# Software for cracking software. Selecting tools for reverse engineering

Written by Nik Zerof



Every reverse engineer, malware analyst or simply a researcher eventually collects a set of utility software that they use on a daily basis to analyze, unpack, and crack other software. This article will cover mine. It will be useful to anyone who has not yet collected their own toolset and is just starting to look into the subject. However, an experienced reverse engineer must also be curious about what other crackers are using.

# WARNING

This article is for information purposes only. Neither the editorial team nor the author assumes any responsibility for possible harm that may arise from the use of these materials.

# Debuggers

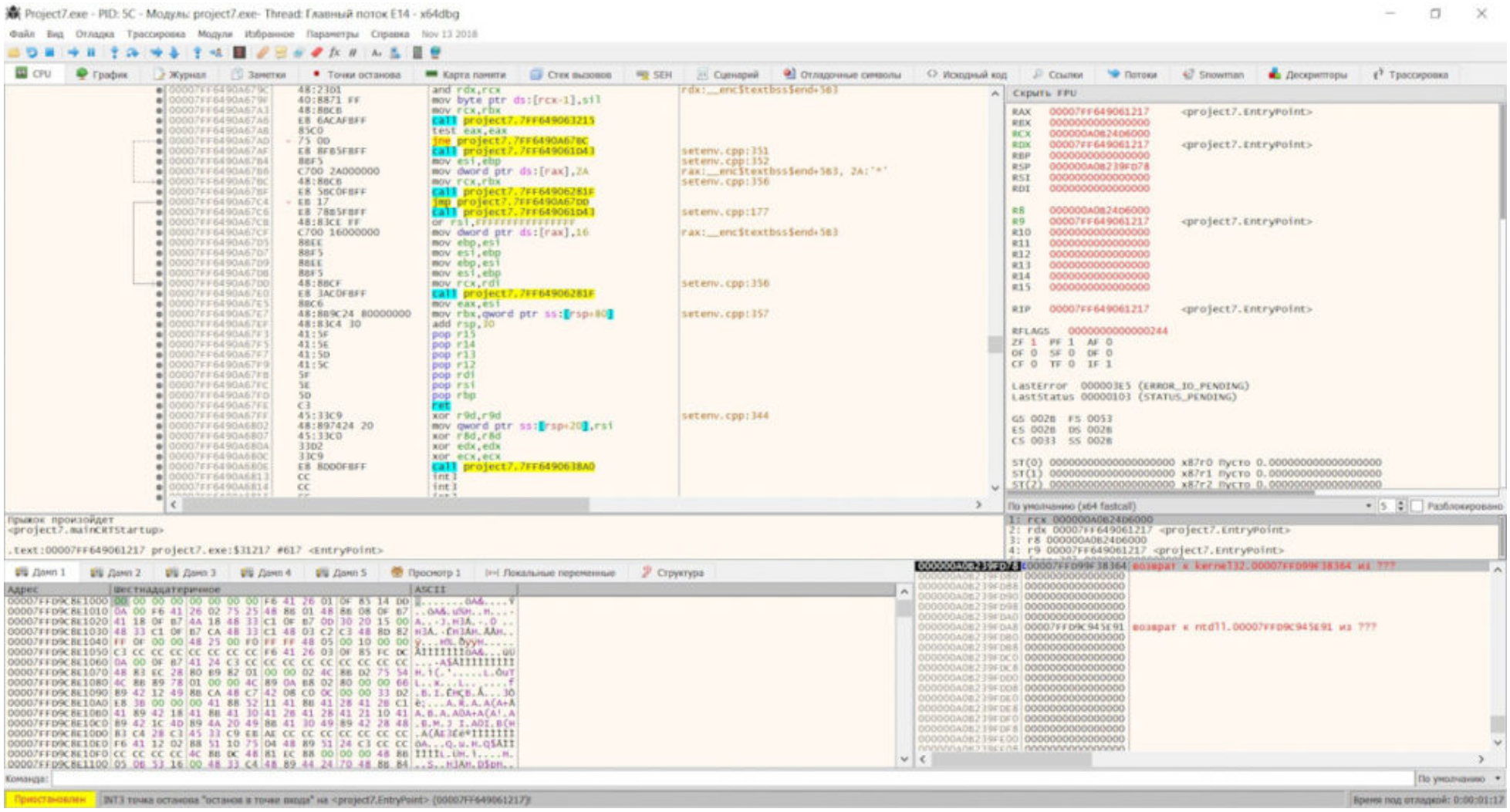
Debugging an application is an essential part of studying it, so every reverse engineer needs a debugger at the ready. A modern debugger must support both Intel architectures (x64 and x86), so this is the first prerequisite.

We must also be able to debug kernel-mode code. You will need this every once in a while, especially if you want to look for zero-day vulnerabilities in OS kernels or reverse engineer malware in drivers. The main candidates are x64dbg and WinDbg. The first debugger works in user mode, while the second one can debug kernel-mode code.

