Windows 调试工具入门—1

NetRoc

http://www.DbgTech.net

一、 引子

Debugging Tools for Windows 是微软发布的一套用于软件调试的工具包(后面如果没有指明，那么我会使用 WinDbg 来作为这一套调试工具的简称)。我第一次接触是在三年前的一个内核驱动项目，由于进行了 IDT 中键盘鼠标中断的 Hook，使用 Softice 调试时造成会造成影响，只得使用 WinDbg 通过串口进行双机调试。自此之后这个 Windows 平台下最为强大的调试工具一直是开发过程中的必备。这里我毫不掩饰的说“最强”，可能很多通过逆向工作而接触调试的朋友不会认同，但是我相信随着对 WinDbg 了解的加深，以及对这套工具在软件开发中应用的了解，他们也会和我有一样的观点。

一直以来，软件调试技术在软件开发者中都没有得到足够的普及和重视，互联网上能找到的系统描述的资料也较少。随着国内软件行业整体的发展和进步，这些技术慢慢开始得到推广。2008 年出版的有关调试的数据比以往都要多。我有幸拜读了 Raymond 的《软件调试》，以及熊力的《Windows 用户态程序高效排错》，获益良多。 这几年的工作中也积累了一些关于 Windows 调试工具的知识，希望能够将这些东西进行一些分享。因此，利用几个月空闲时间翻译了 WinDbg 文档中上半部调试器配置、使用和命令介绍的内容，同时准备写一些关于 WinDbg 调试工具的初级文章。希望能够为对调试技术感兴趣而又苦于没有资料的朋友提供一些帮助。

特别感谢我的前同事小喂。虽然他第一条串口线还是我焊的，但是他对于 WinDbg 的使用和了解程度很快就超过了我。在相当长时间的共事和讨论中，让我学到了很多。

二、 Windows 调试工具的简介和组成

WinDbg 是专门为 Windows NT 系列操作系统设计的调试器，最早是作为 Windows NT 3.1 的工具发布的。其后也一直跟随 NT 操作系统的发展而不断发展完善。如果用一句话来概括，可以说 WinDbg 是为了软件开发而存在的调试工具。软件包中的调试器和小工具的各种功能都是为了配合软件的开发而设计的，并且覆盖到了 Windows 平台下各种不同类型项目的调试(传统的 SDK 或 MFC 应用程序、.NET 平台应用、COM 应用、软硬件驱动程序等等)。

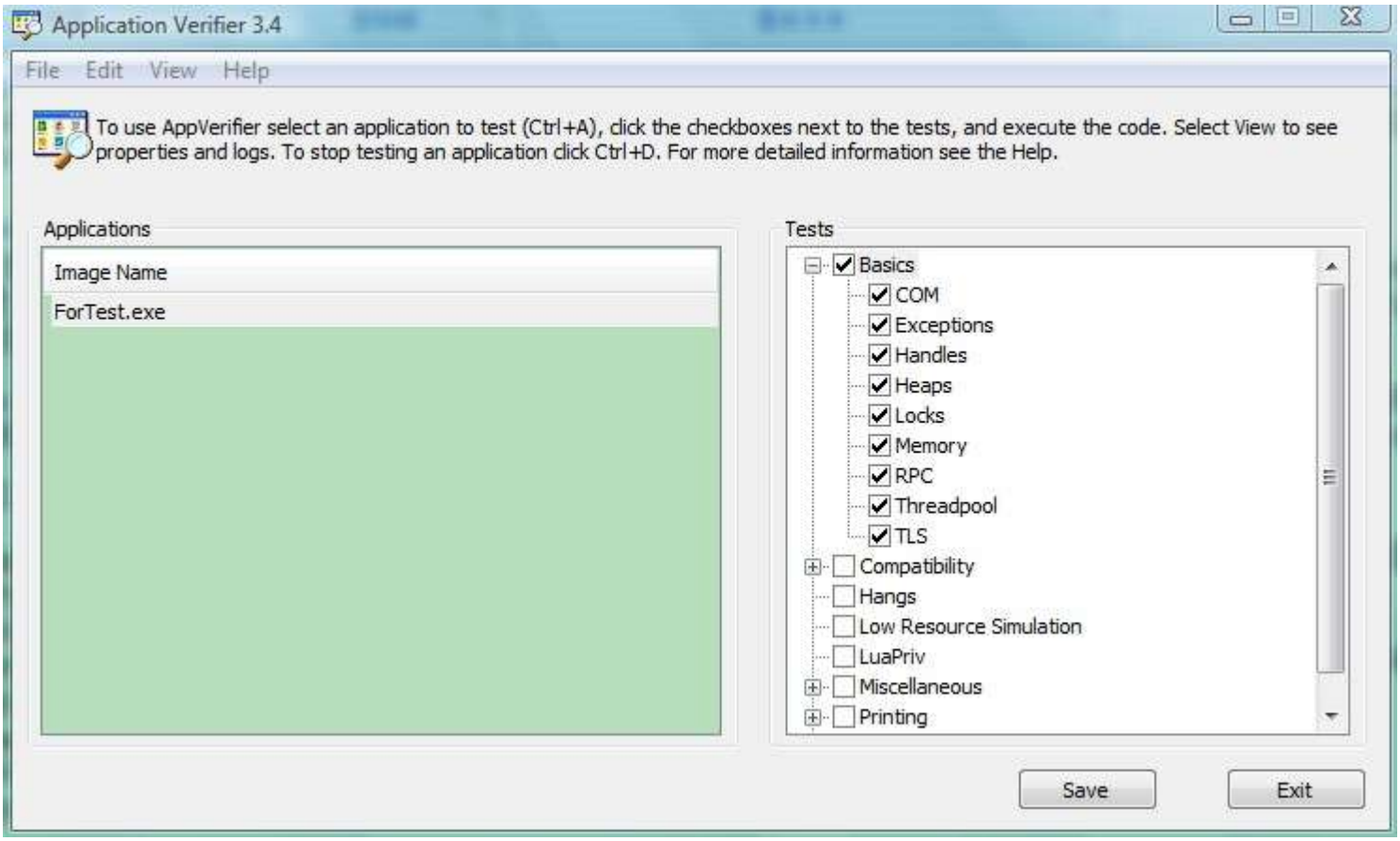
Windows 调试工具包中的调试器包括 WinDbg、KD、CDB 和 NTSD。其中， KD 用于内核调试；CDB 和 NTSD 用于用户态调试，在功能和使用上几乎完全一致；WinDbg 是内核调试器和用户态调试器的综合体，由于功能完善并且具有图形界面，所以是最常用的工具。它们能够在 x86、Itanium 和 x64 机器上的所有 NT 平台操作系统中运行。

