

Using WinDbg in ASL debug and DTM test fail diagnostic

(不完整)

作者： 本文由 freevanx (freevanx@gmail.com) 起草，拥有版权。未经授权，不得转载、分发、传播。含有内部资料或者技术的部分文章内容，只开放给使用本公司 BIOS 的开发者参考。含有本文链接的地址可在下面找到：

http://docs.google.com/View?docID=0AXM7WqiAoyr_ZDk3dnI4el8zOTNobmt0a3BkOQ&a

2010 修订，加入 USB 2.0 debug

简介

WinDBG 在 BIOS 开发中主要作用：

1. 调试 ACPI ASL
2. 在 WHQL DTM 测试中，通过分析 dump 文件，用来诊断 fail 的原因
3. 系统安装失败（Bluescreen）后，分析失败原因，更正 BIOS 代码

一、使用 WinDBG 调试 ASL

下面是我简要介绍 WinDBG 使用方法的帖子，

我想大部分 BIOS 都会遇到 ASL debug 的问题。一般是用 debug card，但是这种方法简单是简单，太简单的方法总是不强大。。比较 powerful 的方法是利用 WinDBG 来 debug ASL，另外，可以利用 Linux kernel 中 ACPI driver 来 debug ASL，取得的效果和 WinDBG 差不多，但是一般的发行版都做不了这个，主要是 debug 选项没打开，虽然我也有心自己编译这样一个 kernel，不过因为没有需求，一直懒得做。。

那么我简单说一下该怎么设置，这个方法有个缺点，WinDBG 必须要和 Windows 连接上才能 debug，不过一般 ACPI 的 code 都是在 WinDBG 连上后才运行，所以没有这个担心。

WinDBG 采用 Host 和 Target 方法进行 debug，这是系统级 debug 常用的方法，使用 Host 机器 debug Target 机器，所以一般要两台机器。。

1. 首先把两台机器连起来，有 3 种连接方法

COM：常用的串口线就可以，但是现在 NB 上基本没有串口，在 Server 系统上现在串口还是比较常见，所以 debug Server 的话可以使用

IEEE1394：这个在 NB 上就比较常见了，Server 上基本没有，所以你的 NB 上有 1394 接口的话就可以用 1394

USB2.0 debug cable，这个要用一种特殊的 cable，国内没有卖的好像，国外的产品好像只有一种，利用 EHCI 的 debug port 输出 debug 信息。

那么最后，如果你这 3 种都没有，怎么办呢？那你 NB 上总有 PCIMCA 卡口吧，让你老板出血买个 PCIMCA 转 COM 口的东东吧~~不贵哦。。

2. 设置 target 机器, 使之可以 debug, 分两步

2.1 设置 OS 使之处于 debug mode, 详情参考 <http://msdn.microsoft.com/en-us/library/ms791518.aspx>, 其实有一个简单的办法, 使用 msconfig 这个程序, 设置 boot.ini->Advance->debug 选项

2.2 替换 Target 机器上的 acpi.sys 文件, 下载你对应 OS 的 checked build(就是 debug 版的意思), 例如 XP 或者 Server 2003, 现在公开拿到的也就是 XP 和 Server 2003, 其他 OS 都需要 MSDN 注册才能拿到, 假设我的 OS 是 Server 2003 SP1, 到微软网站找到这个版本的 checked build, 下载后解压, 到 i386 目录下找到 acpi.sy_, 这个文件是压缩的, 先用 expand 把它解压: expand acpi.sy_ acpi.sys, 然后把 target 机器 boot 到 safe mode, 先在 C 盘搜索 acpi.sys, 把能找到的都改名或者删除, 将从 checked build 中解压的 acpi.sys 替换 target 系统上 C:\Windows\system32\drivers\acpi.sys 这个文件, 重启~~~

