Objectives

- Use the Volatility Standalone executable to analyze the memory dump *Vader_Home_Memory.raw*.
- Discover further evidence of crime, as it is relevant to this investigation.
- Use the Volatility Standalone executable to analyze the memory dump *SilentBanker.vmem.*

PART 1: *Vader_Home_Memory.raw* Memory Analysis Lab:

1. Identify what process(es) and PIDs have open TCP connections.
    a. What command did you use to obtain this data?
    b. Does it appear to be malicious? Why?
    c. What does the local port number indicate to you?

_____

_____

2. Identify what process(es) and PIDs had previously open TCP connections.
    a. What command did you use to obtain this data?
    b. Other than the connection previously mentioned, do any appear to be malicious? Why?
    c. What does the remote port number indicate to you?

_____

_____

3. Based on the PIDs you identified in the previous question, determine what processes were responsible for the suspect network connections.
    -What command did you use to obtain this data?

_____

_____

4. Extract the IRC malware to the local hard drive in both executable file format and in executable memory format. Which one is bigger? Why?

PART 2: SilentBanker Memory Analysis Lab:

1. Identify what process(es) and PIDs have open TCP connections for *SilentBanker.vmem* .
   -What command did you use to obtain this data?

2. Identify what process(es) and PIDs had previously open TCP connections for *SilentBanker.vmem*.
   -What command did you use to obtain this data?

3. Identify what process was victimized by injected malicious code for *SilentBanker.vmem*.
   -What command did you use to obtain this data?

4. Extract the injected malicious code to the hard drive for *SilentBanker.vmem*.
   -What command did you use to obtain this data?