Lab 4: Kmdf Power

# Overview

KMDF framework exposes a different model than WDM. There is no 1-1 map between IRP\_MJ functions and EvtXxxx callbacks.

For example

In this lab we'll learn to work with WinDBG to inspect various aspect of Kmdf power management

## Setup

* We will start with lab 3.

# Debug SmplDeviceEvtD0Entry and SmplDeviceEvtD0Exit

## Step 1

* On target machine, disable Sample Device
* Hookup WinDBG to the target machine
* Reload all module with: .reload
* Ask WinDBG to break when SmplDevice loads: sxe ld smpldevice
* g
* On target machine, enable Sample Device
* Verify: Debugger will break when smpldevice loads
* Using the 'x' command, find the D0 routines: x smpldevice!\*d0\*
* Put breakpoints (bu) on the D0 enter and exit
* g

## Step 2: Break on start

* Break on SmplDeviceEvtD0Entry
* In debugger, loads the wdfkd extension
* See dump about the device with !wdfdevice extension command.
* Find out the WDM object behind the WDF object
* Dump it's content using 'dt'. The type is nt!\_DEVICE\_OBJECT

## Step 3: Hibernate

* Enable hibernation. By default VmWare machine do not support hibernation. Using the powercfg.exe utility enable hibernation.
* Using shutdown.exe hibernate
* Verify you break on SmplDeviceEvtD0Exit
* Verity the target state.
* Try to find out which IRP\_MJ the IoManager has sent to the Framework.

## Step 4: start from hibernate

* Start the virtual machine
* You'll have a break when SmplDevice loads. You'll have to reload all symbols again
* g until you break on SmplDeviceEvtD0Entry
* Note that wdf appears on the stack twice
* Find IoCallDriver on the stack.
* Dump the call stack with 'kv' command.
* The second parameter is IRP. Using the !irp extension, dump the content.
* Note that we are 2nd on the irp stack. Above us there is the PnpManager, which is also a device driver.
* Check out what IRP\_MJ is 16, and what IRP\_MN is 2

## Step 5: Sleep

VmWare doesn't support the intermediate power states s1 through s3. An experimental feature exists, which requires manual modification to the \*.vmx file

* Open machine.vmx file
* Repeat steps 4 and 5 with sleep

# Capabilities

In this section we'll set the device capabilities

## Step 1

* Open the SmplDevice at the device manager. On the details tab see the Power Data.
* See the power data for other devices
* Check out power data for other devices

## Step 2: Change default capabilities

* Within WdfDeviceCreate, use the functions WdfDeviceSetPnpCapabilities and WdfDeviceSetPowerCapabilities to set the following capabilities: device is not removable, and