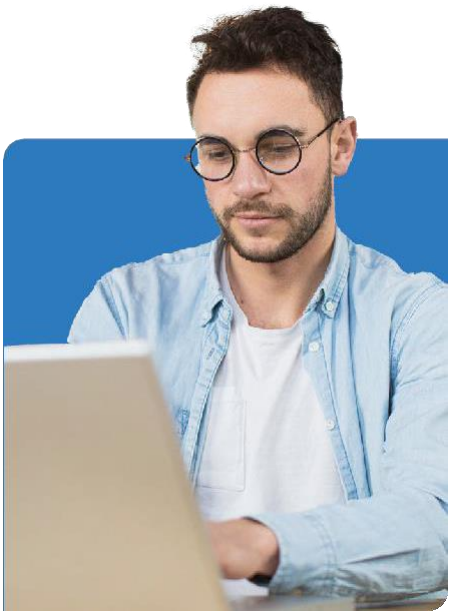
ThriveDX™

Windows Internals

TDXAISD-105



ThriveDX Windows Internals

Time Commitment
4 days (total of 32 hours / 8 hours per day)

Skill Level
Professional Level

Course Category
AI | Software Development

The Windows OS exposes many advanced services to system programmers through the Windows API, and to device driver writers through the Kernel API. The .NET framework wraps these services and runs on top of the Windows API and the Kernel.
Good knowledge of what's going on under the hood of the OS, which services are available and how to best utilize them helps in building better and more efficient software for Windows. This course discusses the internal workings of Windows and its exposed services, so they can be leveraged better by developers, while gaining crucial insight for troubleshooting and debugging as well.

Prerequisites

- Basic knowledge of OS concepts and architecture.
- C reading knowledge is beneficial

Objectives

Understand the underlying mechanism and advanced services of the windows OS and use that knowledge to understand system mechanics, process and thread operations and analyze issues.

Target Audience

Power users that want to understand how the Windows system works, its various mechanisms, and have ways to analyze various scenarios when these occur.

Program Structure

System Architecture -Module 01

- Brief Windows NT History
- Basic Concepts
- Windows Versions
- Tools: Windows, SysInternals, Debugging, Tools for Windows
- Processes and Threads
- Virtual Memory
- User mode vs. Kernel mode
- Objects and Handles
- Architecture Overview
- Key Components
- User/kernel transitions
- Introduction to WinDbg
- Lab: Task manager, Process Explorer, WinDbg

TDX

Processes & Jobs Module 02

- Process Internals & Data Structures
- Creating and terminating processes
- The loader
- Process attributes
- Protected processes and PPL
- UWP Processes
- Minimal and Pico processes
- Jobs
- Nested jobs
- Labs: viewing process and job information

Threads Module 03

- Thread basics
- Creating threads
- Processor Groups
- Thread Priorities
- Thread Scheduling
- Threads and Performance
- Performance Counters
- Thread Stacks
- Thread States
- Thread Synchronization
- Lab: viewing thread information; Performance ,Monitor; Windows Performance Recorder/Analyzer

Memory Management Module 04

- Overview
- Small, large and huge pages
- VMM Services
- Page states
- Address Space Layou
- Address Translation Mechanisms
- Heaps
- Page Faults
- Page Files
- Workings Sets

- Memory Mapped Files
- Page Frame Database
- Other memory management features
- Lab: viewing memory related information

Kernel Mechanisms Module 05

- Trap Dispatching
- Interrupts & Exceptions
- System Crash
- Basic crash dump analysis
- Object Management
- Objects and Handles
- Sharing Objects
- Synchronization
- Synchronization Primitives
- Signaled vs. Non-Signaled
- Windows Global Flags
- Kernel Event Tracing
- Wow64
- Lab: Viewing Handles, Interrupts; Analyzing a crash dump

Management Mechanisms Module 06

- The Registry
- Services
- Starting and controlling services
- Windows Management Instrumentation
- Lab: Viewing and configuring services; Process Monitor

I/O System Module 07

- I/O System overview
- I/O Function
- Device Drivers
- I/O Processing and Data Flow
- IRPs
- Plug & Play
- Power Management
- File systems and mini-filters

- Driver Verifier
- Labs: viewing driver and device information; kernel debugging

Security (if time permits) Module 08

- Security components
- Protecting objects
- SIDs
- Token
- ACLs
- Access checking
- Privileges
- AppContainers
- Logon
- User Access Control (UAC)
- Process mitigations
- Lab: viewing security information