这一段可以参考 <http://blog.csdn.net/EFIBIOS/archive/2007/03/12/1526763.aspx>

3. 设置 Host 机器

3.1 安装 WinDBG, 自己找, 不多说

3.2 配置 symbols, debug symbols 是 target 机器上各个程序函数, 变量等的地址。想要 debug target 系统, symbols 比不可少。在 <http://www.microsoft.com/whdc/DevTools/Debugging/symbolpkg.msp> 这里下作与 target 系统对应的 symbols, 注意, symbols 的版本必须与你 target 上面的 acpi.sys 的版本一致, 不然 debugger 就找不到 acpi.sys 和里面的 acpi debugger 了, checked build 必须使用 checked build 的 symbol file。。然后在 WinDBG 里面设定 symbols 的安装路径。。File 菜单下面。。注意看就能找到。。

然后运行 WinDBG-> kernel debug, 选择 COM 或者是 1394, 然后重启 target, 在 target OS 刚启动的时候, 可以看到 WinDBG 连接上的信息, 和 target OS 的信息, debug ACPI 的话, 可以在 OS 跑滚动条的时候按 CTRL+BREAK 把 target 停下来,

接着调试

4. !amli 看看

5. !amli debugger, 打开 acpi debugger, 如果没有什么反应, 说明成功, 如果有出错信息, 重新检查设置。

6. !amli set traceon

!amli set verboseon

!amli set spewon

打开全局调试输出, 打开这个以后所有 OS run 到的 asl code 都会输出来, 所以会非常慢, 如果你不是调试这里的 code, 那么到你 debug 以前的位置再设置这个。。

使用这个几个选项可以 trace OS 的 acpi 是怎么跑的,

如果你要 debug 某一个 acpi method, 那么可以使用 !amli bp method_path, such as !amli bp _SB.PCI0.PE01._ADR, 那么 OS 在 run 这个 method 的时候会 break 下来, 然后你可以使用 p, 进行单步, 看看执行情况。

在 BIOS 的 ASL code 中, 可以使用以下方法使你想要的东西输出到 WinDBG:

1. 输出一个 value, 如 Store(Local0, Debug)

2. 输出一个字串, 如 Store("Start trace ASL with windbg", Debug)

在 Linux 系统中, 其实也可以使用上面的语法将 ASL 的 debug value 输出来, 不过一般发行版的 Linux, 其 ACPI 驱动都不支持 debug mode, 可以使用得到的发行版的 Linux kernel, 在

compile kernel 的时候选择 ACPI Debug 这项，这样就可以让 ASL 的 debug 信息输出出来。

上面我只是简略的介绍一下，你可以 google 一下，网上有几篇介绍这个的文章。。。

使用 USB 2.0 debug cable debug ACPI 的方法：

Note:

只支持 Vista 和 Win7

可用的 usb 2.0 debug cable:

1. Insyde H2O DDT cable
2. Phoenix PCA cable
3. AMI (OK, I don't know the name)
4. Marketing store, available in US or TW, made by Ajays Technology(Original tech may from PLX), you can buy one as about \$80

前期准备：准备 checked build 版本的 acpi.sys，方法有两种

1. 替换 OS 下的 acpi.sys 为 checked build 版本。在 Vista or win7 中，可以通过以下步骤：在 acpi.sys 文件中右键属性->安全->高级->Owner ->Edit or 编辑，将原本的 Owner Administrators 修改为你的用户，这样就可以替换 sys 文件了。

在 Windows 目录下，可能有多个 acpi.sys 存在，除了 driver 下，可能的地方还有 drivercache, filerepo，最好将所有的文件全部替换掉。。

2. 安装 checked build 版本的 OS（一般没有免费下载，如果有 MSDN 订阅的话，可以通过 MSDN 下载到）

如果使用 H2O DDT or PCA，需要更改 H2O DDT 的驱动为 WinDBG 的 USB 驱动。

设置：

1. OS 端：

运行 msconfig，在“启动”项下，选择“高级选项”，打开后，勾选“调试”选项，在调试设置中，选择“调试端口”为 USB，在 USB 目标名中填入一个名称，不超过 20 个 ASCII 字符。例如“t”

2. Debug 端：

在 WinDbg 中选择 File menu 下的 Kernel debug，在弹出的框中选择 Usb 2.0, Target Name 填入刚才在 OS 下写的 name“t”

重启 Target OS，WinDbg 会自动连接

问题：

在 ICH9 等以后的南桥上，由于 chipset 本身有两个 EHCI，即有两个 EHCI debug port，这样 OS 段有可能会和 WinDbg 连接不上，这个时候最好 disable 不用的那个 EHCI

