WINDOWS DRIVER DEBUGGING

Homepage: https://sites.google.com/site/doc4code/

Email: sj6219@hotmail.com

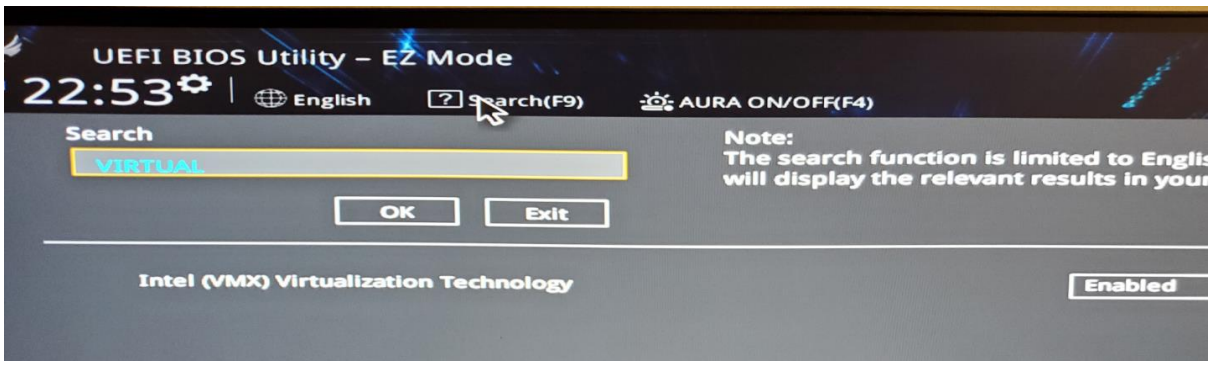
2021/4/5

Windows 10 Pro 이상에서 Hyper-V 를 사용할 수 있다.

SETTING UP VIRTUAL MACHINE KDNET

Setting Up Network Debugging of a Virtual Machine with KDNET - Windows drivers | Microsoft Docs

ENABLE HYPER-V MACHINE IN BIOS



바이오스 설정에서 virtual 관련해 검색해서 설정한다.

INSTALL HYPER-V ON WINDOWS 10

https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v

Powershell 운영자모드에서

Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All

을 실행한다.

CREATE A VIRTUAL MACHINE WITH HYPER-V

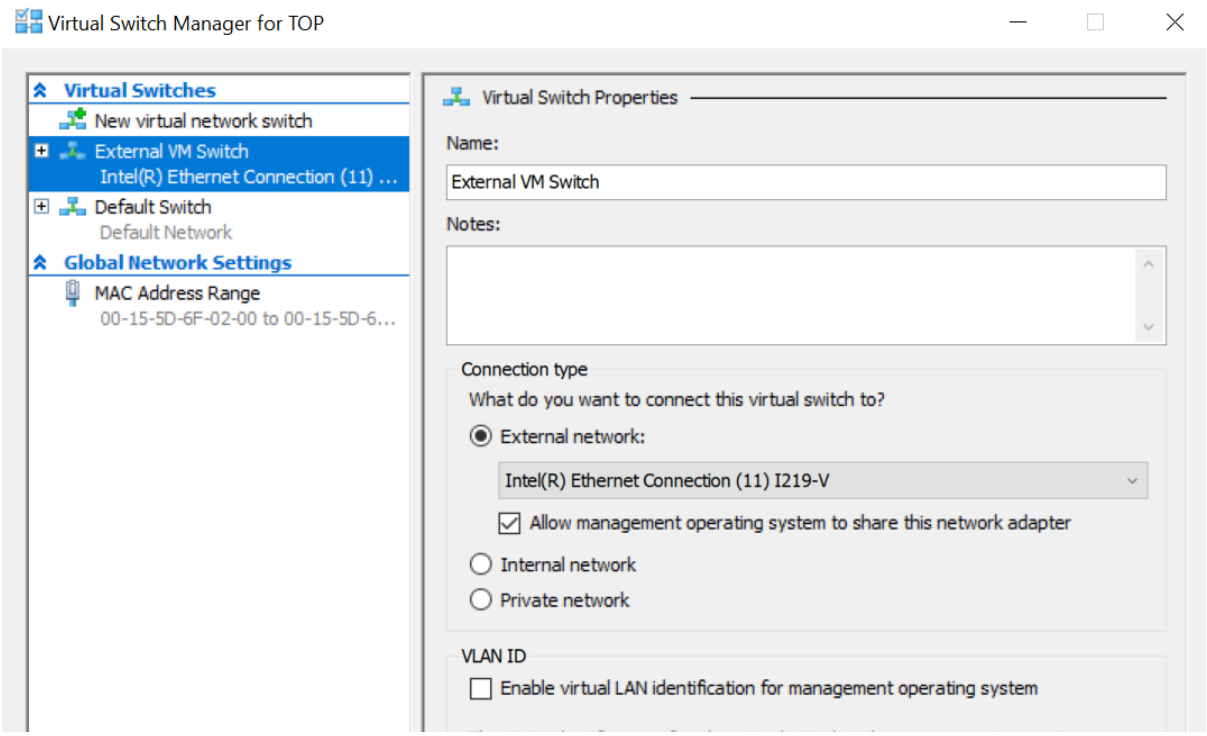
Create a Virtual Machine with Hyper-V | Microsoft Docs

