CFRS 790 – Advanced Computer Forensics

Department of Electrical and Computer Engineering

Computer Forensics Program

George Mason University

Spring 2016

Instructor: Jonathan P. Fowler

E-Mail Address: jfowler9@gmu.edu

Office Location: TCOM Adjunct Faculty Offices

Office Hours: By request only

Class Time: Fridays, 4:30-7:10 p.m.

Location: Nguyen Engineering Building, Room 1505

NOTE: All students MUST have a GMU e-mail account and have access to blackboard.gmu.edu. Students must use their MasonLIVE e-mail account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.

Course Description (from GMU catalog):

This is the capstone course for the MS in Computer Forensics program. CFRS 790 will integrate the concepts and practices developed within the Computer Forensics Program. Students will be exposed to case studies and be required to conduct computer forensic investigations of digital media, intercepted packet switched data, and multisource log information to successfully complete each exercise.

Prerequisites:

CFRS 660, CFRS 661, and CFRS 663; and, a minimum of 18 credits in the MS in Computer Forensics program prior to registration.

Course Objectives:

During this course, students will be able to apply the processes and procedures learned in prior classes to conduct forensic examinations of data from various scenarios using tools and techniques presented throughout the Computer Forensics program. Additionally, students will be able to communicate the results of an examination in both verbal and written methods to various types of audiences.

By the end of the semester, students should be comfortable with not only preparing an expert report based on their analysis of a forensic matter, but should also feel comfortable defending their analyses and findings, both orally and in writing.

Grading:

Grading will be assessed on the following components:

Quiz #1:	15%
Quiz #2:	15%
Project:	25%
Final Exam:	35%
Class Participation:	10%
TOTAL:	**100%**

Course Material:

The text for this course is listed below. Additional electronic material may be posted through the class Blackboard site – if so, I will send an e-mail to the class informing everyone:

- Digital Archaeology: The Art and Science of Digital Forensics, Graves, Michael, 2014, Pearson Education, Inc.

Course Schedule (subject to change):

Class #	Topic(s)	Readings
1	Administrative items; Course overview; Discussion – "What do we do?"; Class Exercise – MAC Times	Chapters 20-21 (not necessary to have fully read)
2	Expert vs. Fact Witness; Notes?? What Notes?; Class Exercise - Identification of Removable Media on Windows/Mac Computers	Chapters 1-2
3	"Raiders of the Lost Files"; Class Exercise – The Diary	Chapter 8
4	Class Exercise – The Diary (cont.)	
5	Network Forensics; Class Exercise – Fun with Odd-Toed Ungulates; Review for Quiz #1	Chapter 12
6	The Deposition – "Do you know what time it is?"; Quiz #1	
7	Cloud Forensics (or, "Great, even more sources of information); Class Exercise – Is it really that simple?	Chapter 13
8	Mobile Forensics ("the phabulous world of phablets	Chapter 14
9	Litigation & Electronic Discovery; Housekeeping; Other Items	
10	Class Presentations	
11	Document Analysis – when what you have isn't always what you have; Class Exercise – The Astronaut; Review for Quiz #2	Chapter 9
12	Anti-Forensics; Class Exercise – The Diary (Revisited); Quiz #2	Chapter 15

13	Class Exercise – Wait, you can do that?	
14	Timeline Analysis – Putting it all Together	
15	Review for Final Exam	

Academic Integrity:

George Mason University is an Honor Code University; please see the Office for Academic Integrity for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely.

What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else's work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions.

When in doubt (of any kind) please ask for guidance and clarification.

Disability Policy:

If you have a documented learning disability or other condition that may affect academic performance, you should (1) make sure this documentation is on file with the Office for Disability Services (located in SUB1, Room 4205, 703-995-2474, http://ods.gmu.edu) to determine the accommodations you need; and, (2) talk with me to discuss your accommodation needs.