二、使用 WinDBG 诊断 DTM 测试 Fail 的原因

在 WLK 测试中 Fail，通常是非常棘手的问题，此时可以利用 BSOD 产生的 .dmp 文件分析 Fail 的原因。系统 BSOD 时产生的 dmp 文件有 3 种，分别为

Small memory dump, 通常是 64KB 大小的 memory dump, 所包含的信息最少
kernel memory dump, 包含 Windows Kernel 运行的 memory 信息
Full Memory dump, 当前系统整个 memory 的 dump

关于如何配置这 3 种 memory dump, 请参考[14].在测试时, 注意给系统盘保留足够大的空间, 以便存放 memory dump 文件, 特别是 Full memory dump 时。

在得到 dmp 文件后, 可以使用 Windbg -》打开 memory dump 文件来打开, 并且可以执行!analyze -v 命令来分析 memory dump 中的信息。

三、使用 WinDBG 诊断 Windows hang

Windows 有一种机制, 可以使用 PS2 keyboard 或者 USB keyboard 的组合键人为的产生一个 memory dump, 所以当遇到原因不明的 system hang 时, 可以将 OS 配置成这种方式, 然后生成一个 memory dump, 分析得到的 memory dump。

详细的配置方法可以参考[13], [15]

Q/A:

在 Vista 中, 应该在具有管理员权限的控制台窗口执行如下命令后再替换 ACPI.sys:
takeown /f acpi.sys
cacls acpi.sys /G <username>:F

External Links:

[1] Tracking ACPI/ASL Using WinDbg:
<http://blog.csdn.net/hgf1011/archive/2009/02/12/3881848.aspx>

[2] 如何使用 WinDBG 跟踪调试 ASL/ACPI?
<http://blog.csdn.net/EFIBIOS/archive/2007/03/12/1526763.aspx>

[3] 如何跟踪 ACPI 代码
http://advdbg.com/blogs/advdbg_system/articles/14.aspx

[4] 如何在 Free 版的 Windows 上安装 Checked 版的 ACPI.sys
<http://blog.csdn.net/EFIBIOS/archive/2007/03/12/1526779.aspx>

[5] Download Windows Symbol Packages
<http://www.microsoft.com/whdc/DevTools/Debugging/symbolpkg.mspx>

[6] Debugging tools for Windows (WinDbg 的在线文档, 你安装了 WinDBG 以后同样会有这个离线版本的文档)
<http://msdn.microsoft.com/en-us/library/cc267445.aspx>

[7] Download WinDBG
<http://www.microsoft.com/whdc/devtools/debugging/default.mspx>

[8] Windows XP Service Pack 3, Checked Build
<http://www.microsoft.com/downloads/details.aspx?FamilyID=D811F258-C95F-479A-BDF1-0D1154D700A5&displaylang=en>

[9] Windows XP Service Pack 2 Checked Build Network Installation Package
<http://www.microsoft.com/downloads/details.aspx?familyid=7a4d8d12-9f5d-42bb-b31c-7b31657c869c&displaylang=en>

[10] Microsoft Windows Server 2003 Service Pack 1 Checked Build (32 bit)
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=f07a5e49-4a13-42cb-898b-278a8b287e16>

[11] Windows Server 2003 Service Pack 2 (32-bit x86), Checked Build
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=096c54b5-7584-4a85-97e6-251a7606809e>

[12] Windows Server 2003 Service Pack 2, x64 Editions, Checked Build
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=bd2576bb-2007-45c6-bff0-5f0b4509b5a4>

[13] Windows feature lets you generate a memory dump file by using the keyboard
<http://support.microsoft.com/kb/244139>

[14] Overview of memory dump file options for Windows Vista, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000
<http://support.microsoft.com/kb/254649>

[15] How to generate a kernel or a complete memory dump file in Windows Server 2008
<http://support.microsoft.com/kb/969028/>

[16] A hotfix is available to enable CrashOnCtrlScroll support for a USB keyboard on a computer that is running Windows Vista SP1 or Windows Server 2008
<http://support.microsoft.com/kb/971284/>