Windows 10 Fall Creators Update (Windows 10 version 1709) 을 설치한다.

CREATE A VIRTUAL NETWORK

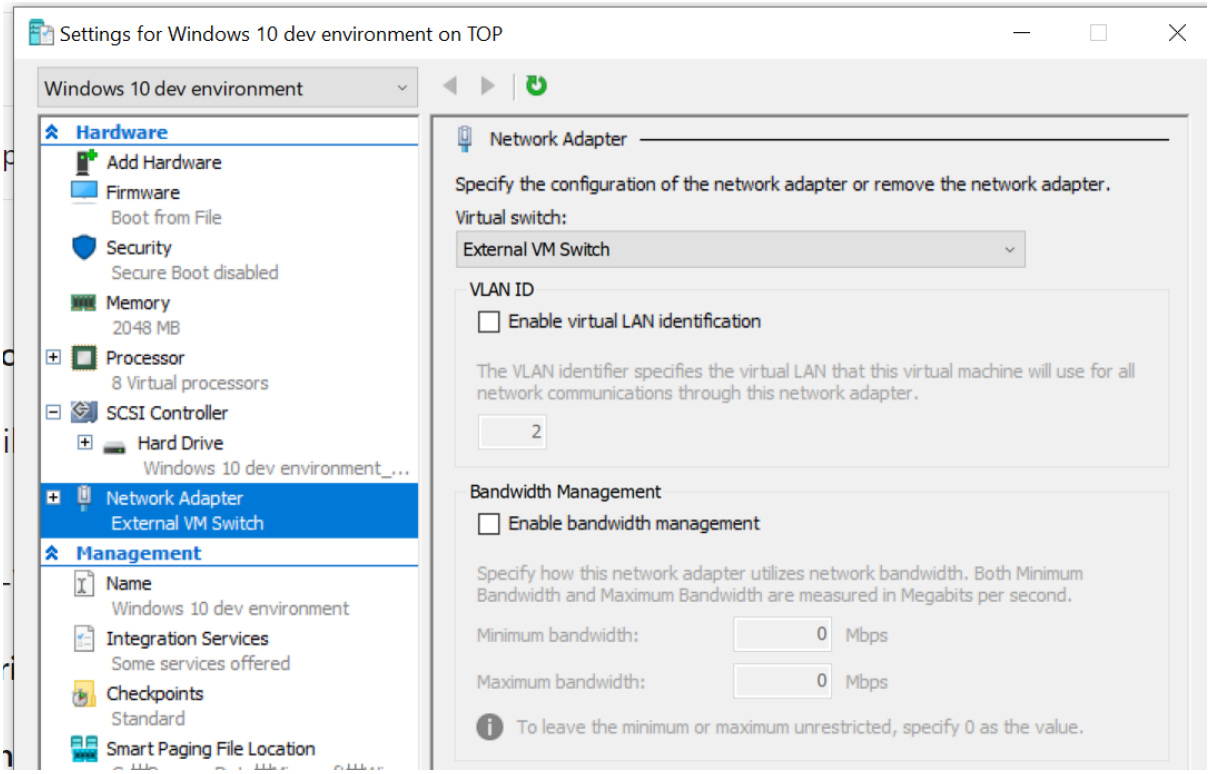
Create a Virtual Network | Microsoft Docs

