

Texas Tech University
A Course on Digital forensics
Memory Forensics
Module 4 – Memory Acquisition
Akbar S. Namin, Spring 2018

DISCUSSION POST-2

Please post a message about given discussion topic, and reply at least 2 of your peers' posts.
Consider discussion rules and rubrics located under Welcome section.

Please, open your favorite search engine and make some Internet search for the following Current Analysis Techniques. You are supposed to write general characteristics of at least 3 analysis techniques and compare them. It should be approximately a half page for each technique, 3 pages in total.

Current Analysis Techniques:

- Acquiring Volatile Memory
- Where to Find Volatile Memory
- Persistence of Data Stored in Memory
- How Volatile Memory Works
- Strings Search
- How Memory is Organized
- Enumerating the Running Processes
- Recovering Memory-Mapped Files
- File Signature Search
- Detecting and Recovering Hidden Data