Texas Tech University
Computer Science Department
CS5332 – Digital Forensics
Spring 2018, Individual Assignment 4
Due Date: TBA

Choose a malware of your choice or a rootkit from the list given in the following link:

https://github.com/d30sa1/RootKits-List-Download

Capture the memory dump while the malware or rootkit is running. And then report an analysis of the malware or rootkit using volatility or any other memory forensics tool. In particular, report what the malware or the rootkit is doing and whether you are able to capture its intended target and behavior.

Deliverable:

A report along with some snapshots showing.