

# 如何使用 WinDBG 跟踪调试 ASL/ACPI?

在现代计算机中，硬件和固件（BIOS）都必须符合 ACPI 规范，以便操作系统可以控制所有模块的自动配置和电源管理。使用 WinDbg 调试 ACPI 代码通常需要两台计算机，一台是目标机（Debuggee），另一台作为主机（Debugger）。下面就介绍一下怎么在两台机器上建立调试环境。

## 1. 配置调试 Debuggee 的连接方式

Windbg 支持 COM 1394 USB2.0 三种不同的连接方式，看到网上有些文章关于使用 USB2.0 来连接，需要购买特殊的 USB 调试线，而且价格不菲，本篇文章就不讨论了。笔记本电脑一般都没有 COM 端口，只好使用 1394 或是 COM 转 USB，但在这里我只想讨论怎么使用 COM 端口来连接。

启动到操作系统，使用 bootcfg 命令或直接使用文本编辑器修改 boot.ini 文件，指定调试使用的端口及参数。为了使用 COM 端口来调试，需要在启动参数中加入 /debug 参数，并指定 /debugport 和 /baudrate 子参数来作为启动项。下面这个 boot.ini 文件的第一个启动项就是配置使用 COM 端口。/debugport 子参数指出使用 Debuggee 的哪个 COM 口，/baudrate 指出连接的速度（默认是每秒 19200 位）。

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Debugging with Cable" /fastdetect /debug /debugport=COM1 /baudrate=57600
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /fastdetect
```

下面的例子使用 bootcfg 命令设置第一个启动项使用 COM1 端口、波特率为 115200 bootcfg 的 /debug 开关打开，/port 开关及 /baud 参数指出端口和速度，/ID 开关指出修改的是第一个启动项。