호스트 기계에 가상 스위치를 만든다.

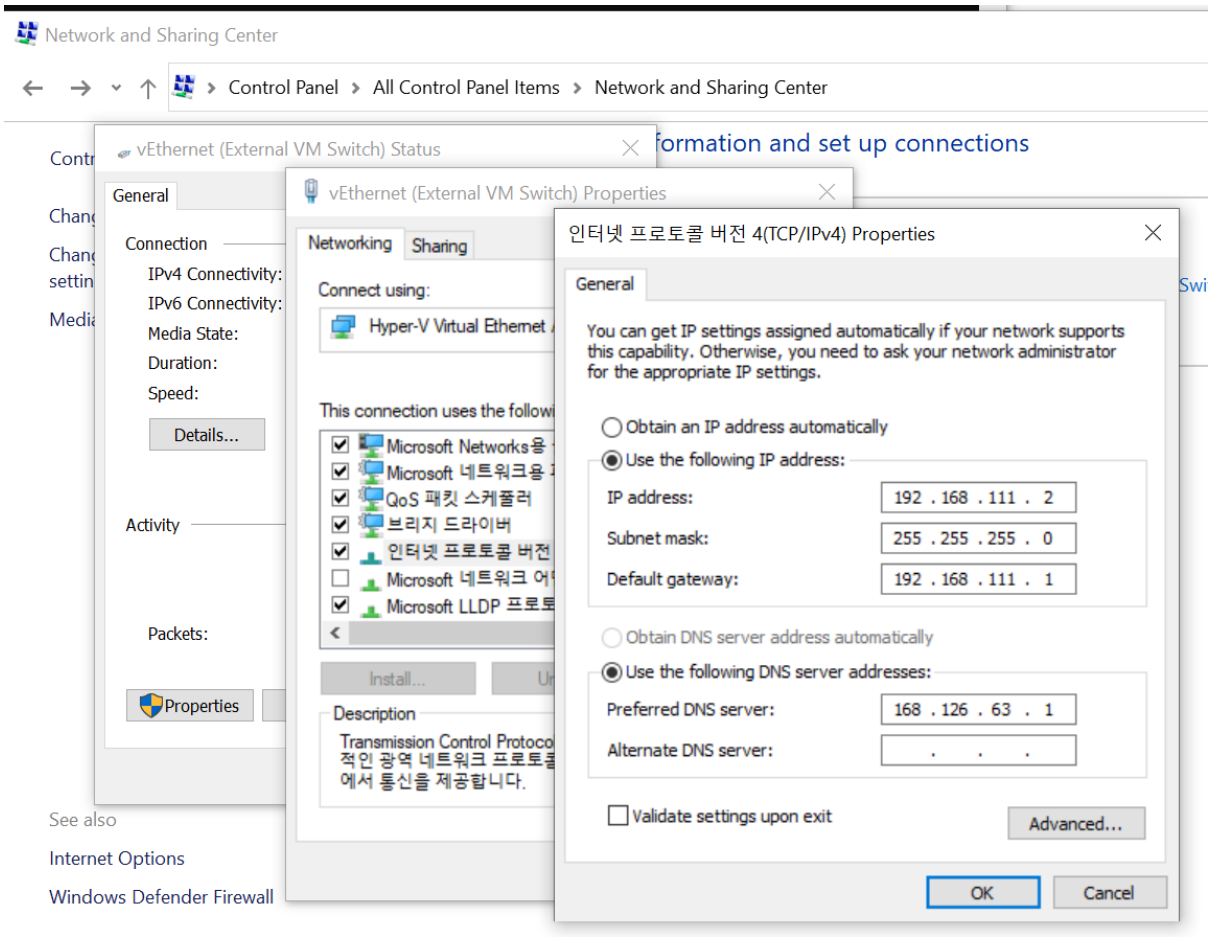


원래 사용하던 네트웍 장치인 Intel® Ethernet