# Dynamic Analysis Lab

*Overview*

This lab will provide an introduction to the use of dynamic analysis tools on malware specimens. The use of these tools will allow students to practice the methods learned in chapter 3 in a secure sandbox environment.

This lab uses a sample executable that does not perform a malicious function. Using the tools mentioned in chapter three (3) and any other tools considered appropriate, analyze the given specimens, and answer the short answers to provide detailed dynamic analysis of the sample.

*Lab 3-1*

This lab uses the file *Lab3_1.exe*. Use the tools and techniques described in chapter three(3) to gain information about the file and answer the questions below.

## QUESTIONS

1. What are the program's imports and strings?
2. Is the malware packed?
3. Are there any indicators of network activity with the sample program?

   **Run the program**
4. What do you notice while monitoring this malware in Process Explorer?
5. Can you identify any live memory modifications?
6. What are the malware's host-based indicators?
7. Which network features does the malware use? (if any)

*Solution and Analysi*

*Unable to verify solutions*