Malware Analysis
Fall 2015
Lab 10 - Intro to Windows Kernel

**Part A**

1. (15%) Write a hello world driver in C for Windows 7 32-bit.
    - The driver should simply print “Hello world” to Dbgview.
    - You can either use DriverLauncher to load the driver into the kernel, or write your own binary to load the driver.

2. (25%) What is the Processor Control Block (PRCB/PCB)?
    - List each fields of the PRCB and describe what the PCRB is used for

**Part B - Lab_10-2.malware**

1. (10%) What is the address of the malicious function called by DriverEntry?

2. (10%) Describe the SIDT and LIDT instructions, what are they used for?

3. (10%) What is the malicious function doing? What is it creating?

4. (30%) What is this sample doing?