CFRS 790 – Advanced Computer Forensics

Department of Electrical and Computer Engineering

Computer Forensics Program

George Mason University

Spring 2013

Instructor: Jonathan P. Fowler

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, Room 5358

NOTE: All students <u>MUST</u> 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, combined with information provided in a standard lecture format.

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:	30%

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

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

Course Material:

There is one (1) text 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.
    -

Course Schedule (subject to change):

Date	Topic(s)	Readings	Assignments Due
01/25/12	Administrative items; Course overview; Overview of expert reports; Class Exercise – MAC Times	Writing/Defending - Chapters 1 to 3 (not necessary to have done before start of class)	
02/01/12	Identifying removable media on Windows/Mac platforms; Hands-on: removable media analysis; Expert Reports – Qualifications and preparing your Curriculum Vitae	Writing/Defending - Chapter 7	
02/08/12	Removable media analysis techniques – what data is stored on removable media?	Writing/Defending - Chapter 4-5	Curriculum Vitae
02/15/12	Presentation/discussion of Case Study #1 – Intellectual Property Theft		
02/22/12	Windows Registry Analysis; Expert reports – Factual assumptions; Quiz Review	Writing/Defending – Chapter 6	
03/01/12	Quiz #1; Review of Windows registry analysis tools	Writing/Defending – Chapter 8	Quiz #1
03/08/12	Internet history analysis – review of browser histories (IE, FireFox, Chrome, Safari, Opera); Expert reports – opinions and conclusions	Writing/Defending – Chapter 10	
03/15/12	** NO CLASS **	** SPRING BREAK **	
03/22/12	Presentation/discussion of Case Study #2 – Accessing/possession of inappropriate material; Expert reports – opinions and conclusions	Writing/Defending – Chapter 10	
03/29/12	Basic OSX/Mac analysis; Expert reports – opinions and conclusions; Review for Quiz #2	Writing/Defending – Chapter 10	
04/05/12	Quiz #2; Expert reports – Red Flags	Writing/Defending – Chapter 14	Quiz #2

04/12/12	Presentation/discussion of Case Study for Expert Report; Expert reports – What doesn't go into an expert report?	Writing/Defending – Chapter 13	
04/19/12	Timeline analysis; Continued discussion of Case Study for Expert Report		
04/26/12	Timeline analysis; Continued discussion of Case Study for Expert Report		
05/03/12	Review for Final Exam	NO READINGS	Expert Report
05/10/12	*** NO CLASS ***	*** FINAL EXAMS ***	Final Exam released on BB on 5/6/ – due by 5:00PM on 5/10

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.