Please complete the following tasks:

**[1 point] Task 1 - Live Kernel Debugging**

For this task, you will need to setup a *Live Kernel Debugging* session similar to what I did in the video. Provide screenshots and a discussion walking through your setup as well as success from a live kernel debugging session, by tracing a call stack beyond user-space.

**[3 points] Task 2 - Host Kernel Debugging**

This task will require that you setup kernel-mode debugging between two virtual machines (although you can use physical if you have them available and find it easier). You will need to provide the VMs for this. You will find resources available online to help with this task, such as the following:

<https://www.vmware.com/support/ws55/doc/ws_devices_serial_2vms.html>

<https://www.vmware.com/support/ws55/doc/ws_devices_serial_advanced_example_debugging.html>

<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/setting-up-network-debugging-of-a-virtual-machine-host>

However, it is ultimately up to you to decide how best to approach this task.

Once you have your debug session working, trace the system call from the Task2.exe program - in particular, the only API call present in the program:



What have you found with kernel debugging when analyzing this? Share and discuss. Have you looked at anything else using kernel debugging? What did you observe?

**[1 point] Task 3 - System Profiling**

Our final task is to look into different performance monitoring/recording tools.

Using Windows Performance Recorder, create a large file and open with Notepad (or similar text editor, if you want to explore); start a trace to record activity during the file load. You can use the fsutil command to create a file of varying size.

Using Windows Performance Analyzer, analyze the results to determine what functional paths are most used during the file load functionality. What are your findings? Share and discuss.

**Deliverable**

A Word document or PDF with detailed steps and discussion from your lab.