Texas Tech University

A Course on Digital forensics

Memory Forensics

Akbar S. Namin, Spring 2018

Online Syllabus

Institution & Program Name: Computer Science Master of Science

Course Code & Title: CS 5280 & Introduction to Memory Forensics

Semester: Spring 2017

Instructor Info

- Name Surname
- E-mail / Office Phone
- Office Location
- Office Hours

Course Information

- ***Description***: This class is an overview of an introduction the logic of solving digital crimes and fighting malware using memory forensics. Module one provides a general overview of the hardware components and operating system structures that affect memory analysis. Module two provides information about data structure for understanding how data is organized within volatile storage is a critical aspect of memory analysis. Module three covers the basic information you need to install Volatility, configure your environment, and work with the analysis plugins. It also introduces you to the benefits of using Volatility and describes some of the internal components that make the tool a true framework. Module four focuses on Windows memory acquisition, many of the concepts apply to other operating systems. Finally module five gives a brief information and activities about Windows memory forensics.

- ***Overview***: The purpose of the course is to give an introductory knowledge and skills about memory forensics. In order to do that, first three module gives fundamental knowledge such as hardware components, operating systems, data structure, and volatility framework. After that, fourth and fifth modules presents the knowledge and activities about memory acquisition and Windows memory forensics.

- ***Prerequisite***: Having an undergraduate degree from computer science or electronic engineering. Students should have, and be able to use Windows OS.

Textbook & Course Materials

- ***Required Text***: The Art of Memory Forensics Detecting Malware and Threats in Windows, Linux, and Mac Memory, Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, ISBN: 978-118-82509-9. It will be distributed online.
- ***Technical Requirements***: All students have to have their own laptop with high speed Internet access.

Learning Environment & Activities

Course Structure

- This course is delivered entirely online through the WWW, specifically Moodle course management system is used.
- Moodle provides learners with a variety of tools such as discussions, quizzes, e-mail, chat, keeping students records, assignment and so on.
- The course website is available for students taking this course. They are able to access the course website with their user name and password on Moodle.
- If you need support for accessing Moodle or getting username and password, please call Texas Tech University technology hotline at: 806-742-HELP.

Learning Activities & Participation

- Students should complete 3 discussions, 5 individual assignments, 1 group presentation and class activity, and 3 quizzes.
- In group presentations and class activity, 2 to 4 students should present one of the topics in Module5, and prepare a class activity such as some applications about Windows memory forensics. In order to arrange group members of each group, instructor and students will discuss it on the first week of the course, and decide on the groups. If there is a problem with group members in the following weeks, please contact with the instructor as soon as possible to rearrange the group.
- Participation: Students should contribute for each discussion subject, and reply at least 2 of their peers' posting. They should, also, complete individual assignments and group activities.
- Expectations: Students are expected to arrange their time for study this course, since it is fully online course. Also, they are expected to be self-motivated.

Grading

Assignment/Activity Name	Description	Points
3 quizzes	Quizzes are used for assessing the students' knowledge about the topics in Module1-2-4.	15 (5 for each)
1 group presentation and class activity	These activities will assess the students' presentation on given topics, and how they organize the class activity.	20
3 discussion posts	Discussion topics are used for assessing the students' synthesis ability about the given topics.	15 (5 for each)
5 individual assignments	They will assess the students' ability to run and apply the certain steps.	50 (10 for each)

Letter Grade	Percentage/Points
A	90-100
B	80-89
C	70-79
D	60-69
F	Below 60

Grading Policies:

- ***Assignment Submission Procedures***: Discussions, individual assignments, and quizzes have an exact due date. They should be submitted on time under the Assignment tab in Moodle.
- ***Late Submission& Missed Assignments:*** All assignments should be submitted on time. If there is late submission, 10% will be reduced for each day. No more than 3 days late won't be allowed. In addition to this, discussion posts and quizzes should be submitted on time. No late submission is allowed for these two activities.

Course Policies

- ***Academic integrity***: All students must maintain the academic integrity and dishonesty which includes plagiarism, using others' ideas or written materials without their permission, stealing computer software, and etc. All of the materials must be cited, paraphrased, or quoted properly. You can find additional information at this link: http://www.depts.ttu.edu/studentjudicialprograms/academicinteg.php. The penalty of the academic dishonesty will be F grade.
- ***Incompletes:*** Incomplete grades may be considered when students have extraordinary cases such as disease. Students have to notify instructor for their excuses. In order to get an incomplete grade, arrangements should be made with instructor. Incompletes are applied with one grade reduction.
- ***Special needs***: Students who have disability may need additional support to meet the course requirements. They should contact with the instructor immediately to make proper adjustments in the course. Students must get a verification from Student Disability Services to get adjustments in the course. Please notice that instructors are not allowed to do adjustments before getting the verification. Please contact with the Student Disability Services which is located at West Hall in 335 or call 806-742-2405.
- ***Religious observances:*** Students who want to be excused from attending classes, activities, and etc. should inform the instructor timely. They should make up the exams, activities, or work when they miss them because of the religious holidays.

Course Objectives

Student Learning Objective/Outcome By completing all course requirements, students will be able to:	**Assignment(s) or activity(ies)** List and brief explanation of activities validating outcome achievement for each objective:
Students will be able to identify the effect of hardware components and operating system structures.	Quiz1 covers the module1 subjects.

Students will be able to identify the data structure about how data is organized within volatile storage.	Quiz2 covers the module2 subjects. Assignment1 covers chapter-2.
Students will be able to install volatility. They will be also able to identify the benefits of volatility and describe the internal components.	Assignment 2-3 – installation of volatility, and running the codes given in pages 59-67 under the "Using Volatility" title. Discussion1 – discussion topic about module3 subjects.
Students will be able to apply windows memory acquisition.	Quiz3 covers the module4 subjects. Assignment4 – Performing some steps in Volatility. Assignment5 – Running the codes given in pages 84-89 under the "An Example of KnTDD in Action" title in course textbook. Discussion2 – discussion topic about emerging and future technologies from security perspective.
Students will be able to identify windows memory forensics, and apply some activities about windows memory forensics.	Group presentations and activities. Each group will present a subject about windows memory forensics, and prepare an activity for class. Discussion3 – discussion topic about current analysis techniques.

Course Outline and Schedule

Module	Topic	Readings	Activities	Due Date
0	Introduction	-	Course Syllabus and Assignments Using course web site	1 week
1	System Overview	Chapter1 of the main book	Quiz1	1 week
2	Data Structures	Chapter2 of the main book	Assignment-1 Quiz2	1 week
3	The Volatility Framework	Chapter3 of the main book	Assignment-2-3: Installation of volatility framework, and running the given codes Discussion1	1 week
4	Memory Acquisition	Chapter4 of the main book	Assignment-4 Assignment-5 Discussion2 Quiz3	1 week
5	Windows Memory Forensics	Chapter5 of the main book	Presentations (2weeks) Discussion3 Group evaluation form after presentations	2 weeks