**MiniFilter Workshop**

Workshop Framework code + Solution is currently here:

<https://github.com/OmerBDeveloper/MinifilterWorkshop/tree/master/FsMinifilter>

**Prerequisites for participants**

**Visual Studio:**

1. Have a version of VS installed
   1. Free option is Visual Studio Community 2017:

<https://visualstudio.microsoft.com/downloads/>

1. Install a new enough SDK:
   1. At least 10.0.10586 from here:

<https://developer.microsoft.com/en-us/windows/downloads/sdk-archive>

1. Install a new enough WDK:
   1. For example <https://go.microsoft.com/fwlink/p/?linkid=859232>
   2. Or just google windows WDK and download the newest

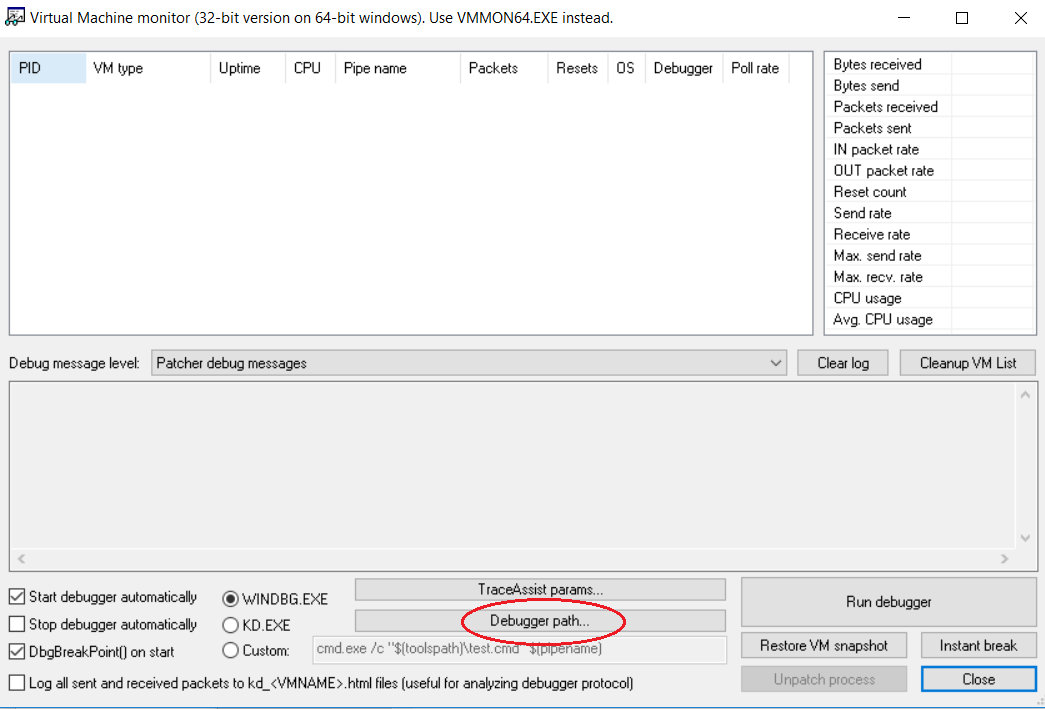
**VirtualBox:**

1. Install windows 7 32 bit from ISO to a new VirtualBox Machine.
2. Create a snapshot “CLEAN”
3. Install VirtualKD on machine
   1. You should have a folder called VirtualKD with the version number
   2. Inside this folder you should have a folder called “Target”
   3. Copy the “Target” machine to the target VM
   4. Run vminstall.exe
4. Reboot
5. Create a snapshot “READY”

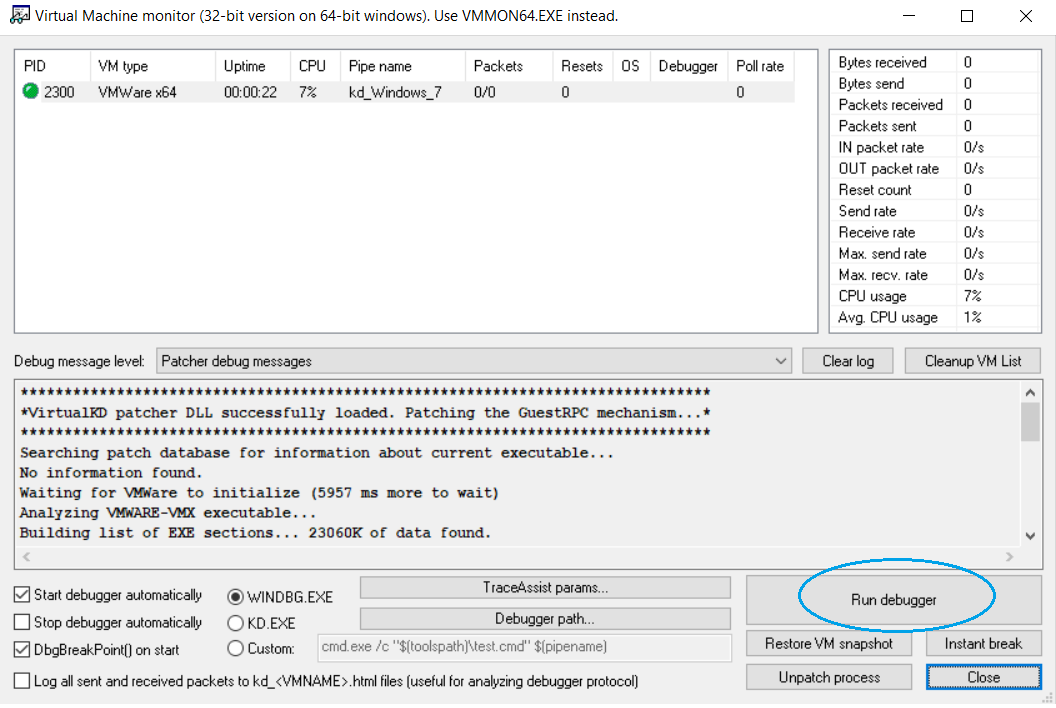
**Running with kernel debugger for the first time**