另外，工具包中还有一些小工具，下面是常用的几个：

- KDbgCtrl：用于控制和配置内核调试的一些参数。例如是否只有当发生异常时才会启用内核调试、设置 DbgPrint 缓冲区大小、如何处理用户模式异常等等。
- ADPlus：这是一个 VB 脚本，可以为一个或多个进程自动创建内存 dump。
- SymStore：用于创建符号存储。当需要创建自己的符号存储时就要用到它了。
- SymProxy：用于在网络中创建单独的 HTTP 符号服务器，以供所有调试器使用。该工具特别适合企业级应用的环境，可以将多个符号存储通过单一的接入点提供使用。
- DbgSrv、KdSrv、Remote.exe：用于远程调试。

- GFlags：用于编辑 Global Flags。
- UMDH：用于对用户模式堆分配的情况进行转储和分析。
- USBView：这是 WinDbg 6.10.3 版本才加入到软件包中的工具，可以查看当前连接到系统中的 USB 设备信息。

另外，Application Verifier 虽然没有包含在软件包中，但是也是一个非常强大的工具。可以对程序运行时的很多状态进行监控，以发现一些普通调试难以找到的错误。下面是 Application Verifier 配置界面的一个截图：



Application Verifier 可以在这个页面下载：http://go.microsoft.com/fwlink/?linkid=108353

三、 Windows 调试器和其他熟知的调试器比较

可能很多已经习惯使用 SoftICE、OllyDbg、IDE 调试器的朋友会提出这样的疑问：在这么多调试器中，为什么要选择 WinDbg？它究竟有什么特点？

设想一下下面几个场景：

- 公司的软件针对企业级用户，该客户在地球另一半的美国。有一天客户抱怨了一个 BUG，但是从抓取的 dump 又没办法看出个所以然，想进行动态调试查找原因。公司预算有限，不能让你过去出差顺便旅游、对方公司有防火墙，不允许外部连接，等等等等。。。怎么办？
- 项目规模很大，涉及到的模块多，版本也多，并且是由不同部门开发的。这些部门可能遍布五湖四海。如何在调试其中某个模块时，能够快速获得它的符号和源文件，而不用每次都从一大堆不同版

本的文件中辛苦找寻？调试到某个阶段，突然发现这不是自己的模块出现问题，如何快速知道这个问题应该找谁解决？项目某些重要模块有保密需要，如何控制调试人员访问符号和源文件的权限？

- 驱动程序怎么才能源码调试？SoftICE 不支持新系统，我要在 Vista 上调试怎么办？
- 软件中包含一个 Windows 服务组件，但是每次还没有登陆到桌面之前就崩溃了，怎么进行动态调试？
- 我想调试 Explorer，调试 IE，调试 CSRSS，调试……，但是调试器一附加上去，系统就会出问题。怎么办？
- 公司发布的软件，有用户反馈和 XXX 安全软件冲突老是造成系统崩溃，但是搭建环境之后却又没有办法重现；对方是个普通用户，鼠标都抓得不太稳。用户很火大，闹着要抓个老虎到公司来找你上司做俯卧撑，后果很严重，怎么办？