Connection(11) 1219-V 로 설정했다.

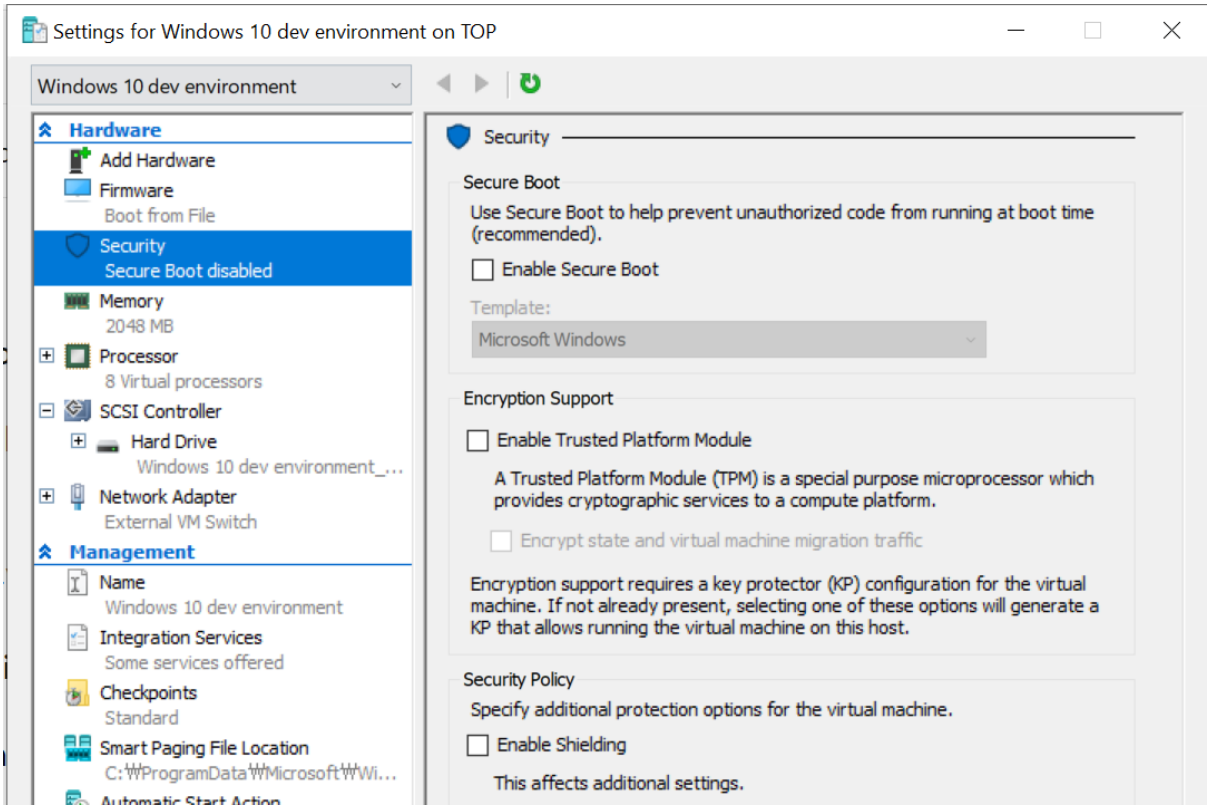
가상기계 설정에서 네트웍을 가상스위치로 변경한다.



