Texas Tech University
A Course on Digital forensics
Memory Forensics
Module 3 – The Agenda
Akbar S. Namin, Spring 2018

MODULE AGENDA

Module 3 - The Volatility Framework (Duration-1 week, online)

By the end of this module, you will be able to install Volatility framework, identify its main features, and run some basic commands.

The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License 2. Analysts use Volatility for the extraction of digital artifacts from volatile memory (RAM) samples.

This module covers the basic information you need to install Volatility, configure your environment, and work with the analysis plugins. It also introduces you the benefits of using Volatility and describes some of the internal components that make the tool a true framework.

Furthermore, there are some links about how to install volatility framework, and memory forensics with volatility.

Outline: The Volatility Framework

1. Why Volatility?
2. What Volatility Is Not
3. Installation
4. The Framework
5. Using Volatility

Activities:

- **Reading & Additional Resources:** Please read the chapter-3 in your course book. You may, also, want to look at these websites for more information:
    - http://www.volatilityfoundation.org/
    - Installation of Volatility part-1: https://www.youtube.com/watch?v=JKvtRXb1JNE

- Installation of volatility part-2: https://www.youtube.com/watch?v=aFX8N-cMXhE
- Memory forensics with volatility: https://www.youtube.com/watch?v=1Cl69Bj9T5s

- **Assignment2:** 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_Assignment2"under assignment link.
- **Assignment3:** Please install the volatility framework. After installation, please run the code given in pages 59-67 under the "Using Volatility" title in your textbook. When you perform each of the command, please get screenshot, paste them to a word document. Then please submit this document "YourSurname_VolatilityCommands" to the assignment area.
- **Discussion Post1:** 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.

  - Topic1: Please write 2 memory forensics tools and their main features except volatility framework. Compare them with volatility framework. Write pros and cons.

  - Topic2: What are the advantages of using volatility framework for finding advanced malware?

Please post a message about given discussion topic, and reply at least 2 of your peers' posts.