```
bootcfg /debug ON /port COM1 /baud 115200 /ID 1
```

## 2 建立 AML 调试环境

AML 调试器被包含在 checked 版（调试版）的 acpi.sys 中，为了完全使用 AML 调试器，这个驱动必须要安装在目标机上。尽管 Free 版（正式版）的 acpi.sys 支持一部分的 AMLI debugger 扩展命令，但它并没有包含 AMLI debugger。

如果你的目标机上已经安装 Windows 的 checked 版，运行的就是 checked 版的 acpi.sys。如果安装的是 free 版的 Windows，你可以选择重新安装一个完整的 checked 版或选择只安装 checked 版的 acpi.sys。（肯定是后一种方式方便

啊J)，我会在另外一篇文章中讲讲怎么在 free版的 Windows中安装 checked版的 acpi.sys

### 3 下载安装 Windbg

Windbg在微软网站上有免费下载，  
<http://www.microsoft.com/whdc/devtools/debugging/default.msp>，现在的版本是 6.6.7.5 安装它没有什么特别之处，如果你曾经在别的机器上安装过，直接拷贝到你现在的机器上也能用。看到某些帖子说最好安装路径上不要有空格，可能会出问题，但我一直没碰到过。

### 4 主机端符号 (Symbol) 文件路径配置

首先，什么是 symbol文件呢？Symbol文件包含了很多调试 DLL、EXE文件的时候需要的数据，但它们在程序运行的时候没什么用。通俗的说，Symbol File是包含了相关二进制文件 (EXE, DLL)调试信息的一种文件，它以 .pdb为扩展名。比如 Windows XP下有一个 GDI32.dll，那么微软在编译该 DLL的时候会产生一个 GDI32.pdb文件，程序员有了这个 PDB文件，愿意的话就可以用它来调试，跟踪到 GDI32.dll的内部去！一般来说，symbol文件包含一下内容：

- a.全局变量 (Global variables)
- b.局部变量 (Local variables)
- c.函数名和它们的入口地址 (Function names and the addresses of their entry points)
- d.FPO data(frame pointer omission), frame pointer是一种用来在调用堆栈 (Call stack)中找到下一个将要被调用的函数的数据结构源代码的行序号 (Source-line numbers)

该文件和二进制文件的编译版本密切相关，比如你修改了 DLL的输出函数等，再编译该 DLL那么原先的 PDB文件就过时了，不能再胜任调试的重担了，这时候你需要的是修改后编译产生的 PDB文件。所以，主机端使用的 Symbol文件一定要和目标机上安装的操作系统的版本要一致。

Symbol文件对于 Windbg来说是至关重要的，如果找不到正确的 Symbol文件，调试功能就没法使用。Windows的 Symbol文件可以在微软网站上免费下载，  
<http://www.microsoft.com/whdc/devtools/debugging/symbolpkg.msp>。可我不建议您这么做，因为不管是 Checked版的还是 Free版的 Symbol都有近 200M，下载过程相当痛苦。好在微软提供了 Symbol服务器，使得 Windbg可以自己在上面查找需要的模块。具体配置方法是：File- Symbol File Path..弹出符号文件对话框，输

入：  
SRV\*C:\Symbols\*http://msdl.microsoft.com/download/symbols,  
“C:\Symbols”可以是本地人一路径，用来保存下载的符号文件。

### 5 联机开始调试

A 启动目标机，当启动到启动菜单的时候，移动方向键，结束倒数计时，使它停在这个地方。

B 在主机上打开 Windbg, File- kernel Debug, 选择相应的连接方式，如果使用 COM端口的话，在对话框中填写主机使用的 COM端口以及所选择的波特率，波特率需要和目标机上的设置相同。

点击 OK就大功告成了，尝试使用 !aml i debugger命令启动 AMLI调试器，如果没什么动静，这就算成功了。开始调试你的 ACPI代码吧

## 如何在 Free 版的 Windows 上安装 Checked 版的 ACPI.sys [收藏](#)

调试 ACPI BIOS 与调试标准的内核代码有很大的不同。普通的驱动程序都是由某一特定的 CPU 的机器码组成，而 ACPI BIOS 不是。ACPI BIOS 是以 ACPI 机器语言 (AML) 的形式储存在 BIOS 芯片中，操作系统加载时被调入内存，由 AML 解释器解释执行。微软提供了一个调试工具来调试 AML 代码——Microsoft AMLI Debugger。这个工具并不是一个独立的程序，它由两部分组成：一部分存在于 Checked 版的 ACPI 驱动 ACPI.sys 中，另外一部分则包含在调试工具 WinDbg 中。为了使用完整的 AMLI Debugger 功能，您必须要安装 Checked 版的 ACPI.sys 到 Debuggee 上。

自从 Windows 9x/Me 以来，所有的 Windows 版本中都存在 AMLI Debugger。对于 Windows XP 及其后的版本中所带的 AMLI Debugger 可以完全处理 64 位 CPU，所以不管你的 Debuggee 和 Debugger 上的 CPU 是 32 还是 64 位的，都不会出现问题。

为了安装 checked 版的 ACPI.sys，您可以在 Debuggee 上安装一个完整的 Checked 版的操作系统，也可以单独安装 ACPI.sys 一个文件，其它模块都使用 Free 版的。后一种方法有以下优点：1、可以得到想要的 Debug 功能，而且不会被其它模块所干扰。2、简单。下面来讲一下具体怎么做。

一、首先你必须到微软网站上下载与你 Debuggee 上安装的操作系统的版本一致的 Checked 版本，这是免费的。2K 及 Xp sp1 <http://www.microsoft.com/whdc/DevTools/tools/chkblids.mspx> , XP sp2 : <http://download.microsoft.com/download/e/c/6/ec6e00ab-ec05-4673-b8db-0658cf65f043/WindowsXP-KB835935-SP2-DEBUG-ENU.exe>。

二、假设使用的是 Xpsp2，使用 Winrar 或别的解压缩软件将 i386\ACPI.sy\_解出来。由于该文件扩展名以下划线结尾，表示它是一个压缩文件，需要使用解压缩工具 (%SystemRoot%\system32\expand.exe)展开。比如，你可以在命令行提示符下输入 :> expand Acpi.sy\_ Acpi.sys。

三、进入安全模式，将展开的 ACPI.sys 覆盖 %SystemRoot%\system32\drivers\acpi.sys。提醒你要记得要把原有 Free 版做备份 J。

到现在，debuggee 上的 Checked 版的 Acpi.sys 算是安装完成了，但为了能使用 AMLI Debugger，还有一个工作不得不作。在我写的关于使用 WinDbg 调试 ACPI 的文章中说过，Debugger 上的 Symbol 版本需要和 Debuggee 上的操作系统的版本一致，否则 WinDbg 不能正常使用。为此，还需要下载对应的 Checked 版的 Symbol，将其中的 ACPI.pdb.sys 更名为

acpi.pdb , 替换 Free 版 symbol 的 sys\acpi.pdb。