**KMDF Hands-on**

Contents

[First Steps 2](#_Toc130889689)

[Fixing the build: signature, inf2cat 2](#_Toc130889690)

[Fixing DebugView 4](#_Toc130889691)

[Display kernel messages 4](#_Toc130889692)

[Install driver via devcon 5](#_Toc130889693)

[Windbg: print driver info 7](#_Toc130889694)

[Fixing Windbg 9](#_Toc130889695)

[Online symbols 9](#_Toc130889696)

[Offline Symbols 11](#_Toc130889697)

# First Steps

**1.** Read this and finish writing your driver: Write a Hello World Windows Driver (KMDF)[[1]](#footnote-1)

**2.** Setup a VM and prepare it for debugging:

* Create a snapshot just in case
* Install WDK
* Install Windbg or DebugView
* Enable test signing[[2]](#footnote-2)
  + bcdedit /set nointegritychecks on
  + bcdedit /set loadoptions DDISABLE\_INTEGRITY\_CHECKS
  + bcdedit /set testsigning on
* Reboot

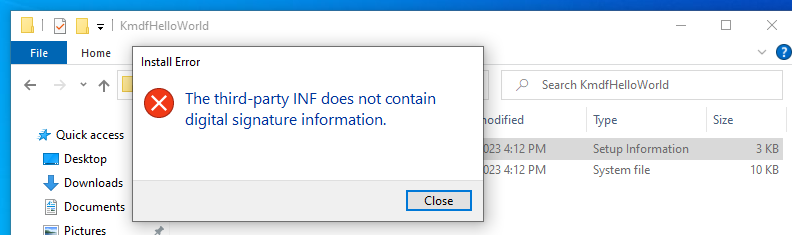
This doesn’t work on a VM: Provision a computer for driver deployment and testing (WDK 10)[[3]](#footnote-3)

Refer to the abovementioned guide only when you have a spare physical machine.

**3.** Install the driver and start debugging

# Fixing the build: signature, inf2cat

If you’ve encountered this issue, even after disabling signature varification and enabled test signing via bcdedit, then keep on reading to see my fix.



First, check if the .cat file was generated. A catalog file contains multiple signatures, each signature corresponds to a single file that’s installed by installing the driver (or copied to another directory by installing the driver). <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/inf-copyfiles-directive>

Graphical user interface, application, email

Description automatically generated

If there isn’t a .cat file, you need to ensure inf2cat is being instructed to generate the catalog file on Visual Studio. Right click on “Project” (instead of “Solution”), and then “Properties”.

Graphical user interface, text, application, email

Description automatically generated

Select “No”, which means do generate the catalog file.

If inf2cat is still not generating the catalog file, delete inf2cat.exe.manifest so that Visual Studio would sign the catalog. <https://developercommunity.visualstudio.com/t/inf2cat-an-attempt-was-made-to-load-a-program-with/785173>

Graphical user interface, text, application, email

Description automatically generated

The installation should work fine from here on. Copy the “.inf, .cat, .sys” into your target machine, right click on the “.inf” file and then “Install”.

# Fixing DebugView

## Display kernel messages

If the following popup shows up but you can’t find your device on “Computer Management”, and DebugView isn’t showing kernel messages, my fix is provided below.

