CFRS 790 – Advanced Computer Forensics

Department of Electrical and Computer Engineering

Computer Forensics Program

George Mason University

Fall 2012

Instructor: Jonathan P. Fowler, EnCE, ACE

E-Mail Address: jfowler9@gmu.edu

Office Location: TCOM Adjunct Faculty Offices

Office Hours: By request only

Class Time: Fridays, 6:00-8:40 p.m.

Location: Nguyen Engineering Building 5358

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.

This will be accomplished through the use of case studies presented in a seminar environment. These case studies will require some research and forensic analysis, culminating in written expert reports outlining their findings and opinions. Additionally, each student will be required to give an oral presentation of their findings for one case study and to answer questions based on their findings and report.

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:

Because the majority of forensic examinations conducted result in written reports being generated, grading will be assessed on the following components:

Curriculum Vitae:	5%
Quiz #1:	15%
Quiz #2:	15%
Expert Report:	25%

(Note: As written expert reports are the primary means in which both attorneys and judges will be introduced to your analyses and opinions, it is essential that the reports be written in a clear, concise manner. As such, all basic grammar, punctuation, and any typographical errors will be taken into account when grading the reports. The maximum amount deducted from any report for any and all types of these errors will be 15%.)

Final Exam:	20%

(Note: The Final Exam will be a take-home exam. Please respect the GMU Honor Code.)

Class Participation:	10%
TOTAL:	**100%**

Course Material:

There are two texts for this course 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:

- Writing and Defending Your Expert Report: The Step-by-Step Guide with Models, Babitsky, Steven and James J. Mangraviti, 2002, SEAK, Inc.
- Depositions: The Comprehensive Guide for Expert Witnesses, Babitsky, Steven and James J. Mangraviti, 2007, SEAK, Inc.

Tentative Course Schedule (subject to change):

Date	Topic(s)	Readings	Assignments Due
08/31/11	Administrative items; Course overview; Overview of expert reports; Practical Exercise	Writing/Defending - Chapters 1 to 5 (not necessary to have done before start of class)	
09/07/11	Review of USB file analysis techniques; Hands-on: USB thumb drive analysis; Expert Reports – Qualifications and preparing your Curriculum Vitae	Writing/Defending - Chapter 7	
09/14/11	Presentation/discussion of Exercise #2 – File Signature Analysis; Overview of depositions	Depositions - Chapter 1	Curriculum Vitae
09/21/11	Review of file identification techniques; Hands-on: Basic techniques to match files to removable media;Depositions – preparing to testify; Review of material covered to date	Depositions – Chapter 3	
09/28/11	Guest Speaker – TBD; Review of registry analysis techniques; Expert reports – Material reviewed	Writing/Defending – Chapter 6	
10/05/11	Presentation/discussion of Exercise #3 – Registry Analysis; Expert reports – Factual assumptions	Writing/Defending – Chapter 8	Quiz #1
10/12/11	Timeline analysis techniques		
10/19/11	Timeline analysis techniques; Depositions – What can you be asked?	Depositions – Chapter 5	
10/26/11	Timeline analysis techniques; Expert reports – Opinions and conclusions	Writing/Defending – Chapter 10	
11/02/11	Introduce practical exercise for expert report; Depositions – Goals of opposing counsel	Depositions – Chapter 2	Quiz #2
11/09/11	Practical exercise for expert report; Expert reports – Red Flags	Writing/Defending – Chapter 14	

11/16/11	Practical exercise for expert report; Depositions – Expert witness testimony	Depositions – Chapter 6	
11/23/11	*** NO CLASS – THANKSGIVING RECESS ***	Writing/Defending – Chapter 13	
11/30/11	Hands-on: Special problems in Forensics; Discussion of Exercise #6; Depositions – Expert witness testimony (continued)	Depositions – Chapter 6	Expert Report
12/06/11	Review for Final Exam; Depositions/Expert Reports – What's left?	NO READINGS	
12/13/11	*** NO CLASS ***	*** EXAMINATION PERIOD ***	

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.