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

MODULE AGENDA

Module 5 - Windows Memory Forensics (Duration: 2 weeks, face to face)

By the end of this module, you will be able to identify windows memory forensics and apply some activities about windows memory forensics. This module introduces you to the concepts of Windows executive objects, kernel pool allocations, and pool tag scanning. Specifically, you will use this knowledge to find objects (such as processes, files, and drivers) by using a method that is independent of how the operating system enumerates the objects. Furthermore, you can identify objects that were used but have since been discarded (but not overwritten), giving you valuable insight into events that occurred in the past. And, you can find an additional resource about malware hunting.

Outline: Windows Memory Forensics

1. Windows Objects and Pool Allocation
2. Process Memory Internals
3. Hunting Malware in Process Memory
4. Disk Artifacts in Memory

Activities:

- **Reading:** Please read the chapter-5 in your course book. There is, also, one more resource for you.
    - Malware Hunting: https://www.youtube.com/watch?v=xxf8Tz7QGjU
- **Discussion Post3:** 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.
    - What are the emerging and future technologies that we will have to worry the most about from a security perspective?

- **Group Presentations:** All groups will present a topic from the chapter-5. Groups will be assigned by the instructor at the end of the second module. Group members can communicate with each other using their personal e-mail. Groups will, also, prepare an activity for peers. After the presentations, all students will complete the group evaluation form to assess the other group's presentation and activity (The form is located under the Module5). After the presentations, all groups will be required to submit their presentations and activity documents.
- The topics are:
    - Windows executive objects
    - Pool-tag scanning and limitations of pool scanning
    - Big page pool
    - Pool-scanning alternatives
- Presentations should take max. 30 minutes. After presentations, there will be Q&A session taking 10 minutes. Then activities will start. They take 30-45 minutes. After the presentation, you will be required to fill out group evaluation form and submit it.