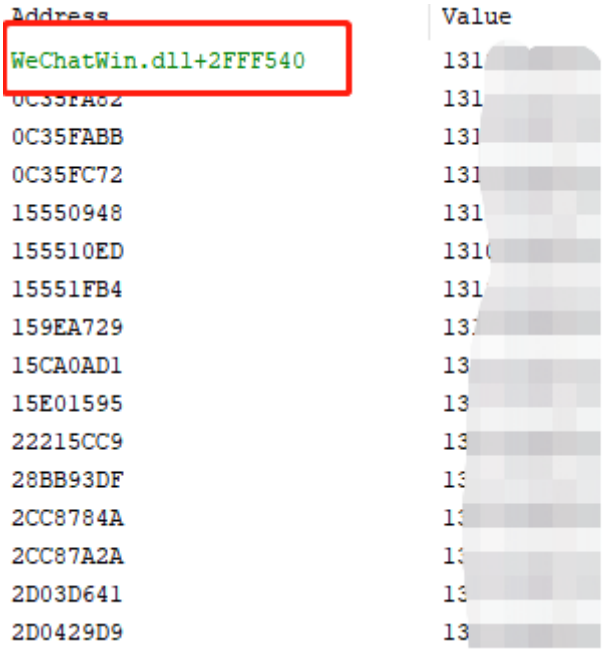


2.2 根据个人信息搜索对应偏移

此处示例手机号，在搜索框中指定当前登录微信的手机号等信息



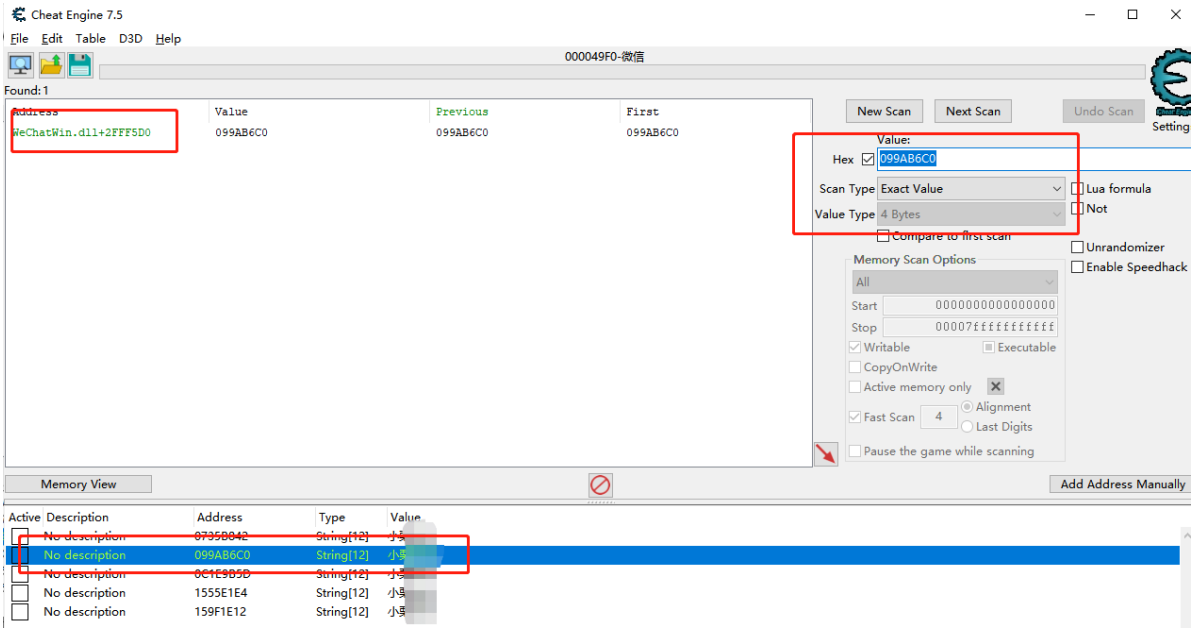
搜索后，红框这种为根据对应动态链接库基址（WeChatWin.dll+十六进制数），当中的十六进制数即为对应偏移



对于用户名字这些，含有不定长度，且存在中文的可能性的，除纯英文字符名为直接偏移地址可读取外，可能同一偏移下存取的为用户字符名

举例类似于微信名为中文名

可搜索到大量这种未带WechatWin.dll开头的直接地址,可通过一个一个查询或是临时改名等方式，确定其原本指针位置



此处我就通过随机点地址，并通过在内存中查找该地址的值去寻找指针位置，当显示也为偏移位置时即成功

对于数据库密钥也是偏移指针给出，同时自你登录某一账号在某一PC上时，在这个PC内，你的数据库密钥就是唯一的。

由于你自己的数据库密钥未知，所以需要通过网上披露的版本位移正确找到你自己的密钥一次，之后就可以通过密钥内容不断查找到新版本中的aeskey偏移。

3.局限

事实上，我们听闻这些两两偏移信息间的位置是相对固定的，所以参照过其它仓库与网络披露的代码去实现通过计算其中一个信息的偏移位置来推演其他信息的位置，但似乎随着版本的更新，带偏移信息之间的相对偏移并不固定，有时会变，故只能做成静态读取偏移的方式。