**Texas Tech University**

**A Course on Digital forensics**

**Memory Forensics**

**Module 2 – Data Structures**

**Akbar S. Namin, Spring 2018**

# QUIZ-2

It covers chapter-2, and includes 4 multiple choice questions, and 1 true-false question.

**Q1-5: 1 points**

**1.** Which of the following data types consume 4 bytes on a 32-bit system?
- **A)** char
- **B)** unsigned int
- **C)** long
- **D)** pointer to an int
- **E)** pointer to a char

**The correct answer is: B, C, D, E**

**2.** Which statement(s) are false about arrays?
- **A)** Elements can be found by multiplying the desired index by the size of an element and adding it to the array's base address
- **B)** Elements are contiguous in memory
- **C)** Elements must be of a single data type (homogenous)
- **D)** Arrays cannot store pointers

**The correct answer is: D**

**3.** Which statements(s) are true about structures?
- **A)** Structures can store various different data types
- **B)** Structure sizes and member offsets can vary depending on compiler optimizations
- **C)** Operating systems and applications make heavy use of structures
- **D)** The names of structure members should indicate their purpose

**The correct answer is: A, B, C, D**

**4.** Linked lists are easily manipulated by rootkits. True or False?

**The correct answer is: True**

**5.** Performing memory forensics at the physical layer (i.e. without virtual address translation) limits analysis because:
- **A.** Strings that cross page boundaries may be fragmented in physical memory.

**B.** You cannot traverse linked lists.

**C.** Some hash tables and trees are never found in physical memory.

**D.** _UNICODE_STRING data types store metadata separately from the actual string content.

**The correct answer is: A, B, D**