1. Run vmmon (part of virtual kd) on the host machine. You need to run that version with the same bit architecture as the target machine (the vm).
2. Set the debugger path of the vmmon to windbg

The path should be something like C:\Program Files (x86)\Windows Kits\10\Debuggers\x86



1. While vmmon is running restart the vm
2. Press Run debugger



1. Vmmon should lunch windbg and you can start debugging

**Kernel Debugging:**

1. Allow receiving out kernel dbgprint messages:
   1. “ed Kd\_DEFAULT\_Mask 8”

**Windbg useful commands:**

1. g \ F5 – for continue the run
2. F10 – next step (debugging)
3. F11 – step into (debugging)
4. .sympath+ c:\path\to\driver.pdb – adds the symbols of the driver
   1. Or just add the path using ctrl + s
5. .srcpath+ c:\path\to\driver\code – adds the source to the debugger
   1. Or just add the path using ctrl + p
6. .reload /f - for telling windbg to load the new symbols we gave it
7. Ctrl + O – open source file
8. Ctrl + break \ *debug -> break* option in the menu – in order to stop the vm

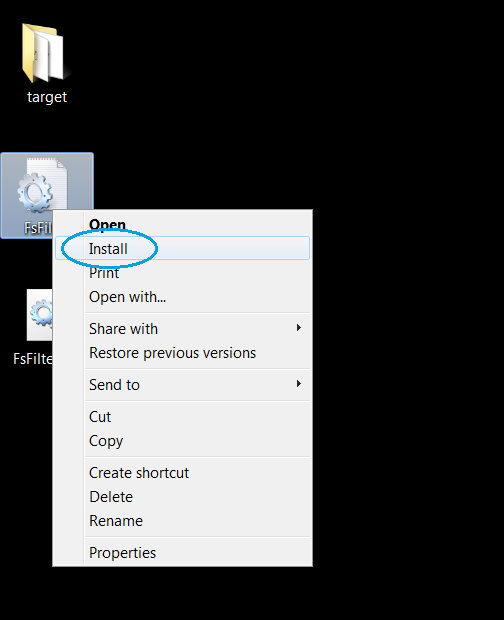
**Installing the driver on the vm:**

After compiling with Visual Studio the driver framework you have few output files, among them:

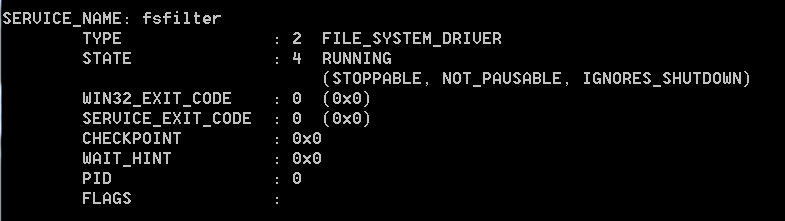
1. FsFilter.inf – a file which let you install the driver on the machine
2. FsFilter.sys – the driver itself
3. FsFilter.pdb the driver symbols – for debugging

In order to install the driver:

1. Copy both FsFilter.inf and FsFilter.sys to the same folder on the vm (you can use desktop)
2. Right-click on the FsFilter.inf and click install



1. Now you have the driver installed on the machine, but **not** running.
2. Run cmd as administrator and type to following command:  
   sc start fsfilter
3. The output should be something like:



1. In order to upgrade you driver to new on, first you should stop the driver
2. Run cmd as administrator and type to following command:  
   sc stop fsfilter
3. Then repeat step 1 with the new files
4. Remember – when you upgrade the driver you need to tell windbg to reload the new symbols, using the .reload /f command