在现实环境中，有很多复杂的调试场景，我们需要专业级的调试器来解决这些问题。而 WinDbg 恰恰提供了这种商业软件环境下的专业级软件调试功能，它和其他很多我们熟知的调试器的区别也在于此。

我们将 WinDbg 和其他调试器分作内核调试器和用户态调试器两类来进行比较。

内核调试方面：

	WinDbg	**SoftICE**
原理	Windows 操作系统内置调试支持	Hook 中断，接管系统
系统和平台支持	x86、Itanium 和 x64 机器上的所有 NT 平台操作系统	x86，由于已停止更新，新版本操作系统中支持不佳，老系统中也常常遇到兼容性问题
符号和源码支持	完美支持符号调试和源码调试，可直接使用微软公共符号	支持符号调试和源码调试，但是需要先转换符号格式
远程调试	通过和远程工具、转发器的配合，实现各种灵活的远程调试方式，以支持不同的网络环境	通过 Virtual SoftICE 支持基于网络的远程调试
硬件需求	通过串口、1394、USB 2.0 接口的双机调试；通过 Pipe 连接的虚拟机调试；或者功能有诸多限制的本地内核调试	单机或者通过 Virtual SoftICE 的双机调试
用户界面	由于是双机调试，调试器只是主控机上运行的一个普通软件。拥有 GUI 界面，可以同时进行其他应用。	单机调试时完全接管系统，字符界面，操作不是很方便。
扩展性	支持脚本和插件，并且软件包本身提供了大量非常有用的插件	支持插件

由于 SoftICE 已经停止更新，WinDbg 可以说是现在 Windows 平台上唯一好用的进行内核调试的工具，并且随着新版本的不断推出，不断地添加对新版操作系统的支持以及完善功能。强大的符号支持，方便的源码调试，使得内核级调试能够事半功倍。

用户态调试方面：

	Windows 调试工具包	OllyDbg	Visual Studio 调试器
原理	Windows 的用户程序调试支持	Windows 的用户程序调试支持	Windows 的用户程序调试支持
系统和平台支持	主要基于 NT 系统，9x 内核下支持不佳并且需要安装附加模块	主要支持 NT 系统，9x 下也可以使用	新版本的 VisualStudio 不支持在 9x 系统下安装。VC6 之前可以在 9x 下调试
符号和源码支持	完美支持符号调试和源码调试，可直接使用微软公共符号	支持符号调试和源码调试	支持。VS2008 开始可以直接使用微软公共符号
远程调试	通过和远程工具、转发器的配合，实现各种灵活的远程调试方式，以支持不同的网络环境	不支持	较新版本 Visual Studio 中支持
无源码调试	反汇编分析能力较弱，GUI 界面偏弱，无源码时调试比较困难	强大的代码分析能力，无符号和源码时也能很好的进行调试	无源码调试的支持很弱，使用不便
用户界面	GUI 界面不是很丰富，大量操作需要通过命令	GUI 界面强大，能够实现大多数调试操作	介于 WinDbg 和 OllyDbg 之间。
扩展性	支持脚本和插件，并且软件包本身提供了大量非常有用的插件	支持脚本和插件，有大量可用的资源	支持插件扩展
Dump 文件调试	支持，分析功能强大	不支持	支持，但是不够强大
.NET 调试	通过 SOS.dll 支持，进行高级调试比较方便	不能直接支持	功能强大易用，绝大多数情况下都能解决问题

由于 WinDbg 功能相当复杂，有很多方面并不能一一比较，例如非侵入式调试、通过 WinDbg 控制 CDB 和 NTSD 来调试系统服务、创建和分析 Dump 文件等等。

总体来说，WinDbg 更适合作为软件项目开发和维护过程中的调试工具使用，而 OllyDbg 更适合逆向工程。

四、 何时使用 Windows 调试工具

根据我个人对 WinDbg 的使用经验来说，它更适合作为开发维护的辅助工具来使用。

如果要进行用户态的逆向工程，推荐使用 OllyDbg、IDA 这些拥有强大汇编程序分析能力的工具。

WinDbg 更适用于以下这些场合：

- 商业软件的 Debug 和客户支持
- 内核驱动的调试，以及对驱动进行逆向工程时进行动态调试

- 研究 Windows 本身的内核或者软件
- 疑难 BUG 的调试，如死锁、COM 调用、资源泄露、堆栈或者堆溢出
- 以性能优化为目的的调试
- 对调试目标基本不造成影响的非侵入式调试