Graphical user interface, application, Word

Description automatically generated

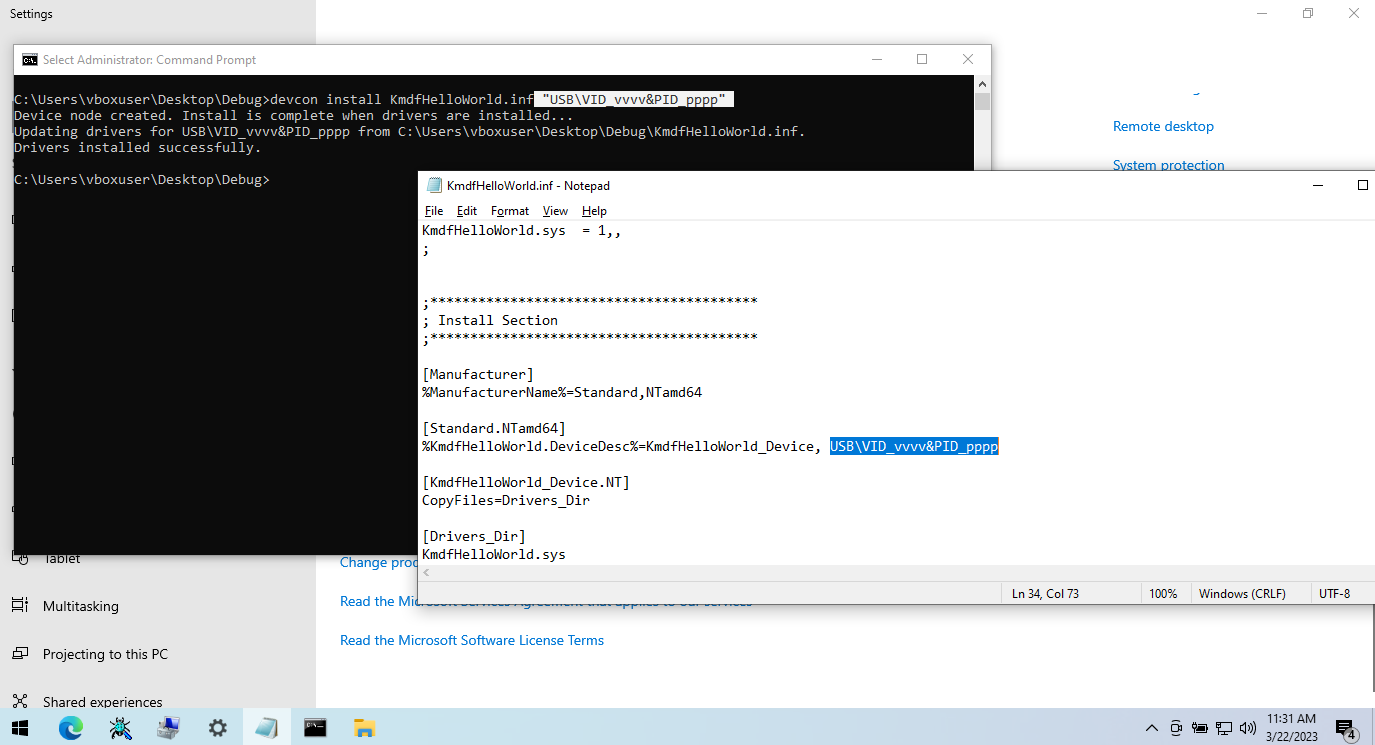
First, ensure DebugView is instructed to capture everything:

Graphical user interface, text, application

Description automatically generated

## Install driver via devcon

And install a device using devcon.exe, find out the “Hardware ID” like this:



Right after installing the driver, you should be able to see something like this in DebugView.

Graphical user interface, text, application

Description automatically generated

This is exactly what we wanted the driver to print by calling KdPrintEx.

Graphical user interface, text, application

Description automatically generated

“kmdfHelloWorld Device” can be seen down at the bottom in “Device Manager”.

Graphical user interface, text, application

Description automatically generated with medium confidence

# Windbg: print driver info

Start up Windbg, select Kernel debugging and select “Local”

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Open Command window (press Alt+1) and enter

!drvobj <driver> 2

Text

Description automatically generated

# Fixing Windbg

## Online symbols

Notice that calling “!drvobj” on Windbg command window gives you only the addresses. It could be valuable information if you can understand what these addresses are.

1 Create a folder C:\\symbols Graphical user interface, application

Description automatically generated

2 Windbg Commands:

.sympath srv\*https://msdl.microsoft.com/download/symbols\*C:\Symbols

.symfix+ c:\symbols [[4]](#footnote-4)

.reload

(or .reload /f)

Table

Description automatically generated

Run !***drvobj*** again, notice that kmdfHelloWorld is a “driver pair”, namely ***(kmdfHelloWorld, Wdf01000)***, meaning that this is a KMDF-based WDM (Windows Driver Model) driver, using WDF (Windows Driver Framework***s****,* aka. ***Wdf01000***). If you find what you’ve just read confusing, you might want to go through “Concepts for all driver developers”[[5]](#footnote-5).

Table

Description automatically generated

As a side note, examining Sonicwall GVC’s driver (you have to first enable the device in “Device Manager”), you’ll see another type of driver pair: minoports and port drivers.

Text

Description automatically generated

The driver uses NDIS as the port (general) driver, and ***SWVNIC*** is a miniport driver.

## Offline Symbols

There’s no long offline symbol packages that you can download.

Text

Description automatically generated with low confidence[[6]](#footnote-6)

You may try using symcheck to get the symbols (PDB, Program Database).

"C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\symchk.exe" /r c:\windows /s SRV\*c:\symbols\\*http://msdl.microsoft.com/download/symbols[[7]](#footnote-7)

But expect to see errors:

Text

Description automatically generated

1. <https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/writing-a-very-small-kmdf--driver> [↑](#footnote-ref-1)
2. <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/the-testsigning-boot-configuration-option> [↑](#footnote-ref-2)
3. <https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/provision-a-target-computer-wdk-8-1> [↑](#footnote-ref-3)
4. <https://stackoverflow.com/questions/30019889/how-to-set-up-symbols-in-windbg> [↑](#footnote-ref-4)
5. <https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/concepts-and-knowledge-for-all-driver-developers> [↑](#footnote-ref-5)
6. <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-symbols> [↑](#footnote-ref-6)
7. <https://stackoverflow.com/questions/50179282/how-to-load-all-windows-symbols-from-server-starting-with-w10-version-1803-bu> [↑](#footnote-ref-7)