호스트의 네트웍 설정에서 DNS 서버 설정을 해줘야 된다.



DISABLE SECURE BOOT



가상기계 설정에서 Secure Boot 설정을 끈다.

DEBUGGING TOOLS FOR WINDOWS

호스트 기계에 Debugging Tools for windows 를 설치한다.

C:₩Program Files (x86)₩Windows Kits₩10₩Debuggers₩x64 에 설치된다.

가상 기계의 C:₩KDNET 디렉토리로 복사한다.

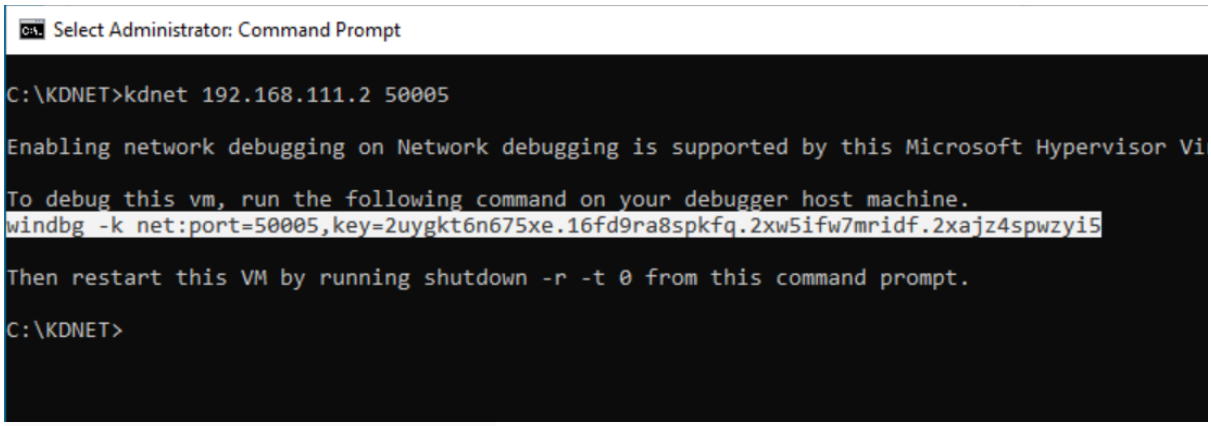
가상기계의 cmd 창에서

cd C:₩KDNET

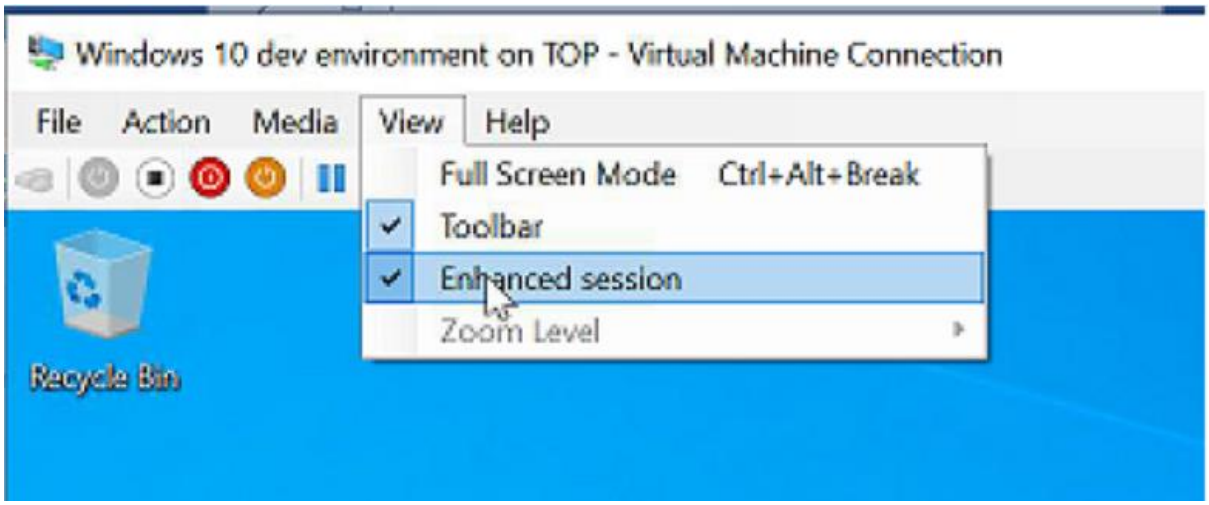
`kdnet 192.168.111.2 50005`

를 실행한다.

`192.168.111.2` 는 호스트 기계의 `ip` 주소이다.



실행할 때 나오는 메시지를 복사한다.



가상 기계에서 Enhanced Session 을 켜면 복사할 수 있게 된다.

