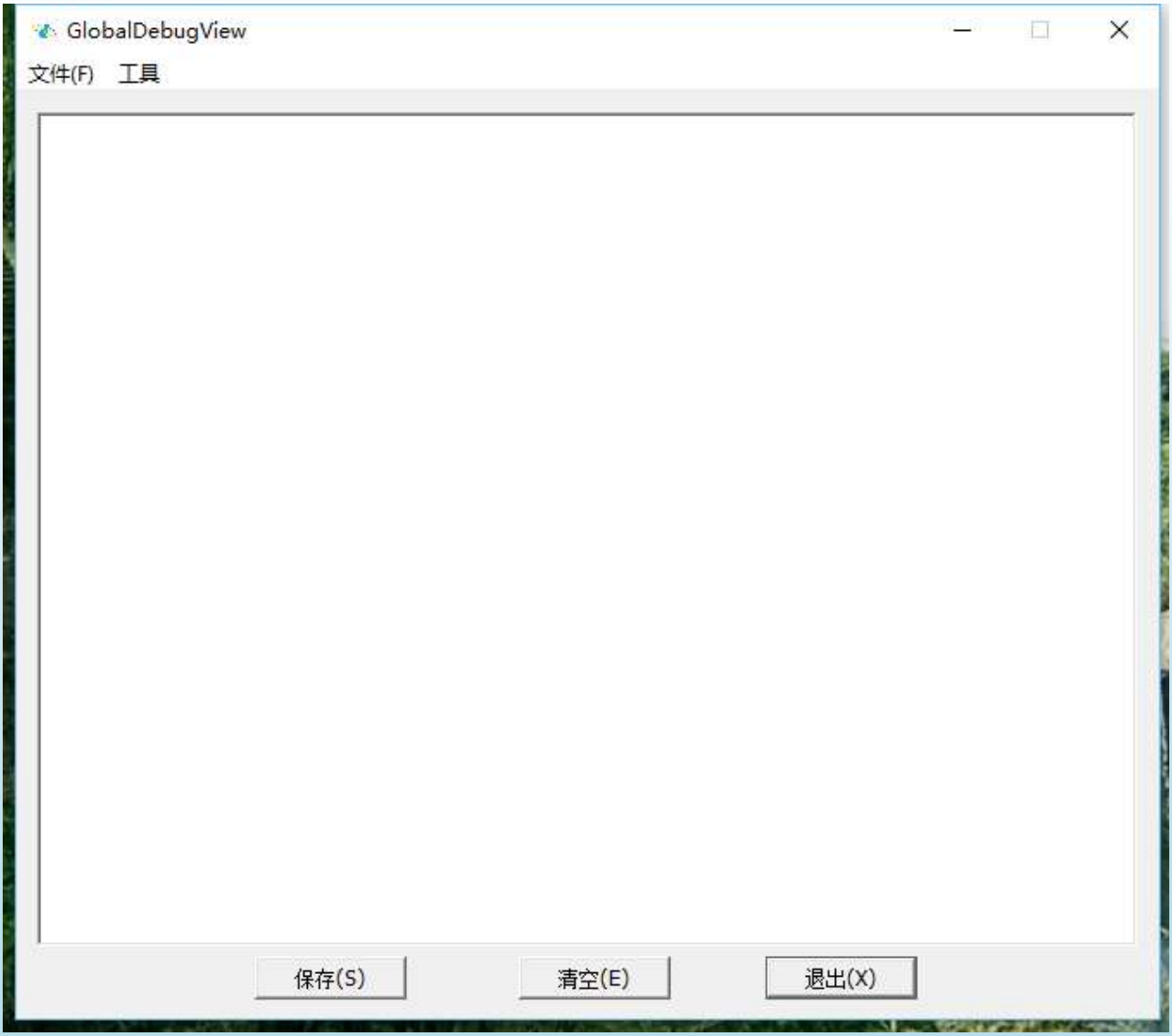
GlobalDebugView

关于 GlobalDebugView?

本人曾使用 API 拦截技术开发出 DebugView(非 Sysinternals 公司的 DbView)，但是这个程序是进程级的，也就是说，只有被此程序加载的进程才会被监控。当然，这也有这个特点的也有一定的优越性，那就是输出较少，容易理解。

GlobalDebugView 是继 DebugView 的一个全局监控软件，以 Windows Hook 技术注入 DLL，以达到全局监视的功能。



如何使用？

1. 此程序具有自动监视/软件代码配合监视两大功能。为什么要分为两种呢？第一个原因是为了避免调试过程中其他软件与目标被调试程序的输出混合，导致混乱。第二个原因是因为 GlobalDebugView 需要 Windows 消息来驱动载入 DLL 才能开启监视，也就是说，在目标被调试程序未创建窗口受到任何消息前，GlobalDebugView 不能拦截 API(因为 DLL 还未被注入)
2. 自动监视不必说，那么软件代码配合监视该如何使用呢?在程序代码中需要开始被监视的位置前写一行代码：