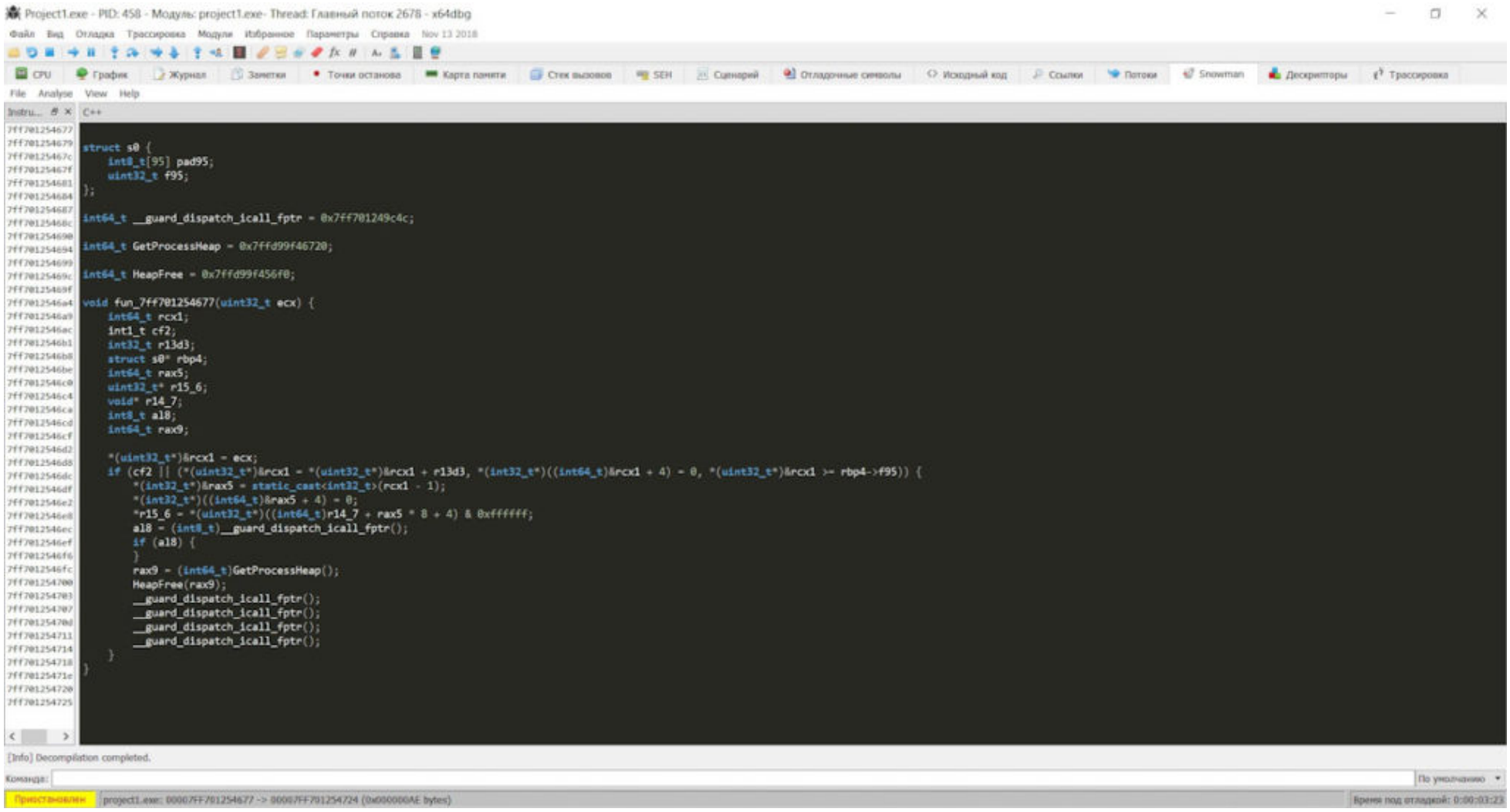
## x64dbg

*x64dbg.com*

This is a modern debugger with a good user interface, a worthy successor of OllyDbg. It supports both architectures (x64 and x86), and there are tons of useful plugins.



x64dbg




Built-in decompiler

Granted, it has its downsides as there are a number of annoying bugs. But it is actively developed and supported. Since the debugger works in user mode, it is of course vulnerable to a wide range of anti-debugging techniques. This is, however, in part offset by the availability of many different debugger hiding plugins.

x64dbg has a built-in decompiler and imports reconstructor (both x64 and x86), supports code graph visualization and read/write/execute/access breakpoints. This debugger has enabled some hackers to break down the infamous Denuvo DRM system!