이 상태에서 디버깅을 하면, 자주 가상 기계와의 연결이 끊겨서 불편하니, 사용한 후 다시 Enhanced Session 을 끈다.

호스트 기계의 cmd 창에서

cd C:₩Program Files (x86)₩Windows Kits₩10₩Debuggers₩x64

windbg -k net:port=50005,key=2uygkt6n675xe.16fd9ra8spkfq.2xw5ifw7mridf.2xajz4spwzyi5

실행한다.

이 상태에서 가상기계를 리부팅하면 디버거와 연결이 된다.

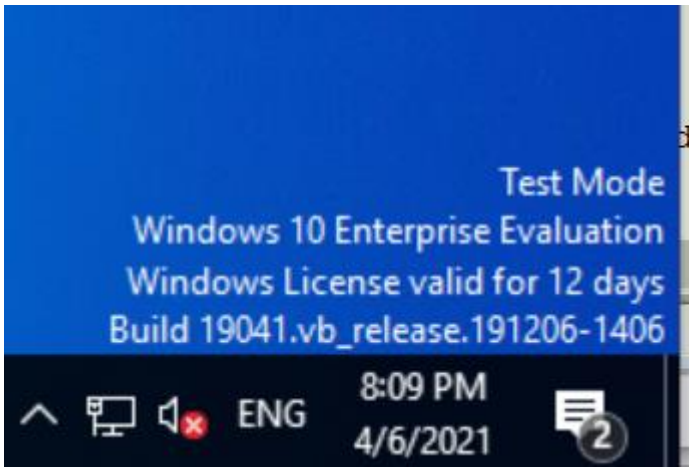
DEBUGGING DRIVER PROGRAM

ENABLE TEST SIGNING'

가상기계 cmd 창의 운영자 모드에서 다음을 실행한다.

```
bcdedit /set testsigning on
```

재부팅한다.



오른쪽 화면 하단에 Test Mode 라고 표시된다.

INSTALL DRIVER PROGRAM

가상기계에 드라이버를 설치한다.

설치 후 windirvert 드라이브를 정지시키려면 다음을 실행한다.

