Objectives:

- Lab 15 will be a live demonstration conducted by the instructor. Please observe and note responses to the following questions.

1. What are the main differences between the tools Regshot and CaptureBat?

2. What important findings were discovered by the Regshot and CaptureBat tools?

3. What does Process Explorer Do?

4. What were the main findings from Process Explorer?

5. What is Wireshark?

6. What were the important findings from Wireshark?

7. What does PEStudio do?

8. Did PE Studio find anything important?

9. What does FakeNet do?

10. Did FakeNet provide any important findings?

11. In your own words, what was the malware and what did it do?