LoadLibrary(_T("GlobalDebugViewDll.dll"));

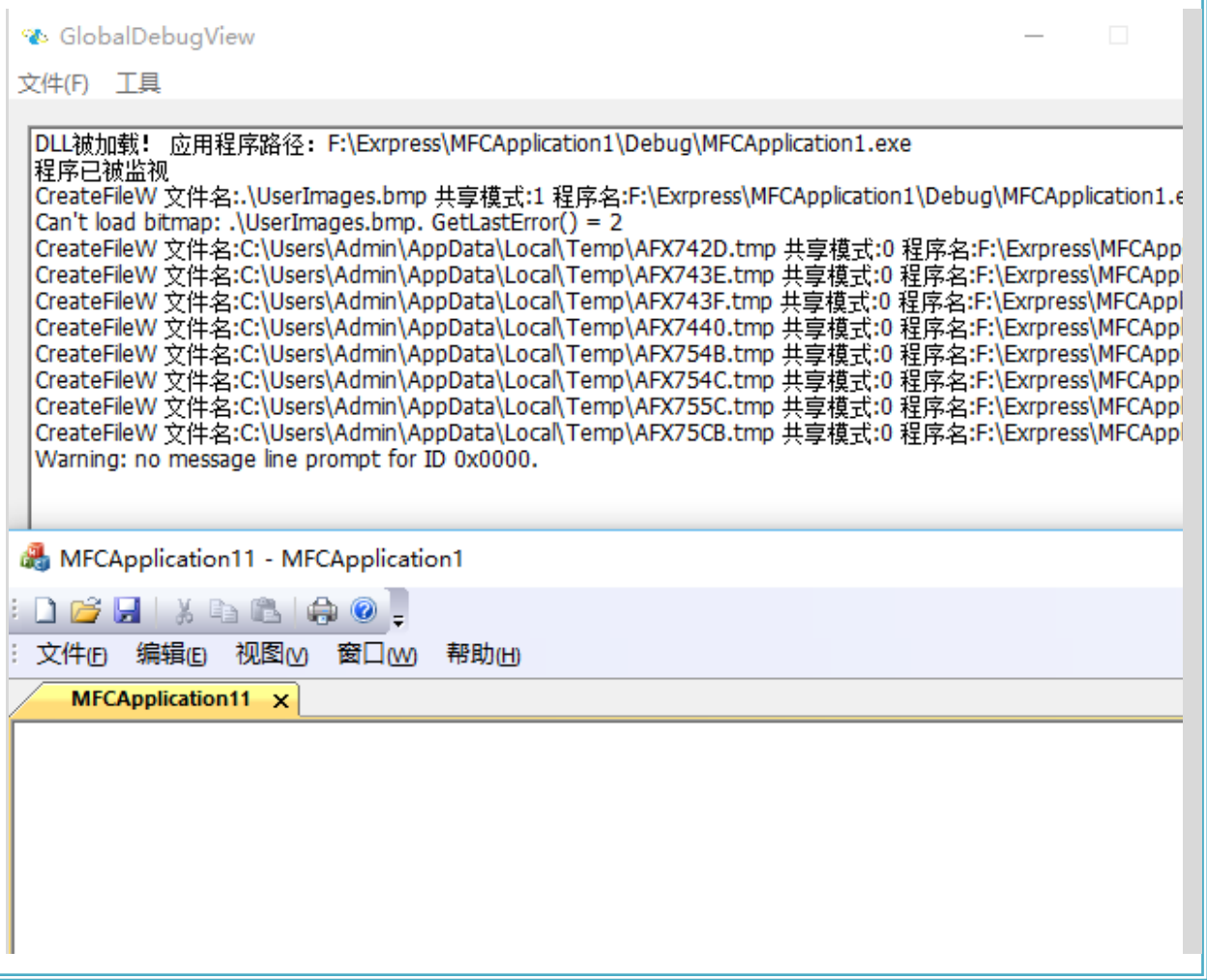
```
int APIENTRY _tWinMain(_In_ HINSTANCE hInstance,
                       _In_opt_ HINSTANCE hPrevInstance,
                       _In_ LPTSTR    lpCmdLine,
                       _In_ int       nCmdShow)
{
    UNREFERENCED_PARAMETER(hPrevInstance);
    UNREFERENCED_PARAMETER(lpCmdLine);

    // TODO: 在此放置代码。
    LoadLibrary(_T("GlobalDebugViewDll.dll"));
```

```
CMFCApplication1App::CMFCApplication1App()
{
    LoadLibrary(_T("GlobalDebugViewDll.dll"));
    TRACE("程序已被监视");
```