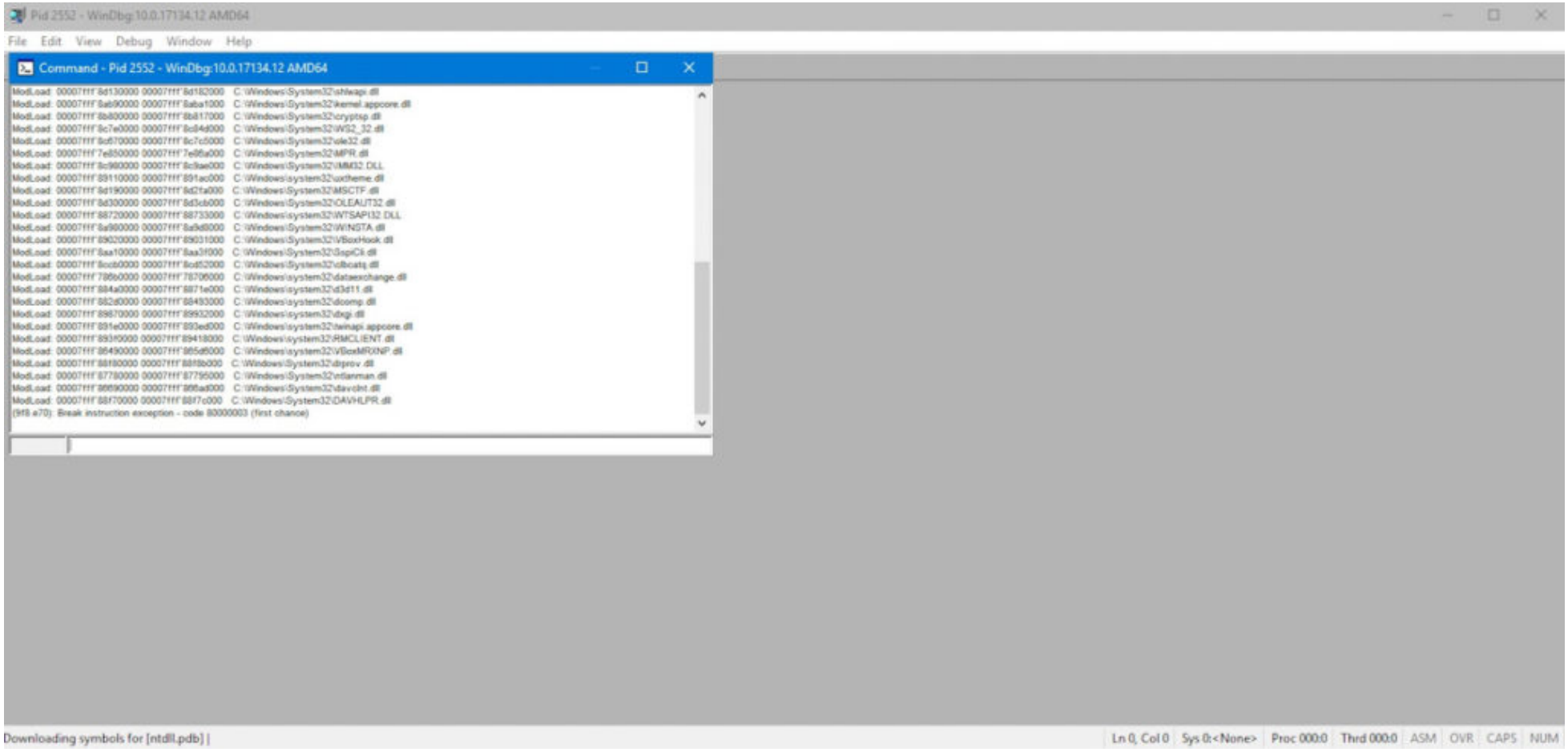
### Why not OllyDbg

We haven't included OllyDbg here because it is very outdated. It does not support the latest operating systems or x64. The app's official website announced a x64 version and even reported some development progress, but the site itself has not been updated since 2014. OllyDbg is undoubtedly a milestone piece of software, but now it seems that its time has passed. There have also been fewer kernel mode debuggers since Syser Kernel Debugger, a successor to SoftICE, was abandoned.

## WinDbg

*Official homepage*

WinDbg is one of the best kernel or driver debugging tools. This debugger is supported by Microsoft and included in the Windows Driver Kit (WDK). This is currently the most up-to-date and powerful kernel code debugger. It does not feature the user-friendly interface of x64dbg, but there are not many other options, as other debuggers don't support kernel-mode code.




WinDbg supports remote debugging and can download debug symbols directly from Microsoft servers. The VirtualKD booster exists to speed up the WinDbg setup for debugging kernel-mode code in a VM. WinDbg is definitely not for beginners, but as you gain experience in reverse engineering and start testing various interesting options, you won't be able to avoid it.

WinDbg enables you to view various system structures and easily disassemble NTAPI functions. Of course it can also be used to debug "regular" applications, but I prefer to unleash this powerful weapon only when it is really needed!

Search

Search

Recent Posts

- Software für das Cracken von Software. Auswahl von Tools für das Reverse Engineering
- Software for cracking software. Selecting tools for reverse engineering
- Attacking a car alarm. How does a car alarm security system work?
- What to See on the Darkweb: A Travel Guide to Hidden Services
- Tips&tricks: Android's hidden capabilities that everyone should know

Recent Comments

- aquageek on Automation for OS X: the JavaScript way
- Vx00001 on Dive into exceptions: caution, this may be hard
- gangaprabha on A saga about a packer which can prepare similar OS images for development and production scenes in various environments
- try harder-Legend's BLog on TOP–10 ways to boost your privileges in Windows systems
- dxon on Building weather station with STM32F3DISCOVERY and WizFi220 Wi-Fi module