



Sign in

Research ▾

Detours

Established: January 16, 2002

Detours is a software package for re-routing Win32 APIs underneath applications. Under commercial release for over 10 years, Detours is licensed by over 100 ISVs and used within nearly every product team at Microsoft.

[What's New](#)

What's New?

Detours Professional 3.0 is available for immediate purchase at the online [Microsoft Store](#). Detours Professional includes a commercial use license that allows the use of Detours in commercial products and in production environments. Detours Professional includes support for either 32-bit or 64-bit processes on x86 and other Windows-compatible processors.

Detours Express 3.0 is available for immediate download under a no-fee, click-through license for research, non-commercial, and non-production use. Detours Express is limited to 32-bit processes on x86 processors.

The APIs in Detours Professional 3.0 and Detours Express 3.0 are identical. The two versions differ in their licensing and processors supported. Detours Professional is required for all commercial or production deployments. Detours

Professional supports x86, x64, IA64, and ARM processors. Detours Express supports only x86; it may be used to prototype (but not deploy) commercial projects.

Detours 3.0 includes the following new features over Detours 2.x:

- Support for 64-bit code on x64 and IA64 processors (Professional Edition only).
- Support for all Windows processors (Professional Edition only).
- Removed requirement for including detoured.dll in processes.
- Compatibility improvements for detouring APIs used by managed-code (MSIL) programs, especially on x64 processors.
- Addition of APIs to enumerate PE binary Imports and to determine the module referenced by a function pointer.

Overview

Overview

Innovative systems research hinges on the ability to easily instrument and extend existing operating system and application functionality. With access to appropriate source code, it is often trivial to insert new instrumentation or extensions by rebuilding the OS or application. However, in today's world systems researchers seldom have access to all relevant source code.

Detours is a library for instrumenting arbitrary Win32 functions Windows-compatible processors. Detours intercepts Win32 functions by re-writing the in-memory code for target functions. The Detours package also contains utilities to attach arbitrary DLLs and data segments (called payloads) to any Win32 binary.

Detours preserves the un-instrumented target function (callable through a trampoline) as a subroutine for use by the instrumentation. Our trampoline design enables a large class of innovative extensions to existing binary software.

We have used Detours to create an automatic distributed partitioning system, to instrument and analyze the DCOM protocol stack, and to create a thunking layer for a COM-based OS API. Detours is used widely within Microsoft and within the industry.

Publications

Detours: Binary Interception of Win32 Functions

[Galen Hunt](#), Doug Brubacher

July 1999

USENIX

Follow Microsoft Research

Like

Follow

YouTube

Share this page

Share

Tweet

Share

Learn

Windows

Office

Skype

Outlook

OneDrive

MSN

Devices

Microsoft Surface

Xbox

PC and laptops

Microsoft Lumia

Microsoft Band

Microsoft HoloLens

Microsoft Store

View account

Order tracking

Retail store locations

Returns

Sales & support

Downloads

Download Center

Windows downloads

Windows 10 Apps

Office Apps

Microsoft Lumia Apps

Internet Explorer

Values

Diversity and inclusion

Accessibility

Environment

Microsoft Philanthropies

Corporate Social Responsibility

Privacy at Microsoft

Company

Careers

About Microsoft

Company news

Investors

Research

Site map

English (United States)

[Contact us](#)

[Privacy & cookies](#)

[Terms of use](#)

[Trademarks](#)

[About our ads](#)

© 2016 Microsoft