当然，要确保 GlobalDebugViewDll.dll 在目标被调试程序目录：

这时，启动程序，在 GlobalDebugView 中什么也不用做，等待输出就是了！

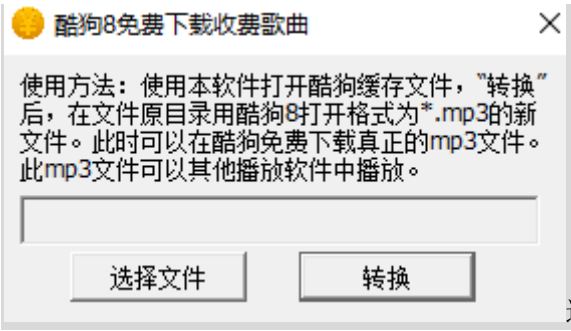


当然，如果要捕获程序已产生消息后的输出或函数调用，用自动监视更为方便，而且在新版 GlobalDebugView 中，还可以利用“筛选进程”选项来筛选你想要的信息，这样就不用为自动监视过多的输出而烦恼。

以下是使用 GlobalDebugView 捕获酷狗的 API 函数调用（自动监视）：

```
CreateFileW 文件名:E:\KuGou\Temp\aeab3f912ec0032264aaa4541b7bf766.kgtemp 共享模式:3 程序名:C:\Progra
CreateFileW 文件名:E:\KuGou\Temp\aeab3f912ec0032264aaa4541b7bf766.kgtemp 共享模式:3 程序名:C:\Progra
CreateThread 线程函数:591778404 父窗口:153464120 标志:0 新线程句柄:8528 程序名:C:\Program Files (x86)\Ku
CreateFileW 文件名:\\.\E: 共享模式:3 程序名:C:\Program Files (x86)\KuGou\KGMusic\KuGou.exe
CreateFileW 文件名:E:\KuGou\Temp\aeab3f912ec0032264aaa4541b7bf766.kgtemp 共享模式:3 程序名:C:\Progra
CreateFileW 文件名:E:\KuGou\Temp\aeab3f912ec0032264aaa4541b7bf766.kgtemp 共享模式:3 程序名:C:\Progra
CreateThread 线程函数:1734261200 父窗口:166802636 标志:0 新线程句柄:9140 程序名:C:\Program Files (x86)\K
CreateFileW 文件名:E:\KuGou\Lyric\李行亮 - 原来都是梦-ef3bfc0d06c3c26d43fe09eba693a936-20353092-000000
CreateFileW 文件名:\\.\E: 共享模式:3 程序名:C:\Program Files (x86)\KuGou\KGMusic\KuGou.exe
CreateThread 线程函数:591778404 父窗口:186825848 标志:0 新线程句柄:9124 程序名:C:\Program Files (x86)\Ku
CreateFileW 文件名:E:\KuGou\Lyric\林俊杰 - 江南-aeab3f912ec0032264aaa4541b7bf766-16054629-00000000.kr
CreateThread 线程函数:591778404 父窗口:153463040 标志:0 新线程句柄:9228 程序名:C:\Program Files (x86)\Ku
CreateFileW 文件名:C:\Users\Admin\AppData\Roaming\KuGou8\SingerRes\林俊杰_1574\120\2016032517594238
CreateFileW 文件名:C:\Users\Admin\AppData\Roaming\KuGou8\SingerRes\林俊杰_1574\120\2016032517594238
CreateThread 线程函数:1805828020 父窗口:43501904 标志:0 新线程句柄:1840 程序名:C:\Program Files (x86)\Ku
CreateFileW 文件名:C:\Users\Admin\AppData\Roaming\KuGou8\playlistV3.db-journal 共享模式:3 程序名:C:\Prograr
CreateFileW 文件名:C:\Users\Admin\AppData\Local\Temp\etilqs_mMGVIZzsS1500Kf 共享模式:3 程序名:C:\Prograr
CreateFileW 文件名:C:\Users\Admin\AppData\Roaming\KuGou8\KGMusicV3.db-journal 共享模式:3 程序名:C:\Progr
CreateFileW 文件名:C:\Users\Admin\AppData\Local\Temp\etilqs_JRPObKZLEEO0zyE 共享模式:3 程序名:C:\Prograr
```

这是一个破解软件中必须的重要功能。使用这个软件，我成功开发出了能够免费下载酷狗 8 收费歌曲的软件：



这个软件就是通过利用 GlobalDebugView 捕获酷狗 CreateFile 的调用，并通过破解其缓存文件来达到目的。而且通过 GlobalDebugView，我还发现了网易云、百度音乐一些收费歌曲的免费下载方法，只有 QQ 音乐是稍复杂的，作者本人至今未能破解。

如何合法利用 GlobalDebugView?

1. 传播本软件时请注明开发者。
2. 利用本软件破解其他程序时，应尊重软件开发者的智力成果，做一个合格的消费者!
3. 本软件仅供学习研究目的，不得将本软件用于非法范围。