Windows 内核与高级调试（2014 新版）

直到今天，Windows 仍然是软件历史上最复杂的操作系统，深入理解这个操作系统对于任何软件工程师来说都是一个巨大的挑战。本培训借助调试器这把利剑，深入 Windows 系统内部，以生动鲜活的方式，解读 IRQL、IRP、设备栈等诸多难以理解的概念，领略 NT 内核的博大精深，感悟软件的真谛。

时间长度：3 天
形式：讲解 + 动手实验 + 真实案例演示

第一部分：Windows NT 核心特征 (2 hours)
地址空间，虚拟内存原理，Page Fault，系统调用，内核态的关键组件，用户态的关键组件，环境子系统，会话

第二部分：WinDBG 精要（1 小时）
WinDBG 的命令类型，常用命令，命令语法，调试符号，符号文件的种类，符号服务器，定制调试事件的方法和重要的调试命令，软件断点、硬件断点，复杂的断点命令

第三部分：内核调试引擎（1 小时）
两种软件哲学，内核调试引擎（结构，重要的函数全局变量，工作原理），五种连接方式，启用方法，PCR，双机用户态调试（Debug WinLogon and CSRSS）

试验一：内核调试环境建立和调试系统崩溃（BSOD）（0.5）

第四部分：调试启动过程 (1.5 hours)
现场跟踪 Windows 系统的启动过程，解析其中的重要步骤和关键细节：内核初始化，CPU 初始化，执行体的阶段 0 和阶段 1 初始化，SMSS（Windows 会话管理），CSRSS 和 WinLogon，UserInit 以及 Shell，用户登录过程

第五部分：内存管理器 (1.5 hour)
内存管理的多级架构，内存管理器，大内存页及其使用，6 大工作线程，内核池，分页内核和非分页内核池，PFN 数据库，虚拟地址空间的管理（VAD）

第六部分：I/O 子系统和内核态驱动 (1.5 hours)
I/O 子系统架构，I/O 管理器，驱动程序类型，设备树，ACPI，理解 ACPI 脚本，PnP，I/O 子系统的建立过程，设备栈，PDO，FDO，IRP，IRQL，驱动程序验证器

试验二：分析双误异常导致的系统崩溃转储文件（0.5 小时）

第七部分：存储和文件系统 (2 hours)
磁盘和文件系统架构，磁盘驱动，端口驱动，卷，分区，文件系统，文件系统的过滤驱动，Mini Filter，实际**案例分析：因为文件过滤驱动而导致的系统死锁**

第九部分：网络（1.5 hours）
背景，NT 的网络架构，WinSock API，LSP (Layered Service Provider)，AFD，Kernel Socket，TCP/IP，NDIS，Windows Filter Platform (WFP)

第十部分：系统崩溃和转储 (1.5 hour)
系统崩溃概览，Windows 蓝屏崩溃（BSOD）的过程，Linux 的 Panic 过程（包括产生 call stack 和寻找函数符号的方法），系统转储

第十一部分：转储分析（1.5 小时）
分析系统转储的方法，自动分析，自动分析的局限，真实**案例解析：双误导致的崩溃，挂死在 DPC**，回退到错误现场的方法，从栈上寻找线索

第十二部分：系统死锁和系统调优（2 小时）
系统挂死，典型原因，解决方法，窗口子系统挂死，资源锁，!locks，IRQL，挂死在高 IRQL，中断风暴；WPT 概览，调优基础，采样和 Instrumentation，WPR 和 WPA，实例讨论：高 CPU 占用率，GPU 调优