

TCOM 590 Sec 003 – Incident Response and Corporate Forensics
Department of Electrical and Computer Engineering
George Mason University
Spring, 2008

Syllabus revised 11/19/07

Administrative Information

Instructor:

Dr. Aleksandar Lazarevich

Email: alazarev@gmu.edu [subject=GMU-TCOM590-Sec/003_Your_name](mailto:alazarev@gmu.edu)

Phone: 703-393-2247

Office hours: By appointment

Teaching Assistant

Mr. Ayman Karamalla <akaramal@gmu.edu>

Course Description

590 Sec 007 Incident Response and Corporate Forensics (3:3:0)

Prerequisites: Permission of Instructor. Much of today's computer is aimed at corporate America. These crimes are perpetrated either directly against the companies or through the victimization of the consumer and using that data to access those same companies. These crimes are usually detected initially as a computer incident. As these incidents are investigated, many become escalated into full blown forensic investigations that are either turned over to law enforcement or become litigations. 80% of computer forensic work today is done by private companies. This course will address incident detection, response, and those aspects of computer forensics pertinent to the investigation of trade secret theft, economic espionage, copyright infringement, piracy, and fraud.

Textbooks

Computer Security Incident Handling Guide, NIST Publication SP800-61 Revision 1 (Draft), Grace, Kent, Kim, September 2007,
<http://csrc.nist.gov/publications/nistpubs/index.html>

Guide to Integrating Forensic Techniques into Incident Response, NIST Publication SP800-86, Kent, Chevalier, Grance, Dang, August 2006,
<http://csrc.nist.gov/publications/nistpubs/index.html>

Computer Forensics – Principles and Practices

Linda Volonino, Reynaldo Anzaldúa, Jana Godwin; 2007; Pearson/Prentice Hall; ISBN: 0-13-154727-5, Publisher's Web page:

<http://vig.prenhall.com/catalog/academic/product/0,1144,0131711261,00.html>

Grading

Raw scores may be adjusted to calculate final grades.

Grades will be assessed on the following components:

Homeworks (5@10% each)	50%
Mid-term exam	25%
Final exam	25%

These components are outlined in the following sections.

Homework

Homework 1 - In a 3-4 page paper, describe an incident response plan. Ensure you include who will respond and escalation criteria and procedures.

Homework 2 - In a 3-4 page paper, address the following: When a running computer is seized it must be powered down for transport to the trusted environment of the forensics lab. Current practice is to simply pull the plug, thereby preserving the operating system's temporary files, which may have forensic value. Are there situations where this is an unwise move? What about temporary data being held in memory on a laptop computer? Hibernating the laptop would preserve that data. How would you redesign computer hardware and software to make the forensic investigator's job easier?

Homework 3 – In a 3-4 page paper, address the following: Windows users commonly run their computers with administrative privileges. What are the implications of this for the forensic investigator? Offer an example situation in which this fact might make a critical difference in an investigation

Homework 4 - In a 3-4 page paper, address the following: When performing forensics during incident response, an important consideration is how and when the incident should be contained. Modify the plan from homework 2 to account for this need.

Homework 5 - In a 3-4 page paper, address the following: The large amount of e-evidence gathered in the Caffrey case (p. 350) was not enough to convict the defendant. Discuss the possible reasons for this. What does it take to prove a case based solely upon e-evidence? Is the burden of proof higher? What are the implications for forensic practice?

Reports will due in Weeks 4, 6, 9, 12, and 15.

Late reports will be assessed a penalty of 25% of the assignment grade for each week or part there of it is late.

Mid-term exams

The mid-term exam will be conducted during class time in Week 7 and will cover material discussed in Weeks 1-6.

The mid-term exam will be “closed book”– no reference materials other than those provided with the exam paper will be permitted.

Final exam

The final exam will be held the week after the final class in the same room used for classes and will cover material from the weeks 9-15.

The final exam will be “closed book” – no reference materials other than those provided with the exam paper will be permitted.

Schedule

Week	Date	Topic	Reading Assignments	Projects Due
Week 1	1/23/2008	Incident Response	SP800-61 Chapt 2-3	
Week 2	1/30/2008	Incident Response (Cont)	SP800-61 Chapt 4-8	
Week 3	2/6/2008	Forensic evidence	Book Chapt 1 & 2	
Week 4	2/13/2008	Evidence Collection	Book Chapt 3	Report 1 due
Week 5	2/20/2008	Policies and Procedures and Data	Book Chapt 4 & 5	
Week 6	2/27/2008	OS & Data Transmission	Book Chapt 6	Report 2 due
Week 7	3/5/2008	Mid-Term	Covers weeks 1-6	
Week 8	3/12/2008	Spring Break		
Week 9	3/19/2008	Computers and the Web	Book Chapt 7 & 8	Report 3 due
Week 10	3/26/2008	Forensic Integration	SP 800-86 Chapt. 2 & 3	
Week 11	4/2/2008	Forensic Integration (Cont)	SP 800-86 Chapt. 4-8	
Week 12	4/9/2008	Detection	Book Chapt 9	Report 4 due
Week 13	4/16/2008	Tracking	Book Chapt 10	
Week 14	4/23/2008	Investigation	Book Chapt 11	
Week 15	4/30/2007	Law, ethics and testimony	Book Chapt 12 & 13	Report 5 due
Week 16	5/7/2007	Final exam	Covers Chapt. 7-14	

This schedule is subject to revision before and throughout the course.

Call 703-993-1000 for recorded information on campus closings (e.g. due to weather).

Important Dates

Last day to add classes

Tues. Feb. 5

Last day to drop with no tuition liability

Tues. Feb. 5

Last day to drop

Fri Feb 22

From

<http://registrar.gmu.edu/calendars/spring08academiccalendar.pdf>

See that Web page for more information.

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Honor Code

Students are required to be familiar and comply with the requirements of the [GMU Honor Code^{\[1\]}](#).

The Honor Code will be strictly enforced in this course.

All assessable work is to be completed by the individual student.

Students must **NOT** collaborate on the project reports or presentation without explicit prior permission from the Instructor.

^[1] Available at www.gmu.edu/catalog/apolicies/honor.html and related GMU Web pages.