Win32调试API第三部分 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022_Win32_E8_B0_83_E8_AF_c98_259396.htm 理论:如果你以前使用过调试器，那么你应对跟踪比较熟悉。当"跟踪"一个程序时，程序在每执行一条指令后将会停止，这使你有机会去检查寄存器/内存中的值。这种单步运行的官方定义为跟踪(tracing)。单步运行的特色是由CPU本身提供的。标志寄存器的第8位称为陷阱标志trap flag。如果该位设置，则CPU运行于单步模式。CPU将在每条指令后产生一个debug异常。当debug 异常产生后，陷阱标志自动清除。利用win32调试api，我们也可以单步运行被调试程序。方法如下: 调用GetThreadContext, 指定 ContextFlags为CONTEXT_CONTROL， 来获得标志寄存器的值 设置CONTEXT结构成员标志寄存器regFlag中的陷阱标志位 调用 SetThreadContext 等待调式事件。被调试程序将按单步模式执行，在每执行一条指令后，我们将得到调试 事件，u.Exception.pExceptionRecord.ExceptionCode值为EXCEPTION_SINGLE_STEP 如果要跟踪下一条指令，需要再次设置陷阱标志位。 例:.386.model flat,stdcall option casemap:none include \masm32\include\windows.inc include \masm32\include\kernel32.inc include \masm32\include\comdlg32.inc include \masm32\include\user32.inc includelib \masm32\lib\kernel32.lib includelib \masm32\lib\comdlg32.lib includelib \masm32\lib\user32.lib .data AppName db "Win32 Debug Example no.4",0 ofn OPENFILENAME FilterString db "Executable

Files",0,"*.exe",0 db "All Files",0,"*.*",0,0 ExitProc db "The debuggee exits",0Dh,0Ah db "Total Instructions executed : %lu",0 TotalInstruction dd 0.data? buffer db 512 dup(?) startinfo STARTUPINFO pi PROCESS_INFORMATION DBEvent DEBUG_EVENT context CONTEXT .code start: mov ofn.lStructSize,SIZEOF ofn mov ofn.lpstrFilter, OFFSET FilterString mov ofn.lpstrFile, OFFSET buffer mov ofn.nMaxFile,512 mov ofn.Flags, OFN_FILEMUSTEXIST or OFN_PATHMUSTEXIST or OFN_LONGNAMES or OFN_EXPLORER or OFN_HIDEREADONLY invoke GetOpenFileName, ADDR ofn .if eax==TRUE invoke GetStartupInfo,addr startinfo invoke CreateProcess, addr buffer, NULL, NULL, NULL, FALSE, DEBUG_PROCESS DEBUG_ONLY_THIS_PROCESS, NULL, NULL, addr startinfo, addr pi .while TRUE invoke WaitForDebugEvent, addr DBEvent, INFINITE .if DBEvent.dwDebugEventCode==EXIT_PROCESS_DEBUG_EVENT invoke wsprintf, addr buffer, addr ExitProc, TotalInstruction invoke MessageBox, 0, addr buffer, addr AppName, MB_OK MB_ICONINFORMATION .break .elseif DBEvent.dwDebugEventCode==EXCEPTION_DEBUG_EVENT .if DBEvent.u.Exception.pExceptionRecord.ExceptionCode==EXCEPTION_BREAKPOINT mov context.ContextFlags, CONTEXT_CONTROL invoke GetThreadContext, pi.hThread, addr context or context.regFlag,100h invoke SetThreadContext,pi.hThread, addr context invoke

ContinueDebugEvent, DBEvent.dwProcessId, DBEvent.dwThreadId, DBG_CONTINUE .continue .elseif DBEvent.u.Exception.pExceptionRecord.ExceptionCode==EXCEPTION_SINGLE_STEP inc TotalInstruction invoke GetThreadContext,pi.hThread,addr context or context.regFlag,100h invoke SetThreadContext,pi.hThread, addr context invoke ContinueDebugEvent, DBEvent.dwProcessId, DBEvent.dwThreadId,DBG_CONTINUE .continue .endif .endif invoke ContinueDebugEvent, DBEvent.dwProcessId, DBEvent.dwThreadId, DBG_EXCEPTION_NOT_HANDLED .endw .endif invoke CloseHandle,pi.hProcess invoke CloseHandle,pi.hThread invoke ExitProcess, 0 end start 