Practical Malware Analysis

Chapter 2/3 Quiz

Chapter 2

1. What is an “air gapped network”?

2. What are the advantages and disadvantages of using a virtual machine for malware analysis?

3. What are the advantages and disadvantages of using dedicated hardware for malware analysis?

Chapter 3

1. What are two ways to run a DLL for analysis?

2. What is a mutex?

3. What is one way to recognize process replacement?

Bonus: Give the full path of one registry key commonly used for persistence.