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

## MODULE AGENDA

**Module 4 - Memory Acquisition (Duration: 1 week, online)**

By the end of this module, you will be able to apply windows memory acquisition.

Memory acquisition (i.e., *capturing*, *dumping, and sampling*) involves copying the contents of volatile memory to non-volatile storage. It is one of the most important steps in the memory forensics process. You need to consider how acquisition tools work or how they encounter problems, before trusting them completely. Otherwise, you may end up with corrupt memory images, destroyed evidence, and limited, if any, analysis capabilities.

Furthermore, there is a link having videos about memory analysis with volatility.

**Outline: Memory Acquisition**

1. Preserving the Digital Environment
2. Memory Dump Formats
3. Converting Memory Dumps
4. Volatile Memory on Disk

**Activities:**

- **Reading:** Please read the chapter-4 in your course book. There is, also, an additional resource.
    - Memory Analysis with Dumplt and Volatility: https://www.youtube.com/watch?v=8BvZT9CR-4g&list=PLz2xkyHmktyi0bpUz2NeXXXgCZHIkPtcm
- **Quiz3:** Please complete the Quiz3 located under the Module4. Quiz3 covers the chapter4 topics, and includes 2 multiple choice, 1 true-false, and 1 open-ended questions. No late submission will be allowed.

- **Assignment4:** Please get screenshot all of the steps you will do, paste them a word document, and answer the questions. Please upload your file "YourSurname_Assignment4" under the assignment link.
- **Assignment5:** Please run the code given pages 84-89 under the "An Example of KnTDD in Action" title. When you perform each of the command, please get screenshot, paste them to a word document. Then please submit this document "YourSurname_Assignment5" to the assignment tab.
- **Discussion Post2:** 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. The topic is about current analysis techniques.

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