Texas Tech University
A Course on Digital forensics
Memory Forensics
Module 2 – The Agenda
Akbar S. Namin, Spring 2018

MODULE 2 - AGENDA

Module 2 - Data Structures (Duration: 1 week, online)

By the end of this module, you will be able to identify how data is organized within volatile storage. Data structures provide the template for interpreting the layout of the data. They are the basic building blocks that programmers use for implementing software and organizing how the program's data is stored within memory. It is important for you to have a basic understanding of the common data structures and how they are manifested within RAM.

This knowledge is beneficial for you to determine the most effective types of analysis techniques, to recognize malicious data modifications, and to make inferences about previous operations performed on the data. Additionally, this knowledge is base for learning why certain attacks (that manipulate the structure(s)) are successful and how memory analysis tools can help you detect such attacks.

Outline: Data Structures

1. Basic Data Types
   - Singly Linked List
   - Doubly Linked List
   - Circular Linked List
   - Embedded Doubly Linked List
   - List in Physical and Virtual Memory
   - Hierarchical Trees
   - Tree Traversal
   - Analyzing Trees in Memory

Activities

- **Reading:** Please read the chapter-2 in your course book.

- **Quiz2:** Please complete the Quiz-2 located under the Module2. It covers chapter-2, and includes 4 multiple choice questions and 1 true-false question. No late submission will be allowed.
- **Assignment1:** Please perform each step of the assignment. Get screenshot of each step you do, write your explanation for the last step, and upload your file "YourSurname_Assignment1"under assignment link.