sc stop windirvert

SET BREAKPOINT

WinDivert64 모듈을 다시 로딩하려면

.reload /f WinDivert64.sys

W 로 시작하는 모듈을 나열하려면

lm m W*

WinDivert64!windivert_caller 로 시작하는 심볼을 나열하려면

x WinDivert64!windivert_caller*

함수에 WinDivert64!windivert_caller_context 에 중단점을 설정하려면

bm WinDivert64!windivert_caller_context

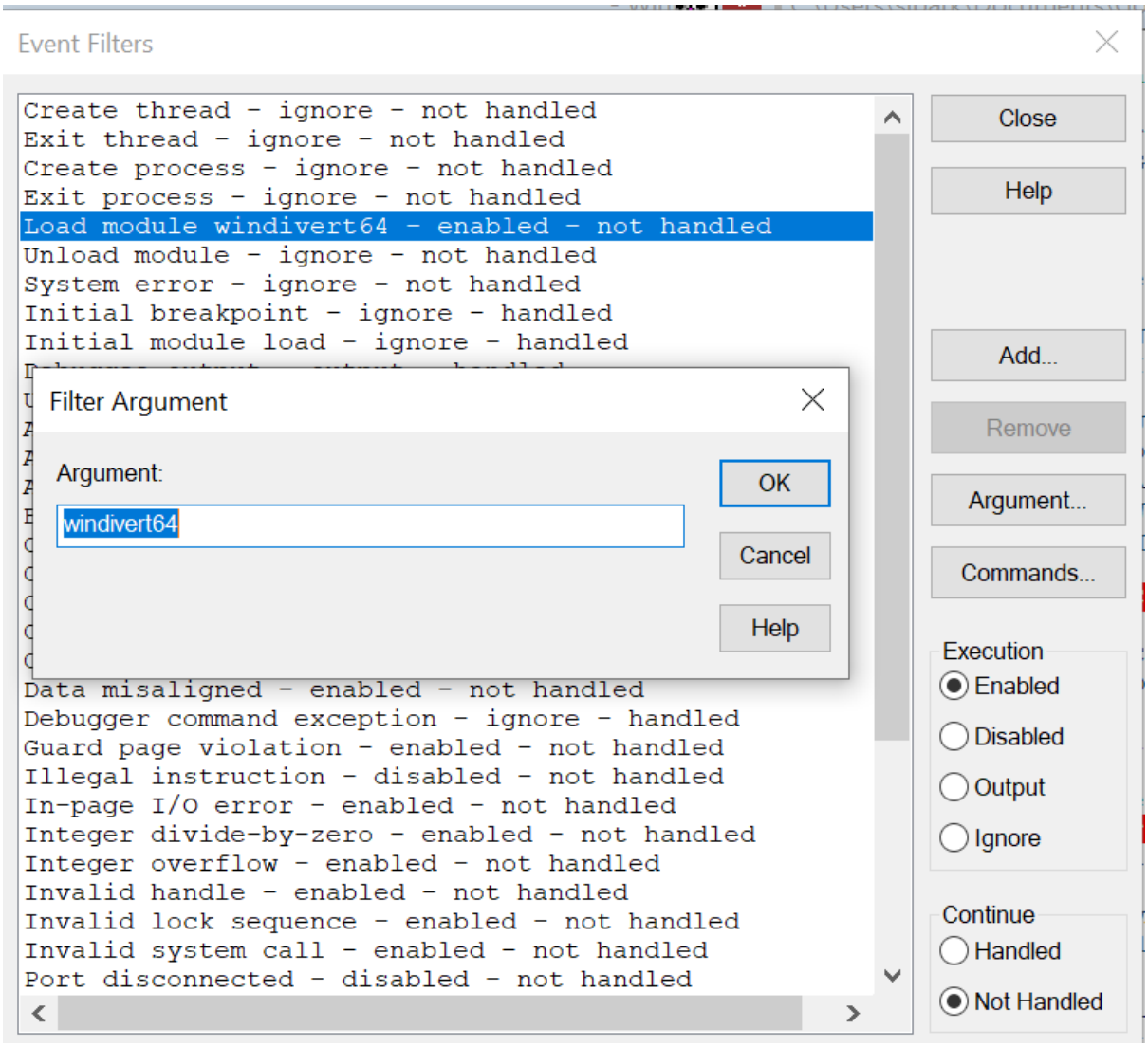
BREAKING AT DRIVER START UP

WinDbg > Debug > Event Filter >

Load Module >

Execution : Enabled

Argument > windivert64



실행(Go)하면 드라이버가 로딩되고, DriverEntry 호출하기 이전 순간에 멈춘다. Break Point 걸고 실행하면 된다.

그냥

bm WinDivert64!DriverEntry

만 해도 되는 듯 하다.